Fall 2022

On Multiplication Groups of Quasigroups

Ahmed Al Fares
Claremont Graduate University

On Multiplication Groups of Quasigroups

Ahmed Al Fares

Institute of Mathematical Sciences

Claremont Graduate University

APPROVAL OF THE REVIEW COMMITTEE

This dissertation has been duly read, reviewed, and critiqued by the Committee listed below, which hereby approves the manuscript of Ahmed Al Fares as fulfilling the scope and quality requirements for meriting the degree of Doctor of Philosophy.

Lenny Fukshansky

Mathematical Sciences Department, Claremont McKenna College

Professor

Gizem Karaali, Chair

Department of Mathematics and Statistics, Pomona College

Professor

Ali Nadim

Institute of Mathematical Sciences, Claremont Graduate University

Professor

Michael Orrison

Department of Mathematics, Harvey Mudd College

Professor

Abstract

On Multiplication Groups of Quasigroups

by

Ahmed Al Fares

Claremont Graduate University: 2022

Quasigroups are algebraic structures in which divisibility is always defined. In this thesis we investigate quasigroups using a group-theoretic approach. We first construct a family of quasigroups which behave in a group-like fashion. We then focus on the multiplication groups of quasigroups, which have first appeared in the work of A. A. Albert. These permutation groups allow us to study quasigroups using group theory. We also explore how certain natural operations on quasigroups affect the associated multiplication groups. Along the way we take the time and special care to pose specific questions that may lead to further work in the near future.

Acknowledgements

First and foremost, I dedicate this dissertation to give thanks to God for giving me the strength and the patience throughout my academic career. I would also to thank my family, my parents, my wife, and my siblings for the all the support they have given me. I give special thanks to my wife for being with me from the first day supporting, encouraging, and being always by my side in every step. Throughout the years, I had incredible support from my friends. Friends that I knew all my life, and others that came to my life during my graduate studies.

Attending CGU, I consider myself extremely lucky to meet some of the greatest and nicest people. Special thanks go to Dr. Gizem Karaali, my Ph. D. dissertation advisor, for all the incredible things I learned from her. I was fortunate to have given the opportunity to work with such a great individual. As my academic advisor, I would like to express my appreciation to Dr. Ali Nadim for being there for me throughout these eight years. I would also like to thank all my professors at CGU and the Claremont Colleges and all the staff that took part in any form or shape in this journey. I would like to specifically thank Charlotte Ballesteros, the CGU IMS coordinator.

I would like to thank my dissertation committee members for their comments, questions, and suggestions that helped a great deal with forming this dissertation. A special thanks to Professor Fukshansky and Professor Orrison for the suggestions and detailed comments they gave on a draft of this dissertation and on during the dissertation defense and dissertation proposal presentations. Thanks to you all Dr. Fukshansky, Dr. Karaali, Dr. Nadim, and Dr. Orrison.

I would not have made it this far without the help of all my professors during my B. S. and M. S. degrees. Especially Dr. Mike Krebs who was my master's thesis advisor at California State University Los Angeles. I would also like to thank Dr. Gary Brookfield who inspired my interest in abstract algebra, and Dr. Anthony Shaheen both of which were part of my master's thesis committee. I would like to also thank other professors who I enjoyed taking and learning in their classes. I would like to also thank my other professors from CalStateLA: Dr. Gerald Beer, Dr. Derek Chang, Dr. Borislava Gutarts and Dr. Bebasree Raychaudhuri; and my academic advisor Dr. Daphne Liu.

I would like to also thank all my other professors during my CGU journey: Dr. Michelle Bligh, Dr. Marina Chugunova, Dr. Stephan Garcia, Dr. Chiu-Yen Kao (CMC), and Dr. Andrew Nguyen. Also, I would like to than Dr. Allon Percus with whom I had my admission interview and was the first to welcome me to CGU.

This journey would not have been possible without my Professor from King Fhad University of Petroleum and Minerals. I would like to specifically thank Dr. Rajai Alassar and Dr. Stephen Binns.

I would like to end with what I started this acknowledgement with: I thank you God for everything.

Table of Contents

Chapter 1

Introduction

This thesis explores quasigroups and their multiplication groups. In this chapter we begin with some algebraic preliminaries where we briefly introduce the main terms and set the notation used in the rest of the thesis (Section 1.1). Then we describe the contents of the thesis (Section 1.2). Finally we offer some motivation for the work done here (Section 1.3).

1.1 Preliminaries

1.1.1 Latin Squares - A Quick Introduction

We start this section by giving the definition of a Latin square.

Definition 1.1.1 *A* **Latin square of order** *n is a square array of n rows and n columns built up from n different symbols so that no symbol occurs more than once in any row or column.*

Example 1.1.2 *Below are two Latin squares of order 3.*

A	B	C
B	C	A
C	A	B

A	B	C
C	A	B
B	C	A

Definition 1.1.3 *[16] A Latin square with n characters is said to be reduced if both the first row and first column entries are in the order 1 through n.*

Example 1.1.4 *There are 576 size 4×4 Latin squares. Only four are reduced Latin squares of order 4. These are:*

*	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	2	1
4	4	3	1	2

*	1	2	3	4
1	1	2	3	4
2	2	3	4	1
3	3	4	1	2
4	4	1	2	3

*	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

*	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

The name "Latin square" was inspired by mathematical papers by Leonhard Euler, who used Latin characters as symbols [48]. The Latin characters can be replaced by the integers $1, 2, \ldots, n$, which is the way most Latin squares are going to be presented in this dissertation.

Latin squares, in various disguises, appear throughout history and in contemporary culture, most notably in the form of magic squares and sudoku puzzles. As mathematical structures, their modern study typically belongs in combinatorics (combinatorial design theory) though through their connections to quasigroups, they have also found a natural home in algebra. All this work has led to a variety of interesting applications; we describe some in Section 1.3.

The exact number of order n Latin squares is known up to $n = 11$ [1]. More generally, the most accurate lower and upper bounds for the number L_n of order n Latin squares are

$$\prod_{k=1}^{n} (k!)^{n/k} \geq L_n \geq \frac{(n!)^{2n}}{n^{n^2}}. \tag{1.1.1}$$

A formula to calculate L_n is

$$L_n = n! \sum_{A \in B_n} (-1)^{\sigma_0(A)} \binom{\operatorname{per} A}{n}. \tag{1.1.2}$$

For more on L_n, see [46].

One of the classical problems involving Latin squares is that of finding mutually orthogonal Latin squares. To explain this problem we need:

Definition 1.1.5 *[22] Two order n Latin squares $S = [s_{ij}]$ and $T = [t_{ih}]$ are said to be* **orthogonal** *if every ordered pair of symbols occurs exactly once among the n^2 pairs (s_{ij}, t_{ij}), $i, j = 1, 2, \ldots, n$.*

Example 1.1.6 *There are no orthogonal Latin squares of order $n < 3$ [22]. The two Latin squares given below are orthogonal.*

	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

	1	2	3
1	2	3	1
2	1	2	3
3	3	1	2

To see this we compute the nine ordered pairs:

	1	2	3
1	1,2	2,3	3,1
2	2,1	3,2	1,3
3	3,3	1,1	2,2

Definition 1.1.7 *[22] A set of order n Latin squares is said to be* **mutually orthogonal** *if each pair of Latin squares is orthogonal. Such a set is called a* **set of mutually orthogonal Latin squares** *or a* **set of MOLS**.

The tables given in Example 1.1.6 form a mutually orthogonal set of Latin squares. To get a larger set, we look at order 4 Latin squares.

Example 1.1.8 *[8] The set consisting of the three Latin square given below is a set of MOLS.*

	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

	1	2	3	4
1	1	2	3	4
2	4	3	2	1
3	2	1	4	3
4	3	4	1	2

	1	2	3	4
1	1	2	3	4
2	3	4	1	2
3	4	3	2	1
4	2	1	4	3

More generally, a set of MOLS of order n can have at most $n-1$ elements. A closed formula for the exact number of MOLS of order n is not known however.

A perhaps more natural notion of equivalence for Latin squares is the following:

Definition 1.1.9 *[16] Two Latin squares are* **isotopic** *if each can be turned into the other by permuting the rows, columns, and symbols. This isotopy relation is an equivalence relation; the equivalence classes are the isotopy classes.*

A simple example of isotopic Latin squares is the following:

Example 1.1.10 *Since the Latin square labeled Q can be obtained from the one labeled P by swapping the second and third row, the two Latin square are isotopic.*

P	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

Q	1	2	3
1	1	2	3
2	3	1	2
3	2	3	1

Table 1.1: Tow Isotopic Latin squares of order 3.

1.1.2 Latin Squares and Groups

In the following we assume the reader is familiar with basic group theory as in [12]. For the sake of completeness we provide some of the fundamental definitions here; for these and others, we refer the reader to [12].

Definition 1.1.11 *A* **binary operation** $*$ *on a set G is a function $* : G \times G \to G$. For any $a, b \in G$ we shall write $a * b$ for $*(a, b)$. We say the operation $*$ is* **commutative** *if $a * b = b * a$ for all $a, b \in G$. We say that the operation is* **associative** *if $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.*

Definition 1.1.12 *A* **group** *is a set, G, together with a binary operation $\cdot$ satisfying the following axioms:*

(i) **Closure:** *For all g, h in G, $g \cdot h$ is also in G.*

(ii) **Associativity:** *For g, h and k in G, $(g \cdot h) \cdot k = g \cdot (h \cdot k)$.*

(iii) **Identity element:** *There exists a unique element e in G such that, for every element g in G, $e \cdot g = g \cdot e = g$.*

(iv) **Inverse element:** *For each g in G, there exists a unique element h in G, commonly denoted g^{-1} (or $-g$, if the operation is denoted "$+$"), such that $g \cdot h = h \cdot g = e$, where e is the identity element.*

If in addition, $g \cdot h = h \cdot g$ for all $g, h \in G$, we say G is an **abelian** *group.*

The set of integers under addition is an example of a group. Throughout this thesis, we will use $\mathbb{Z}$ and $\mathbb{Z}_n$ to respectively denote the groups of integers and integers modulo n under addition. We will also use S_n and D_{2n} respectively to denote the symmetric group of order $n!$ consisting of all permutations of n letters and the dihedral group of $2n$ elements which is the standard symmetry group of a regular n-gon.

Definition 1.1.13 *A* **subgroup** *H of a group G, denoted $H \leq G$, is a subset of a group that forms a group under the binary operation of the group.*

Definition 1.1.14 *Let S_n be the symmetric group on n letters. A subgroup G of S_n is called a* **permutation group**.

Definition 1.1.15 *Let G be a group and let $H \leq G$. For $g \in G$, the* **left** *and* **right cosets** *of H in G are respectively given by*

$$gH = \{gh \mid h \in H\} \qquad \text{and} \qquad Hg = \{hg \mid h \in H\}.$$

Definition 1.1.16 *[38] Let G be a group and let $H \leq G$. A set containing exactly one element from each left coset of H is called a* **left transversal**.

Replacing the word "left" with "right" gives the definition of a right transversal. We note that the word 'transversal' is more general than defined in 1.1.16. A subset that contains exactly one element from each member of a given collection is called transversal.

Example 1.1.17 *Here we list several examples of transversals for a range of finite groups.*

- *Let* $H = \{(0,0),(1,1)\} \leq \mathbb{Z}_2 \times \mathbb{Z}_2$*, then* $S = \{(0,0),(1,0)\}$ *is a left transversal of* H*.*
- *Let* $G = D_8$ *and* $K = \langle r \rangle$*, then* $T = \{1, s\}$ *is a left transversal of* K*.*
- *In the above, the subgroups* H *and* K *are both normal, which implies that* S *and* T *are both left and right transversal of* H *and* K *respectively.*
- *Now consider the subgroup* $H = \langle (12),(123) \rangle$ *of* S_4*. a left transversal of* H *is* $\{(1)$*,* (14)*,* (142)*,* $(243)\}$*. The set* $\{(1)$*,* (24)*,* (1423)*,* $(234)\}$*, on the other hand, is a right transversal of* H*, while* $\{(1),(14),(24)(34)\}$ *is both a left and a right transversal of* H*.*

It is well-known that groups can be represented using Latin squares. That is, the multiplication table of the binary operation $\cdot$ for any given group $(G, \cdot)$ is a Latin square. For example, one can see that the second and the fourth tables in Example 1.1.4 are respectively the multiplication tables of $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$. However, not all Latin squares describe groups. For example, the table given on the left in Example 1.1.2 is the multiplication table of a group (that is isomorphic to $\mathbb{Z}_3$), while the table on the right is not.

Thinking of Latin squares as multiplication tables of a more general algebraic structure leads us to quasigroups, which are the precise algebraic counterparts of Latin squares. A quasigroup can be thought of as an algebraic object that differs from a group in that associativity and identity axioms are not required. We define quasigroups more formally in Chapter 2; see Section 2.1.

Example 1.1.18 *As already mentioned, Latin squares represent different types of algebraic objects. For example, the Latin square to the left in Table 1.2 represents* $\mathbb{Z}_4$*, the one in the middle represents the Klein four-group, while the third represents a quasigroup that is not a group (compare with Table 2.2).*

Table 1.2: Three Latin Squares of Order 4

1	2	3	4
2	4	1	3
3	1	4	2
4	3	2	1

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

1	2	3	4
2	1	4	3
4	3	1	2
3	4	2	1

1.1.3 More Group Theory

This thesis focuses on group-theoretic approaches to the study of quasigroups. Before we move on, we include here a few more group-theoretic constructions that we will need. In the following, given a group G we will use the notation $\mathrm{Aut}(G)$ to denote the group of automorphisms of G. Once again, the standard reference for the definitions below is [12]; for definitions from other sources, we provide specific citations.

Definition 1.1.19 *A* **group action** *of a group G on a set S is a map from $G \times S$ to S (written as $g \cdot s$ for all $g \in G$ and $s \in S$) satisfying the properties:*

- $g_1 \cdot (g_2 \cdot s) = (g_1 g_2) \cdot s$, *for all* $g_1, g_2 \in G, s \in S$, *and*
- $1 \cdot s = s$ *for all* $s \in S$, *where* $1 \in G$ *is the identity of* G.

Definition 1.1.20 *Let G be a group acting on a nonempty set S.*

1. *The equivalence class $\{g \cdot s \mid g \in G\}$ is called the* **orbit** *of G containing s.*
2. *The action of G on S is called* **transitive** *if there is only one orbit. That is, for elements $a, b \in S$ there exists $g \in G$ such that $a = g \cdot b$. If there is at most one such g, we say the group action is* **semiregular**. *A group action is* **regular** *if there exists exactly one $g \in G$ that maps a to b.*

Definition 1.1.21 *[29] A group G is said to act* **semitransitively** *on a finite set S if all orbits are of size equal to $|S|$, the cardinality of S.*

An example of such a group action will show up in the discussion in Subsection 2.4.2.

Definition 1.1.22 *Let H and K be groups and let $\phi : K \to \mathrm{Aut}(H)$ be a group homomorphism. The* **semidirect product of H and K with respect to ϕ** *is the group $G = H \rtimes_\phi K$ which is the set $H \times K$ equipped with the operation*

$$(h_1, k_1)(h_2, k_2) = (h_1\phi(k_1)(h_2), k_1k_2) \tag{1.1.3}$$

If $\cdot$ denotes the left multiplication action determined by ϕ, (1.1.3) can be written as

$$(h_1, k_1)(h_2, k_2) = (h_1k_1 \cdot h_2, k_1k_2). \tag{1.1.4}$$

Definition 1.1.23 *Let G and H be groups with centers $Z(G)$ and $Z(H)$, respectively. Let $C \leq Z(G)$ and let $D \leq Z(H)$ such that $C \cong D$. An* **(external) central product of** *G and H with respect to ϕ is defined to be the quotient $(G \times H)/K$ where $K = \{(g, \phi(g)^{-1}) | g \in C\}$. The central product of G and H will be denoted by $G \circ H$.*

We may think of $G \circ H$ as the direct product of G and H "collapsed" by identifying each element $c \in C$ with corresponding element $d = \phi(c) \in D$.

Definition 1.1.24 *[14] Let G be a group and let $H, K \leq G$. We say that G is an* **internal central product** *of H and K if* **both** *the following conditions hold:*

1. *Every element of H commutes with every element of K, i.e., the subgroups centralize each other.*
2. *$G = HK$, i.e. G is the product of the two subgroups.*

In this case H and K are both central factors of G.

Definition 1.1.25 *[14] A group G is an internal central product of two subgroups H, K if (1) G is generated by H and K and (2) every element of H commutes with every element of K. Sometimes the stricter requirement that $H \cap K$ is exactly equal to the center is imposed, as in [25]. The subgroups H and K are then called central factors of G.*

Example 1.1.26 *[28] The Pauli group G_1 on 1 qubit is the 16-element matrix group consisting of the 2×2 identity matrix and all of the Pauli matrices*

$$G_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\} = \langle X, Y, Z \rangle$$

where

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

G_1 is isomorphic to the central product of $\mathbb{Z}_4$ and D_8, i.e. $G_1 \cong \mathbb{Z}_4 \circ D_8$.

The following defines a special kind of semidirect product group, the holomorph:

Definition 1.1.27 *Let H be a group and let $K = \mathrm{Aut}(H)$ with ϕ the identity map from K to $\mathrm{Aut}(H)$. Let $G = H \rtimes Aut(H)$ is called the* **holomorph** *of H and is denoted by $\mathrm{Hol}(H)$.*

Here is an example of the holomorph of $H = \mathbb{Z}_2 \times \mathbb{Z}_2$.

Example 1.1.28 *Let $H = \mathbb{Z}_2 \times \mathbb{Z}_2$. Then $\mathrm{Aut}(H) \cong S_3$, and so $G = H \rtimes \mathrm{Aut}(H) \cong S_4$. The calculations were carried out using GAP [1].*

Definition 1.1.29 *Let G be a group. The* **inner holomorph** *of G can be defined as the semidirect product $G \rtimes \mathrm{Inn}(G)$ where $\mathrm{Inn}(G)$ is the inner automorphism group with the usual action. It is a subgroup of the holomorph $G \rtimes \mathrm{Aut}(G)$ and is a quotient of the direct product $G \times G$.*

When G is a group with an automorphism whose restriction to the center is the inverse map, this is isomorphic to the central product of two copies of G with the center $Z(G)$ of both copies identified: $G *_{Z(G)} G$. If G is a group whose center is a direct factor, this group is isomorphic to the direct product of $G \times \mathrm{Inn}(G)$.

Definition 1.1.30 *Let G be a group and let $H \leq G$. Then H is a direct factor of G if one of the following equivalent conditions holds:*

[1] See Section A.3 to read about GAP.

1. *There is a subgroup $K \leq G$ such that $G = H \times K$.*

2. *H is normal and there is a normal subgroup $K \leq G$ such that $HK = G$ and $H \cap K$ is trivial.*

3. *There is a subgroup $K \leq G$ such that $K \leq C_G(H)$ (the centralizer of H in G), $HK = G$, and $H \cap K$ is trivial.*

4. *There is a collection of subgroups $H_i, i \in I$, with H equal to one of the H_i's such that G is the internal direct product of the H_i's.*

1.2 The Organization of This Thesis

As mentioned already, this thesis explores some algebraic properties of quasigroups. This chapter is introductory. In its first section we provide some prerequisite definitions and set our notational conventions (Section 1.1). In the last section we provide a brief overview of the history and applications of Latin squares and quasigroups and aim to motivate the work of this thesis (Section 1.3).

Chapter 2 formally introduces quasigroups as algebraic structures (Section 2.1) and develops the elements of quasigroup theory following the modern algebraic pathway: subobjects (Section 2.2), structure-preserving maps (Section 2.3), special subobjects (Section 2.4). Section 2.5 explores natural ways of building new quasigroups from older ones (e.g., via direct and semidirect products).

Chapter 3 formally introduces multiplication groups of quasigroups (Section 3.1), which allow us to use basic group theory to access more structural information about quasigroups. In particular, Section 3.2 explores the multiplication groups of quasigroups which are actually groups, with a view towards how things change in the broader context of quasigroups that are not necessarily groups. Section 3.3 looks into connections between certain standard operations on Latin squares and the corresponding changes in the multiplication groups of the associated quasigroups. Section 3.4 zeroes in on conjugate quasigroups and their

multiplication groups.

Chapter 4 explores loops and their multiplication groups. Loops are especially nice quasigroups; they have an identity-like element, which makes their theory closer to that of groups (see Definition 4.1.5 for a precise definition). Section 4.1 presents basic definitions and examples of loops and some of their generalizations. Section 4.2 lists, with examples, some of the known results about loops. Section 4.3 explores the properties of the multiplication groups of loops.

Finally Chapter 5 concludes this thesis with a recap, a list of the main results, and a look towards the future, describing possible research directions left open for further inquiry.

1.3 Why Care?

According to [50], "[t]he first known occurrences of latin squares seem to have been in their use on amulets and in rites in certain Arab and Indian communities from perhaps the year 1000: the nature of the sources makes the dating difficult. Most similar amulets contain not a latin square, but a magic square - an $n \times n$ array filled with the symbols $1, 2, \ldots, n^2$ for which the sum of the numbers in any row, column, or main diagonal is the same." See Figures 1.1-1.2.

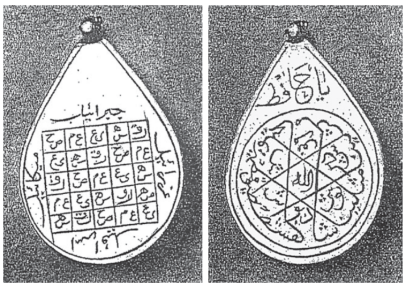

Figure 1.1: A silver amulet from Damascus. On one side is a Latin square, and on the other side are the names of the Seven Sleepers, who, according to legend, slept in a cave for two hundred years from about the year 250. [50]

Orthogonal Latin square first appeared formally in 1782 in the famous Graeco-Latin square conjecture made by Leonhard Euler. A Graeco-Latin square is defined as follows:

Figure 1.2: Latin squares of different orders using different symbols. [50]

Definition 1.3.1 *[10] An order n* **Graeco-Latin square** *is a square array of n rows and n columns of ordered pairs from a set of n symbols such that in each row and each column, each symbol appears exactly once in each coordinate, and each of the n^2 possible pairs appears exactly once in the entire square.*

See the table at the bottom of Example 1.1.6 for an example of a Graeco-Latin square. Such a square exists for any $n > 1$ except for $n = 2, 6$.

Latin squares have been used in various applications. For example, Latin squares have been implemented in coding theory and cryptography. Some of the applications in this field include error correcting, message authentication and data recovery. [33, 34, 37].

Latin squares found use also in experiment design. This use of Latin squares was pioneered by R. A. Fisher. He recommended Latin squares for agricultural crop experiments. At about the same time, Jerzy Neyman developed the same idea during his doctoral study at the University of Warsaw. For more on these types of applications see [22, 4].

As seen above, Latin squares have been of interest for a long time. As their algebraic counterparts, quasigroups are much newer on the mathematical scene. More generally, everywhere-defined and partially-defined binary algebraic operations have been studied since the nineteenth century. A groupoidal was the name Oystein Ore gave to everywhere-defined operation, which is why a set with an everywhere defined operation is called a groupoid (Definition 2.1.14). If the operation were partially defined, the resulting structure was called a halfgroupoid by Bruck. After Nicolas Bourbaki, groupoids were renameed magma. In [32], Pflugfelder presents a comprehensive history of the development of study of quasigroups and

loops. We highlight here some of the historical details about quasigroups.

Subtraction of natural numbers was the first used nonassociative operation, before the apperance of the nonassociative system known as Cayley numbers which are due to Arthur Cayley in 1845. In 1929, Anton K. Suschkewitsch, a Russian professor of mathematics, published his paper 'On a Generalization of the Associative Law' in which he noted that associativity is not used in the proof of Lagrange's theorem for groups. This was the reason behind the construction of the so called 'general groups' to give an early attempt toward modern loop theory. Those 'general groups' seems to be the start of modern quasigroups as isotopes of groups.

In the 1920s, Artin proved a theorem which was later used by Moufang in her famous paper on quasigroups. Quasigroups appeared, under a different name, as an algebraic structure with a left and right division, see for example [35], and [36]. Some important publications in quasigroups are 'Theory of Quasi-Groups' (1937) by Hausmann and Ore, 'Quasi-Groups Which Satisfy Certain Generalized Associative Laws' (1939) by Murdoch [30] and 'Quasi-Groups' (1940) by Garrison [13]. Then in 1943, Albert published two important papers which he titled 'Quasigroups. I' [2] and 'Quasigroups. II' [3].

Even though quasigroups are newcomers in the mathematical scene, they have found several applications already. As they are the algebraic counterpart of Latin squares, it makes sense that they would have related applications. Indeed quasigroup-based cryptographic symmetric structures theory uses quasigroups that are isotopic to groups [45]. In differential geometry, loops, more specifically Moufang loops (see Definition 4.2.9), can be associated to Malcev algebras in a way which generalizes the Lie correspondence between Lie groups and their tangent Lie algebras, see for example [9].

As groups are algebraic structures whose theory and structure have been well studied and well understood, they make a very useful tool in understanding and generalizing the theories of other algebraic structures. The tools of group theory may be used in understanding quasigroups and loops by looking at their multiplication groups, which are certain permutation

groups associated to quasigroups. It is well-known that the notion of multiplication group was first introduced by A. A. Albert in [2]. The importance of multiplication groups comes from the connections between the structure of a quasigroup and that of its multiplication group. For example, multiplication groups play an important role in the theory of normality of quasigroups and loops [38]. This thesis tries to use the connection between quasigroups and groups by investigating their multiplication groups and how certain constructions on a quasigroup carry over to its multiplication group.

We end this chapter with a short summary of the different types of algebraic structures so as to contextualize quasigroups in the broader algebraic world. Starting with a set, one defines a binary operation to equip the set with. Depending on the properties of the operation, the system will define one or more of the structures given in Figure 1.3.

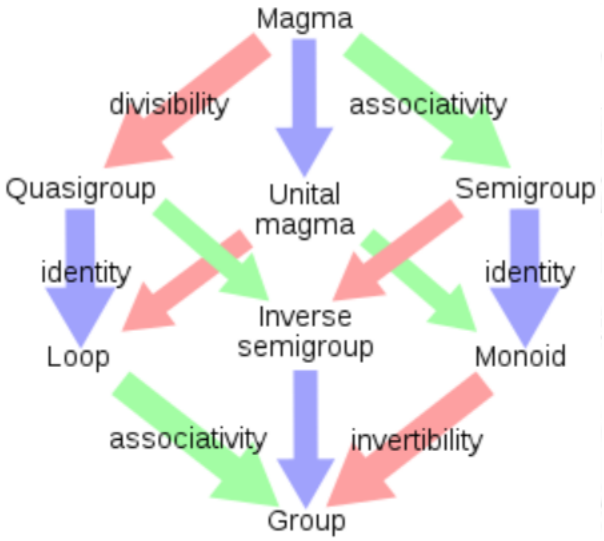

Figure 1.3: Different Algebraic Structures. The image is from the semigroup page.

Figure 1.3 shows the connections between different algebraic structures. This thesis focuses on quasigroups. Similar to many other mathematical concepts, certain terms are sometimes defined differently or, as in this case, slightly altered. In fact, [32] explains that before the term “loop" was introduced, quasigroups were assumed by some mathematicians to posses an identity, while others assumed a one-sided identity, and yet some others assumed no identity. In this thesis, we will adopt the convention that a quasigroup is nonempty and

need not have an identity element (see Definition 2.1.1).

In our context, a magma will be defined to be a set that is closed under the operation it is equipped with (see Definition 2.1.14). Then according to Figure 1.3, a magma with divisibility is a quasigroup, which becomes a loop with the addition of an identity element. If in addition associativity holds, we get a group.

In comparison, a magma with an identity is called a unital magma, which becomes a monoid if the operation is associative; with the further addition of invertibility we get a group. A unital magma becomes a loop if divisibility holds, and a unital associative magma with divisibility defined is again a group.

Likewise, an associative magma is called a semigroup. A semigroup with an identity is a monoid, which becomes a group when invertibility is added. A semigroup with invertibility is called an inverse semigroup, which is a group if a unital element exists.

Note that in Figure 1.3, if we begin with a magma and get a quasigroup by adding divisibility to it, we can then add associativity to get an inverse semigroup. It turns out, however, that in the case of a quasigroup, associativity immediately leads to the existence of an identity element (see Theorem 4.2.8). In other words, the path from quasigroups to inverse semigroups collapses and gives us groups immediately.

Chapter 2

Quasigroups

This chapter systematically describes and explores the algebraic theory of quasigroups. We follow the standard algebraic path of defining substructures, structure-preserving maps, and special substructures. In that spirit, we start by formally defining what a quasigroup is, following that with examples of quasigroups (Section 2.1). Among several other stand-alone examples, we introduce a family of quasigroups defined on the set of nth roots of unity which will appear repeatedly in the rest of the thesis. Next, in Section 2.2 we define subquasigroups. Then in Section 2.3 we study two different types of structure-preserving maps: homomorphisms and homotopies of quasigroups. We follow that with an exploration in Section 2.4 of some special types of subquasigroups, including normal and central subquasigroups (2.4.1), Lagrangean subquasigroups (Subsection 2.4.2), and Sylow subquasigroups (Subsection 2.4.3). We wrap up the chapter with Section 2.5, where we generalize a handful of natural group-theoretic constructions to the context of quasigroups (e.g., direct and semidirect products).

Throughout this chapter, one of our underlying motivations is to zero in on the similarities and the differences between groups and quasigroups.

2.1 Quasigroups: Basic Definitions and Examples

In this section, we give different ways to define a quasigroup, and provide several examples. We begin with:

Definition 2.1.1 *A* **quasigroup** $(Q, \star)$ *is a nonempty set,* Q*, with a binary operation,* $\star$*, whose multiplication table is a Latin square. That is, for each* $a, b \in Q$*, there exist unique elements* $x, y \in Q$ *such that both of the following hold*

$$a \star x = b, \qquad y \star a = b. \tag{2.1.1}$$

Some call these structures *combinatorial quasigroups*. Here is the way that term is defined:

Definition 2.1.2 (Combinatorial Quasigroup) *[42] The structure* $(Q, \cdot)$ *is a (two-sided) quasigroup if specification of any two of* x, y, z *in the equation*

$$x \cdot y = z \tag{2.1.2}$$

determines the third uniquely. In a left quasigroup, specification of x *and* z *in (2.1.2) determines* y *uniquely. It is a right quasigroup if its opposite is a left quasigroup.*[1]

As can be seen these are equivalent definitions. Yet another equivalent definition of a quasigroup is the following:

Definition 2.1.3 (Equational Quasigroup) *[42] A quasigroup* $(Q, \cdot, /, \backslash)$ *is a set* Q *with three binary operations of multiplication, right division* $/$*, and left division* $\backslash$*, satisfying*

$$(SL)\ x \cdot (x\backslash y) = y;\ \ (SR)\ y = (y/x) \cdot x;\ \ (IL)\ x\backslash(x \cdot y) = y;\ \ (IR)\ y = (y \cdot x)/x. \tag{2.1.4}$$

Q is a right-quasigroup if it satisfies (SR) and (IR), and it is a left-quasigroup if it satisfies (SL) and (IL).

[1] The opposite Q^{OP} of a quasigroup is the set Q taken with the operation:

$$Q \times Q \to Q; (x, y) \mapsto y \cdot x \tag{2.1.3}$$

Compare with the definition of the opposite algebra in [12].

In [40] it was shown that if $(Q, \cdot, /, \backslash)$ is an equational quasigroup, then $(Q, \cdot)$ is a combinatorial quasigroup. In the following we will use the term "quasigroup" to describe a structure that can be defined using any of these three equivalent alternatives (also see Definition 2.1.15).

We will soon show that a quasigroup that is associative is a group (Theorem 4.2.8). A quasigroup is called **commutative** if its operation is commutative. A quasigroup is **abelian** if it (or rather, the binary operation defined on it) is both associative and commutative.[1] Together with Theorem 4.2.8, this means that an abelian quasigroup is in fact an abelian group.[2]

The relations in Definition 2.1.1 always hold if Q is a group. Therefore, every group is a quasigroup.

Example 2.1.4 *Take for example $G = (\mathbb{Z}_n, +)$, the integers modulo n under addition. Picking $a, b \in G$ it can easily be verified that there exist $x, y \in G$ such that $a+x = b$ and $y+a = b$.*

More generally for g, h in a group G, we can always find x, y such that $gx = h$ and $yg = h$: just let $x = g^{-1}h$ and $y = hg^{-1}$. On the other hand, not every quasigroup is a group.

Example 2.1.5 *Let Q be the quasigroup whose multiplication table is given by the Latin square on the right in Example 1.1.18. Picking any $a, b \in Q$, we can find $x, y \in Q$ such that the conditions in Definition 2.1.1 are satisfied. However, associativity does not hold; since, for example, $(1 \star 4) \star 3 = 1$ while $1 \star (4 \star 3) = 2$. Thus, the quasigroup defined by this Latin square is not a group.*

---

[1] We should note that in [30], an abelian quasigroup is defined to be a quasigroup Q such that for all $a, b, c, d \in Q$ we have

$$(ab)(cd) = (ac)(bd). \tag{2.1.5}$$

The author claims that Condition (2.1.5) imposes a generalized commutativity law, and that quasigroups that satisfy (2.1.5) are direct generalizations of abelian groups [30]. See for example Section 2.4.3 and Theorem 2.3.7. In this thesis we will not use this definition but instead refer explicitly to Condition 2.1.5 when we need it.

[2] References such as [41] allow for empty quasigroups; in such a context, the only abelian quasigroup that is not a group would be the empty one.

Example 2.1.6 *Subtraction is a nonassociative binary operation which is why* $(\mathbb{Z}, -)$ *is not a group. However since given* $a, b \in \mathbb{Z}$*, we have* $a-(a-b) = b$ *and* $(b+a)-a = b$*, it follows that* $(\mathbb{Z}, -)$ *is a quasigroup. One can similarly verify that* $(\mathbb{Z}_n, -)$*, integers modulo* n*, is also a quasigroup.*

Note that both $(\mathbb{Z}, -)$ and $(\mathbb{Z}_n, -)$ are quasigroups with no identity. A quasigroup with an identity is called a **loop**; see Definition 4.1.5. Here is an example of a loop we will see again.

Example 2.1.7 *Let* L *be the quasigroup of order* 5 *whose multiplication table is given below:*

*	1	a	b	c	d
1	1	a	b	c	d
a	a	1	c	d	b
b	b	d	1	a	c
c	c	b	d	1	a
d	d	c	a	b	1

Note that the element 1 *here acts as a two-sided identity element. Note also that* L *is not a group because it is not associative.*

Next we consider a series of examples constructed from the nth roots of unity. We will later prove some results involving this family of quasigroups. We start with the third and fourth roots of unity.

Example 2.1.8 *Let* $Q_3 = \{1, \omega, \omega^2\}$ *with* $\omega = e^{2i\pi/3}$*. This is a quasigroup under the operation* $x \circ y = \bar{x}y$*, where* $\overline{x}$ *is the complex conjugate of* x*. The multiplication table under the operation* $\circ$ *is given in Table 2.1. (Note also that this table is the Latin square we saw as an example of a Latin square that does not come from a group in Example 1.1.2.)*

Table 2.1: Multiplication table of $Q_3 = \{1, \omega, \omega^2\}$

$\circ$	1	ω	ω^2
1	1	ω	ω^2
ω	ω^2	1	ω
ω^2	ω	ω^2	1

Example 2.1.9 *Let $Q_4 = \{-1, -i, 1, i\}$, comprised of the roots of the monic polynomial $x^4 - 1$. This is also a quasigroup under the operation $x \circ y = \bar{x}y$, where $\overline{x}$ is the complex conjugate of x. The multiplication table is Table 2.2*

Table 2.2: Multiplication table of $Q_4 = \{-1, -i, 1, i\}$

$\circ$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	$-i$	i	1	-1
$-i$	i	$-i$	-1	1

To generalize let us adopt the notation Q_n for the set whose elements are the n^{th} roots of unity, taken together with the operation $\circ$ defined by $x \circ y = \bar{x}y$. We now prove that $(Q_n, \circ)$ is a quasigroup for any given positive integer n.

Theorem 2.1.10 *Let $Q = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$ be the set comprised of the nth roots of unity. Then Q is a quasigroup under the operation $a \circ b = \bar{a}b$.*

Proof: Let $a, b \in Q$, we want to find x and y such that the conditions of Definition 2.1.1 hold. That is, we want to find $x, y \in Q$ such that $a \circ x = b$ and $y \circ a = b$ or equivalently $\bar{a}x = b$ and $\bar{y}a = b$. Since any element of Q is a power of ω, we let $a = \omega^k$ and $b = \omega^m$ for $k, m = 1, 2, \ldots, n-1$. Then $x = \omega^{k+m}$ and $y = \omega^{k-m}$ respectively satisfy the two equations. They are the unique such element and uniqueness follows from the fact that these are complex numbers. $\square$

We will be looking at the family Q_n of quasigroups several times throughout this dissertation. On that note, if we define $Q = (Q_n, *)$ where $*$ is defined for $a, b \in Q$ by $a * b = a\bar{b}$ then Q is also a quasigroup, Theorem 2.1.11.

Note the analogy between Example 2.1.4 and the Q_n defined here. Just like the additive group $\mathbb{Z}_n$ and its multiplicative counterpart made up of the nth roots of unity, the two sets of structures are isomorphic as quasigroups. We will be able to make this precise in Section 2.3 when we define the notion of a quasigroup isomorphisms and isotopies.

The following considers the nth roots of unity equipped with the operation $a * b = a\bar{b}$.

Theorem 2.1.11 *Let $Q = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$ be the set of nth roots of unity. Define $*$ on Q by $a * b = a\bar{b}$ for all $a, b \in Q$. Then Q is a quasigroup. Furthermore, the multiplication table of $(Q, *)$ is the transpose of that of $(Q, \circ)$ given in Theorem 2.1.10.*

Proof: Showing that $(Q, *)$ is a quasigroup follows by a similar argument of that in the proof of Theorem 2.1.10. Now, let $(Q, \cdot)$ be Q with the usual multiplication of complex numbers. Observe that the multiplication table of $(Q, \circ)$ can be obtained by relabeling the head-column of the multiplication table of $(Q, \cdot)$ with $\bar{a}$ instead of a, and that of $(Q, *)$ is obtained by replacing the head-row with $\bar{b}$ instead of b. Thus, since $(Q, \cdot)$ is a group, the two tables are the transpose of one another. □

Example 2.1.12 *Consider Q_4 and let the operations $\circ, *$ and $\cdot$ be as described in the proof of Theorem 2.1.11. Compare the multiplication table of $(Q, *)$, given below, with that of $(Q, \circ)$, given in Example 2.1.9.*

$*$	1	-1	i	$-i$
1	1	-1	$-i$	i
-1	-1	1	i	$-i$
i	i	$-i$	1	-1
$-i$	$-i$	i	-1	1

Constructing the quasigroups Q_n and $(Q, *)$ from Theorem 2.1.11 is done by twisting the operation in an existing group structure. Doing so results in losing some of the properties of the group operation. This idea, however, preserve some structure and defines a quasigroup. The following result gives a generalization of Theorems 2.1.10 and 2.1.11.

Theorem 2.1.13 *[27] Let $(G, \cdot)$ be a group and let $\phi, \psi \in \mathrm{Aut}(G)$. Define the binary operation $*$ for $g, h \in G$ by $g * h = \phi(g) \cdot \psi(h)$. Then $(G, *)$ is a quasigroup.*

We defined a quasigroup in terms of a set and a binary operation on it (Definition 2.1.1). A quasigroup Q can also be defined as an algebraic structure with certain conditions on the left and right multiplication operators, which are respectively defined, for $x, y \in Q$, by

$$L_x(y) = xy \quad \text{and} \quad R_x(y) = yx. \tag{2.1.6}$$

In order to present this perspective, we begin with the most general algebraic structure we will need:

Definition 2.1.14 *[7] A* **magma** *(or* **groupoid***), M, is a set equipped with a binary operation, $\star$ such that for $x, y \in M$ we have $x \star y \in M$.*

Then we can make the following definition:

Definition 2.1.15 *[49] A* **quasigroup** *Q is a magma in which the left and right multiplication operators L_q and R_q are bijective for all elements $q \in Q$. Further, the maps L_q^{-1} and R_q^{-1} are always defined, and given $p \in Q$, $L_q^{-1}(p) = q \backslash p$, left division, and $R_q^{-1}(p) = p/q$, right division.*

Remark 2.1.16 *In terms of the maps in (2.1.6) the four quasigroup identities from Definition 2.1.3 can be expressed as*

$$(SL)\ L_x L_x^{-1} = id; \quad (SR)\ R_x R_x^{-1} = id; \quad (IL)\ L_x^{-1} L_x = id; \quad (IR)\ R_x^{-1} R_x = id. \tag{2.1.7}$$

Example 2.1.17 *The tables below define two magmas. In the table to the right, the maps L_q and R_q for $q \in Q$ all bijective, and therefore Q is a quasigroup. On the other hand, this is not the case for the magma defined by the table to the left. Thus, P is not a quasigroup.*

P	0	1	2
0	0	0	0
1	0	1	2
2	0	2	0

Q	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Definition 2.1.15 describes a way to see that every Latin square defines a quasigroup, and every quasigroup has a Latin square as its multiplication table.

The idea of orthogonality of Latin squares (Definition 1.1.5) carries over to quasigroups. We may think of two quasigroups being orthogonal to one another if there multiplication tables are orthogonal Latin squares. A formal definition is the following:

Definition 2.1.18 *[22] Let Q be a finite set. We say that the two quasigroups $(Q, \cdot)$ and $(Q, *)$ are* **orthogonal** *if for any $a, b \in Q$, there exists unique $x, y \in Q$ such that*

$$x \cdot y = a, \quad x * y = b. \tag{2.1.8}$$

Starting with an abelian group Charles C. Linder proved the following result in [26].

Theorem 2.1.19 *If G is an abelian group of order n and p is the smallest prime divisor of n. Then there are $p-1$ mutually orthogonal quasigroups of order n, including G itself.*

We note that those possible quasigroup are the $(G, \circ_i)$ where $\circ_i$ is defined for $a, b \in G$ we have $a \circ_i b = a^i b$. One example of such a quasigroup is the family Q_n which, in Theorem 2.1.10, we showed are quasigroups.

2.2 Subquasigroups

Whenever talking about an algebraic object, it is natural to look into the subsets of the object that has the same structure (e.g. subgroups of groups, subspaces of vector spaces, etc). We follow the tradition and start by given a definition of subquasigroup.

Definition 2.2.1 *A* **subquasigroup** *of a quasigroup $(Q, \star)$ is a subset S of Q that is itself a quasigroup under the same binary operation $\star$. We say $(S, \star)$ is a subquasigroup of $(Q, \star)$.*

The following are some examples on subquasigroups.

Example 2.2.2 *Let $G = (\mathbb{Z}, +)$. Since G is a group, it is a quasigroup. and since $H = (2\mathbb{Z}, +)$ is a subgroup, H is a subquasigroup of G.*

More generally if Q is any group its subgroups are also subquasigroups. The converse also holds, with exception of the empty subquasigroup in the case a quasigroup is not define to be nonempty.

Theorem 2.2.3 *A subquasigroup H of a group G is a subgroup of G.*

Proof: Let $1 \in G$ denote the identity element of G. Since H is a subquasigroup, then for $h \in H$ there exists an element $k \in H$ such that $h \cdot k = h$, i.e. $1 \in H$. Similarly, there is an element $\ell \in H$ such that $h \cdot \ell = 1$, i.e. $\ell = h^{-1}$. Associativity is automatic, and the proof is complete. □

Example 2.2.4 *Consider the quasigroup $Q = (\mathbb{Z}, -)$ (Example 2.1.6), let $R = \{2n \mid n \in \mathbb{Z}\}$, then $(R, -)$ is a subquasigroup of Q.*

Next we explore the subquasigroup structure of the quasigroups Q_n that we defined earlier. We start with Q_3 and Q_4:

Example 2.2.5 *Let $\omega = e^{2\pi/3}$, and consider the quasigroup $Q_3 = \{1, \omega, \omega^2\}$ equipped with the operation $x \circ y = \bar{x}y$. The subquasigroups of Q_3 are $\{1\}$ and Q_3 itself.*

Example 2.2.6 *Now consider $Q_4 = \{1, -1, i, -i\}$ with $x \circ y = \bar{x}y$ for any $x, y \in Q_4$. It is easy to verify that $\{1\}$, $\{1, -1\}$ and Q_4 are the subquasigroups of Q_4.*

Now let's consider a bigger quasigroup, Q_{12}.

Example 2.2.7 (Constructing all subquasigroups of Q_{12}) *Denote $\omega = e^{2\pi i/12}$, and write $Q_{12} = \{1, \omega, \omega^2, \ldots, \omega^{11}\}$. One subquasigroup is $\{1\}$. If we let S_1 to be the subquasigroup that contains ω, then $1, \omega^2 \in S_1$ since $1 \circ \omega = \omega$ and $\omega \circ \omega^2 = \omega$. We can similarly show that $S_1 = Q_{12}$, i.e. ω generates Q_{12}. Likewise, if a subquasigroup contains ω^5, ω^7 or ω^{11}, then one can show that this subquasigroup is S_1. The other quasigroups can be obtained with similar calculations. The subquasigroups of Q_{12} are:*

$$\{1\}, \{1, \omega^6\}, \{1, \omega^4, \omega^8\}, \{1, \omega^3, \omega^6, \omega^9\}, \{1, \omega^2, \omega^4, \omega^6, \omega^8, \omega^{10}\}, \text{ and } Q_{12}.$$

The above examples of Q_3, Q_4 and Q_{12} can be generalized as follows:

Theorem 2.2.8 *Let Q_n be the quasigroup consisting of the nth roots of unity together with the binary operation $a \circ b = \bar{a}b$, for $a, b \in Q_n$. Then Q_n has exactly one subquasigroup with k elements for every k that divides n. Furthermore, these are all the subquasigroups of Q_n.*

Proof:

We first show that there exists a subquasigroup of order j where j divides n. Let j be a divisor of n, then we can write $n = kj$ for a positive integer $k \leq n$. The subquasigroup generated by ω^j is

$$\langle \omega^j \rangle = \{1, \omega^j, \omega^{2j}, \ldots, \omega^{(k-1)j}\}.$$

which is a subquasigroup of order k, and it is the smallest subquasigroup that contains ω^j. To show that this is the only subquasigroup k, a divisor of n ($n = kj$, for some positive integer j), consider an order k subquasigroup S of Q_n. Let d be the smallest positive integer such that $\omega^d \in S$, we will show that d divides n and $S = \langle \omega^d \rangle$.

Let $\omega^j \in S$, then by the division algorithm there are unique integers q and r such that $j = dq + r$ where $0 \leq r < d$. Write

$$\omega^j = \omega^{dq+r} = (\omega^d)^q \omega^r.$$

Since $\omega^d, \omega^j \in S$ and S is a subquasigroup, we have $\omega^r \in S$, but $0 \leq r < d$ and d is the smallest positive integer such that $\omega^d \in S$, i.e. $r = 0$ and d divides j. That is $S = \langle \omega^d \rangle$. Completing the proof. □

We recall that the left and right cosets of a subset P of a quasigroup Q are defined in the usual way. That is, $qP = \{qp \mid p \in P\}$ and $Pq = \{pq \mid p \in P\}$. The following are some properties of subquasigroups

Proposition 2.2.9 *[47] The following are elementary properties of a finite quasigroup Q.*

P1. If $P \subset Q$ and $q \in Q$ then P, qP and Pq have the same order.

P2. If $S \subset Q$ and for $a, b \in S$ there is a unique $c \in S$ such that $x * b = c$, then S is a subquasigroup.

P3. If S is subquasigroup of Q then $a \in S$ and $b \notin S$ imply $ab \notin S$.

Although the quasigroup family of Q_n seems to resemble groups in satisfying Lagrange's Theorem, it is not true in general that the order of a subquasigroup divides the order of the quasigroup. In fact, a quasigroup of prime order may have a proper subquasigroup and a quasigroup of composite order may have no proper subquasigroups [6]. That is, Lagrange Theorem for subgroups (the order of a subgroup divides the order of the group) is not always true for quasigroups. The following is an example of such a quasigroup.

Example 2.2.10 *[13] Let L be the quasigroup we defined in Example 2.1.7. That is L is the quasigroup whose multiplication table is given by the Latin square:*

*	1	a	b	c	d
1	1	a	b	c	d
a	a	1	c	d	b
b	b	d	1	a	c
c	c	b	d	1	a
d	d	c	a	b	1

The subset $P = \{1, a\}$ is a subquasigroup of order 2 which clearly does not divide 5, the order of L.

Even though we do not have an exact counterpart to Lagrange's Theorem, we can still say somethings about the orders of subquasigroups. The following gives an upper bound of the order of a subquasigroup of a quasigroup.

Theorem 2.2.11 *[47] Let Q be a quasigroup of order n and let P be a subquasigroup of order k. Then $2k \leq n$.*

Proof: For $q \in Q$, and $p \in P$, if $q \notin$ then $pq \in Q$, $pq \notin P$. This means $Pq \subset Q$, and $Pq \cap P = \emptyset$. Since by property one in Proposition 2.2.9 P and Pq are of the same order k, it follows that $2k \leq n$. □

For more results on the restriction of the order of subquasigroups of a given quasigroup, we refer the reader to [47].

2.3 Homomorphisms and Homotopies of Quasigroups

In this section, we present the basics about homotopy and homomorphisms. We first recall that a Latin square of order n is an $n \times n$ array filled with n letters in which each symbol appears exactly once per row and once per column, Definition 1.1.1.

Example 2.3.1 *Consider the quasigroup, Q, whose multiplication table is obtained by swapping the first and last row of the multiplication table of $\mathbb{Z}_5$. Then the two Latin squares are isotopic. However, Q is nonassociative. The reader can verify that $(1 \cdot 1) \cdot 2 \neq 1 \cdot (1 \cdot 2)$ in Q.*

Definition 2.3.2 *[40] Let Q and R be quasigroups, and define the maps f, g and h as*

$$(f, g, h) : (Q, \cdot, /, \backslash) \to (R, \cdot, /, \backslash)$$

between the quasigroups Q and R. The triple of maps defines a **homotopy** *if*

$$h(x \cdot y) = f(x) \cdot g(y) \tag{2.3.1}$$

for all $x, y \in Q$.

Example 2.3.3 *Let $(P, \cdot)$ and $(Q, *)$ respectively denote the quasigroups in Example 1.1.10. Let $g : P \to Q$ be defined by the permutation (23), and let $f : P \to Q$ and $h : P \to Q$ be the identity map. Then for $x, y \in P$ we have*

$$h(x \cdot y) = f(x) * g(y).$$

See Table 2.3

In case f, g and h in Definition 2.3.2 are the same map, we get the definition of quasigroup homomorphism which can be formally defined as follows:

Definition 2.3.4 *[40] Let Q and R be quasigroups. Define the map*

$$f : (Q, \cdot, /, \backslash) \to (R, \cdot, /, \backslash).$$

We say f is a quasigroup **homomorphism** *if*

$$f(x \cdot y) = f(x) \cdot f(y)$$

x	$g(x)$	$y = h(y)$	$g(x) * h(y)$	$x \cdot y = f(x \cdot y)$
1	1	1	1	1
1	1	2	2	2
1	1	3	3	3
2	3	1	2	2
2	3	2	3	3
2	3	3	1	1
3	2	1	3	3
3	2	2	1	1
3	2	3	2	2

Table 2.3: Calculations for Example 2.3.3

for all $x, y \in Q$. If f is also bijective, then f is a quasigroup **isomorphism**, *in which case we say Q and R are* **isomorphic** *and write $Q \cong R$.*

Every group isomorphism is a quasigroup isomorphism since groups are quasigroups.

Example 2.3.5 *Let P and Q be as in Example 1.1.10. The two quasigroups defined by theses Latin squares are isotopic but they are not isomorphic. Let R be the quasigroup defined by the table given below, then P and R are isomorphic. One isomorphism is to take $f, g, h : P \to R$ defined by the permutation* (123).

R	1	2	3
1	3	1	2
2	1	2	3
3	2	3	1

In this context, an isotopy may be defined as follows:

Definition 2.3.6 *[40] Let Q and R be quasigroups with the maps f, h and h defining a homotopy between them. If f, g, h are bijective, then the triple (f, g, h) is an* **isotopy** *and we say Q is* **isotopic** *to R and we write $Q \sim R$. Further, if $f = g = h$, then this is a quasigroup isomorphism.*

A quasigroup isotopy $(f, g, h) : Q \to Q$ in which h is the identity map is called a **principle isotopy** [40]. The concept of quasigroup isotopy first introduced in [2] by A. A. Albert [32].

Referring back to the discussion following Theorem 2.1.10, we can now show that $(\mathbb{Z}_n, +)$ and $(Q_n, \circ)$ are isotopic. Define the isotopy (f, g, f) from $\mathbb{Z}_n$ to Q_n by $f(x) = \omega^x$ and $g(x) = \overline{\omega^x}$ for $x \in \mathbb{Z}_n$. Then for $x, y \in \mathbb{Z}_n$, we have

$$f(x + y) = g(x) \circ f(y).$$

The following is a result that involves abelian quasigroups according to the definition given by Murdoch, that is, quasigroups that satisfy (2.1.5).

Theorem 2.3.7 *[11] Let $(Q, \cdot)$ be a quasigroup satisfying (2.1.5). Then for every element $q \in Q$ there exists a principle isotope (Q, ϕ_p) of $(Q, \cdot)$ which is an abelian group with p as the identity element in (Q, ϕ_p). Moreover, for any $p, q \in Q$ the groups (G, ϕ_p) and (G, ϕ_q) are isomorphic.*

2.4 Special Subquasigroups

In the following we will need Definition 2.5.7 and:

Definition 2.4.1 *[40] Let Q be a quasigroup. Then a* **congruence** *on Q is an equivalence relation on Q that is a subquasigroup of $Q \times Q$ (when considered as a subset of $Q \times Q$).*

Definition 2.4.2 *Let $f : Q \to R$ be a quasigroup homomorphism, then the kernel of f, denoted* $\ker f$*, is defined by*

$$(x, y) \in \ker f \iff f(x) = f(y). \tag{2.4.1}$$

The kernel of a quasigroup homomorphism $f : Q \to R$ forms a subquasigroup of $Q \times Q$. Further it is a **congruence** relation on Q. Conversely, given a congruence relation V on a quasigroup Q, the natural projection

$$\Pi_V : Q \to Q^V, \quad \text{defined by } q \mapsto q^V$$

which sends $q \in Q$ to its equivalence class

$$q^V = \{p \in Q \mid (q, p) \in V\}$$

in the set of all equivalence classes, is a quasigroup homomorphism. Let's look at the following example.

Example 2.4.3 *Let $\phi : S_3 \to S_3$ be the group homomorphism that maps* (123) *to* (132) *and* (12) *to* (13)*. Then as a quasigroup homomorphism*

$$\ker \phi = \{(x, y) \in S_3 \times S_3 \mid \phi(x) = \phi(y)\}.$$

Since ϕ is bijective, the kernel of the quasigroup homomorphism is

$$\ker \phi = \{(x, x) \mid x \in S_3\} \cong S_3.$$

2.4.1 Normal and Central Subquasigroups

We can now define what a normal subquasigroup is:

Definition 2.4.4 *[40] A subquasigroup P of a quasigroup Q is said to be* **normal**, *written $P \trianglelefteq Q$, if there is a congruence V on Q having P as a single congruence class.*

We define the diagonal quasigroup of a quasigroup Q by

$$\hat{Q} = \{(q, q) \mid q \in Q\} \tag{2.4.2}$$

A group G is abelian if and only if the diagonal group $\hat{G}$ is a normal subgroup of $G \times G$. Certainly, if G is abelian, then so is $G \times G$ whence each subgroup of $G \times G$ is normal. Conversely, if $\hat{G} \triangleleft G \times G$ then for all $g, h \in G$, we have

$$(g, h)^{-1}(g, g)(g, h) = (g, h^{-1}gh) \in \hat{G} \tag{2.4.3}$$

so that $g = h^{-1}gh$ [40].

Definition 2.4.5 *[43] A quasigroup is called* **central** *if the diagonal subquasigroup $\hat{Q}$ is a normal subquasigroup of $Q \times Q$, i.e., if there is a congruence on $Q \times Q$ with $\hat{Q}$ as a congruence class.*

Central quasigroups are the quasigroup analogues of abelian groups. The map $f : Q \to Q'$ is a quasigroup homomorphism if it preserves all three quasigroup operations. An equivalence relation V on a quasigroup Q is a congruence if it is a subquasigroup of $Q \times Q$.

Definition 2.4.6 *A quasigroup Q is said to be* **simple** *if its only congruence relations are the equality relation and the universal relation $Q \times Q$.*

The following will come in handy in Chapter 4.

Theorem 2.4.7 *[43] Let Q' and Q be central quasigroups. Define the multiplication in Q' by $x \cdot y = xa' + yb' + 0^2$, and the multiplication in Q by $x \cdot y = xa + yb + 0^2$. Let $f : (Q', +) \to (Q, +)$ be an abelian quasigroup homomorphism. Let m_1, m_2 and m_3 be elements of Q such that $m_3 = m_1 \cdot m_2 - f(0^2)$. Define the maps $f_1, f_2, f_3 : Q' \to Q$ for all $x, y, z \in Q'$*

$$(f_1(x), f_2(y), f_3(z)) = (f(xa')a^{-1}, f(yb')b^{-1}, f(z)) + (m_1, m_2, m_3). \tag{2.4.4}$$

Then $(f_1, f_2, f_3) : Q' \to Q$ is a homotopy.

Proof: Let $x, y \in Q'$. Then

$$\begin{aligned} f_1(x) \cdot f_2(y) &= f_1(x)a + f_2(y)b + 0^2 \\ &= (f(xa')a^{-1} + m_1)a + (f(yb')b^{-1} + m_2)b + 0^2 \\ &= f(xa') + f(yb') + m_1a + m_2b + 0^2 \\ &= f(xa' + yb' + 0^2) - f(0^2) + m_1 \cdot m_2 \\ &= f(x \cdot y) + m_3 \\ &= f_3(x \cdot y). \end{aligned}$$

Completing the proof. □

In the rest of this section, we will need to use certain terms and constructions involving multiplication groups. Though these structures will be formally reintroduced and explored in details in the following chapters of this thesis, we find it important to list the formal definitions here in order to allow us to introduce certain important classes of subquasigroups.

Definition 2.4.8 *We call the group generated by left and right multiplications by elements of Q the* **multiplication group** *of Q, we'll denote it by* $\mathrm{Mul}(Q)$. *We can write* $\mathrm{Mul}(Q) = \langle R_q, L_q \mid q \in Q \rangle$ *where R_q and L_q are the right and left multiplication by $q \in Q$, respectively.*

The group generated by R_q, right multiplications maps, is called the **right multiplication group** of Q, and similarly, the group generated by L_q is the **left multiplication group** of Q. We will respectively denote these two groups by $\mathrm{RMul}(Q)$ and $\mathrm{LMul}(Q)$. The left and right multiplication groups of a quasigroup need not be isomorphic. However, it is possible for a quasigroup to have isomorphic left and right multiplication groups.

Definition 2.4.9 *Let Q be a quasigroup and let P be a subquasigroup of Q. The groups $\mathrm{LMul}_Q(P) = \langle L_p \mid p \in P\rangle, \mathrm{RMul}_Q(P) = \langle R_p \mid p \in P\rangle$ and $\mathrm{Mul}_Q(P) = \langle L_p, R_p \mid p \in P\rangle$ respectively define the* **relative left, relative right and relative multiplication** *groups of P in Q.*

Now we are ready to talk about Lagrangean subquasigroups.

2.4.2 Lagrangean subquasigroups

We start this section by defining right and left Lagrangean subquasigroups.

Definition 2.4.10 *[42] The subquasigroup P is said to be right Lagrangean in the left quasigroup Q if $\mathrm{LMul}_Q(P)$ acts semitransitively (Definition 1.1.21) on Q. Similarly, We say P is a left Lagrangean in the right quasigroup Q if P is right Lagrangean in Q^{OP}. We say P is a Lagrangean subquasigroup if it is both right and left Lagrangean.*

In the group case, $\mathrm{LMul}_Q(P)$ always acts semitransitively on Q, in the sense that each orbit has size $|P|$. That is, if Q is a group, then the set of orbits of $\mathrm{LMul}_Q(P)$ on Q is $\{Px \mid x \in Q\}$, the set of cosests of P [42]. Let's first consider an example of a quasigroup that is a group.

Example 2.4.11 *Let $Q = \mathbb{Z}_4$, and take $P = \{1, a^2\}$ the relative left multiplication group is $\mathrm{LMul}_Q(P) = \langle L_{a^2}\rangle$. The orbits of the action of P on Q are $\{1, a^2\}$ and $\{a, a^3\}$, which are the cosets of P. In fact, Lagrange's Theorem implies that each subgroup of a finite group is right Lagrangean.*

We now consider the infinite quasigroup $(\mathbb{Z}, -)$.

Example 2.4.12 *Take the $Q = (\mathbb{Z}, -)$ and let $P = (2\mathbb{Z}, -)$ be the subquasigroup of even integers under subtraction. Then $\mathrm{LMul}_Q(P)$ contains all the left multiplication maps by even integers and so the only orbit of the action is Q.*

Now, let's consider the family of quasigroup Q_n starting with Q_3.

Example 2.4.13 *Let $Q = Q_3 = \{1, \omega, \omega^2\}$ equipped with the operation $a \circ b = \bar{a}b$. The only subquasigroups are $P = \{1\}$ and Q itself. The action of $\mathrm{LMul}_Q(P)$ on Q has the singletons as its orbits. The action of $\mathrm{LMul}(Q)$ on Q has a single orbit, namely Q itself.*

Next, we consider Q_4

Example 2.4.14 *Consider $Q = Q_4 = \{\pm 1, \pm i\}$ with the same operation in Example 2.4.13. Let $P = \{\pm 1\}$. Then $\mathrm{Mul}_Q(P) = \{L_1, L_{-1}\}$ and the orbits of the action of $\mathrm{LMul}_Q(P)$ on Q are $\{\pm 1\}$ and $\{\pm i\}$, both of which has order 2. Also, as in the case of Q_3, if $P = \{1\}$, the orbits are the singletons and in case $P = Q$, the only orbit is Q. Thus all subquasigroups of Q_4 are right Lagrangean.*

Now, we consider the quasigroup $Q = (Q_{12}, \circ)$, with $\circ$ is again as in the above two examples.

Example 2.4.15 *Let $Q = (Q_{12}, \circ)$, and denote the proper subquasigroups of Q by S_i where i is refers to the order of that subquasigroup. As in the case of Q_4, the subquasigroups S_1 and Q are both right Lagrangean. For $S_2 = \{1, \omega^6\}$, the relative left multiplication group is $\mathrm{LMul}_Q(S_2) = \langle L_{\omega^6} \rangle$. The orbits of the action of L_2 on Q are $\{1, \omega\}$, $\{\omega, \omega^7\}$, $\{\omega^2, \omega^8\}$, $\{\omega^3, \omega^9\}$, $\{\omega^4, \omega^{10}\}$, and $\{\omega^5, \omega^{11}\}$. Thus, S_2 is right Lagrangean. Similar calculations shows that all subquasigroups of Q are right Lagrangean.*

This leads us to the following:

Theorem 2.4.16 *Let $Q = (Q_n, \circ)$ where for $a, b \in Q_n$, we have $a \circ b = \bar{a}b$. Then, the subquasigroups of Q are all right Lagrangean.*

Proof: Let $P = S_k$ be the order k subquasigroup of Q and let $L = \mathrm{LMul}_Q(P)$. Let ω^d be a generator of P, i.e. $P = \langle \omega^d \rangle = \{1, w^d, \ldots, \omega^{(k-1)d}\}$, then $L = \langle L_{\omega^d} \rangle$. Consider the action of L on Q, and denote the orbit of $q \in Q$ by $\mathcal{O}_q$. The orbits of which are then

$$\mathcal{O}_1 = P, \quad \mathcal{O}_\omega = \{\omega, \omega^{1-d}, \ldots, \omega^{1-(k-1)d}\}, \quad \ldots, \quad \mathcal{O}_{\omega^{n-1}} = \{\omega^{n-1}, \omega^{n-(d+1)}, \ldots, \omega^{(n-1)-(k-1)d}\}.$$

Each of which are of order k, i.e. $\mathrm{LMul}_Q(P)$ acts semitransitively on Q, and therefore P is right Lagrangean. □

Similar calculations as those used in proving Theorem 2.4.16 will yield that the subquasigroups of Q_n are also left Lagrangean, and therefore are Lagrangean subquasigroups in Q_n. We also note, as can be seen in the proof of Theorem 2.4.16 we see that Q_n acts in a group-like way in the sense that the orbits of the action of $\mathrm{LMul}_Q(P)$ are precisely the right cosets of P.

Corollary 2.4.17 *Let $Q = (Q_n, \circ)$ where for $a, b \in Q_n$, we have $a \circ b = \bar{a}b$. Then the subquasigroups of Q_n are left Lagrangean, and therefore Lagrangean in Q.*

Proof: Let Q^{OP} be the opposite quasigroup of Q. That is, the set Q equipped with the operation $*$ where for $a, b \in Q$, we have $a * b = b \circ a = \bar{b}a$. It follows by Theorems 2.1.11 and 2.4.16 that each subquasigroup of Q is left Lagrangean in Q. Consequently, the subquasigroups of Q are Lagrangean in Q. □

Definition 2.4.18 *[42] Let Q be a quasigroup, and let r be a natural number with $r \leq |Q|$. Consider the action of $\mathrm{LMul}(Q)$ on the set of all size r subsets, $\mathcal{P}_r(Q)$. An orbit of this action is called* **overlapping** *if it contains non-disjoint pairs of elements. Otherwise, it is a* **nonoverlapping** *orbit.*

For finite quasigroups, the above described action will have nonoverlapping orbits if $r \mid |Q|$. If G is a group then every subgroup H of G lies in a nonoverlapping orbit, and each nonoverlapping orbit contains a subgroup. [42]

Example 2.4.19 *Let Q be the quasigroup whose multiplication table is the Latin square given in Example 2.2.10. The left multiplication group is then* $\mathrm{LMul}(Q) = \{L_1, L_a, L_b, L_c, L_d\}$. *Calculating the orbits of the action of* $\mathrm{LMul}(Q)$ *on* $\mathcal{P}_2(Q)$, *we see that the orbit containing the subset* $\{1, a\}$ *is* $\{\{1, a\}, \{b, c\}, \{b, d\}, \{c, d\}\}$ *which clearly contains overlapping sets.*

Here are some more results involving related ideas

Corollary 2.4.20 *[42] Let Q be a finite commutative quasigroup. Let P be a subquasigroup of Q that is not normal. Then P lies in an overlapping orbits.*

Proof: Let the orbit that contains P be denoted by $O_P = \{L_q \cdot S \mid L_q \in \mathrm{LMul}(Q)\}$. That means for $q \in Q$, the subset $qP \in O_p$. Thus, if $p \in P$, then pP and P have at least one element in common, namely p^2. □

Corollary 2.4.21 *[42] Let P be a subquasigroup of a finite commutative quasigroup Q. Then P lies in a nonoverlapping orbit if and only if it is a normal subquasigroup of Q.*

2.4.3 Sylow Subquasigroups

Next, we consider another type of subquasigroups, which are the Sylow subquasigroups.

Definition 2.4.22 *[42] Let Q be a finite left quasigroup, and let p be a prime number. A subset P of Q is said to be a (left) Sylow p-subquasigroup of Q if*

(a) P is a subquasigroup of Q;

(b) $|P|$ is a power of p;

(c) $|P\backslash Q|$ is coprime to p;

(d) $|P| \cdot |P\backslash Q| = |Q|$.

Example 2.4.23 *[42] If Q is a group, and $P \neq \emptyset$, then P is a Sylow p-subgroup if and only if P is a Sylow p-subquasigroup.*

Proposition 2.4.24 *[42] Let Q be a quasigroup of order $p^r \cdot m$, for a prime number p, comprime with m. Let P be a subquasigroup of order p^r. The following are equivalent:*

(a) P is a Sylow p-subquasigroup of Q;

(b) $|Q\backslash P| = |Q|/|P|$;

(c) P is right Lagrangean in Q.

With this proposition and Theorem 2.4.16 in mind, let's consider the following example.

Example 2.4.25 *Let $Q = Q_{12}$ equipped with the operation defined for $a, b \in Q_{12}$ by $a \circ b = \bar{a}b$. Theorem 2.4.16 shows that all subquasigroups of Q are right Lagrangean. Thus, it follows by Proposition 2.4.24 that $P = \{1, \omega^3, \omega^6, \omega^9\}$ is a Sylow 2-subquasigroup.*

This leads to the following consequence of Theorem 2.4.16

Corollary 2.4.26 *Let Q be as in Theorem 2.4.16. If $n = p^k \cdot m$ for a prime p coprime with m, then Q contains a Sylow p-subquasigroup.*

Proof: This follows from the facts that Q has a subquasigroup of order k for every divisor k of n, and the fact that these subquasigroups are right Lagrangean. □

We wrap up this section with the following definition and facts from [42].

Definition 2.4.27 *Let d be a positive integer, and let Q be a quasigroup whose order is a multiple of d. Consider the action of $\mathrm{LMul}(Q)$ on $\mathcal{P}_d(Q)$ the set of size d subsets of Q. For the quasigroup Q, the integer d has one of the following types:*

- **Type** *J if at least one overlapping orbit exists.*
- **Type** *I if the action has at least one nonoverlapping orbit that contains a subquasigroup of Q.*
- **Type** *H if the action has nonoverlapping orbits, each of which contains a subquasigroup of Q.*

- **Type** G *if it has type* H*, and if each subquasigroup in a nonoverlapping orbit is (right) Lagrangean.*

Proposition 2.4.28 *Suppose that* Q *is a finite quasigroup of order* dm*, and that* d *has type* G *for* Q*. Then in the action of* $\mathrm{LMul}(Q)$ *on the set of size* r *subsets of* Q*,* $\mathcal{P}_r(Q)$*, each nonoverlapping orbit contains a unique subquasigroup of* Q*.*

Corollary 2.4.29 *Suppose that a finite quasigroup* Q *has more than one singleton subquasigroup. Then none of those singleton subquasigroups is Lagrangean.*

Proposition 2.4.30 *Let* Q *be a quasigroup of order* $p^r \cdot m$*, for a prime* p *comprime with* m*. Suppose that the divisor* p^r *of* $|Q|$ *has type* G *in the classification of Definition 2.4.27.*

2.5 Other Constructions on Quasigroups

Group theory offers us a wide range of ways to construct new groups from old. In this section we consider possible quasigroup counterparts of these constructions.

2.5.1 Conjagacy Classes of Quasigroups

The importance of Conjugacy classes of groups is evident in understanding the structure of groups, specially nonabelian ones. So it only make sense to ask what will that look like for general quasigroups. We start with the definition of conjugacy classes of quasigroups is:

Definition 2.5.1 *[21] The multiplication group* G *of* Q *has a* **diagonal action** $\hat{G}$ *on* $Q \times Q$*, namely* $\hat{g} : Q \times Q \to Q \times Q$*;* $(x, y) \mapsto (xg, yg)$ *for each* g *in* G*. The orbits under this action are called the* **(quasigroup) conjugacy classes** *of* Q*.*

Example 2.5.2 *Let* $Q = Q_4 = \{1, -1, i, -i\}$ *whose multiplication group is the dihedral group* $G = D_8$ *(see Section 3.1.2). Studying the action as described in the above definition on* $Q \times Q$*, the quasigroup conjugacy classes are* $C_1 = \{(1, 1), (-1, -1), (i, i), (-i, -i)\}$*,* $C_2 =$

$\{(1,i),(i.-1),(-1,-i),(-i,1),(-1,i),(-i,-1),(1,-i),(i,1)\}$, *and* $C_3 = \{(1,-1),(i,-i),$ $(-1,1),(-i,i)\}$. *Notice that the conjugacy classes* C_1, C_2, C_3 *are the relations of equality, diametrical opposition, and adjacency on the unit circle respectively.*

Example 2.5.3 *In* Q_3*, the conjugacy classes are* $C_1 = \{(1,1),(\omega,\omega),(\omega^2,\omega^2)\}$*, and* $C_2 = \{(1,\omega),\ (\omega,\omega^2),(\omega^2,1),(1,\omega^2),(\omega,1),(\omega^2,\omega)\}$*, where* $\omega = e^{2i\pi/3}$.

Similarly, one can calculate the conjugacy classes of Q_n (the quasigroup consisting of the nth roots of unity) or any other quasigroup.

Example 2.5.4 *The conjugacy classes of* Q_5 *are* $C_1 = \{(g,g) \mid g \in Q_5\}$*,* $C_2 = \{(g,h) \mid g,h$ *are adjacent on the unit circle*$\}$ *and* $C_3 = \{(g,h) \mid g,h$ *are one apart the unit circle*$\}$ *in which* $|C_1| = 5$*,* $|C_2| = |C_3| = 10$.

For Q_7*, the conjugacy classes are* C_1, C_2 *and* C_3 *are as in the case for* $Q5$*, but with 7, 14 and 14 elements respectively. In addition,* $C_4 = \{(g,h) \ : \ g,h$ *are two apart on the unit circle*$\}$*, with* $|C_4| = 14$.

In the case of Q_8*, the classes* C_1, C_2, C_3 *and* C_4 *can be describe in similar terms as in the cases for* Q_5 *and* Q_7*. The sizes of these classes are 8 for* C_1 *and 16 for each of the other three. Additionally,* C_5 *is the diametrical opposition on the unit circle, and it has 8 elements.*

In the next example, we compare the quasi conjugacy classes with of $(Q_5, \circ)$ to the quasi conjugacy classes of the cyclic group $\mathbb{Z}_5$:

Example 2.5.5 *Let* $Q = (Q_5, \circ)$ *with the operation* $a \circ b = \bar{a}b$ *for* $a, b \in Q$*. As shown in Example 2.5.4, the quasigroup has three quasi conjugacy classes.*

On the other hand, there five quasi conjugacy classes of $\mathbb{Z}_5$ *which are* $C_1 = \{(1,1),\ldots,(5,5)\}$*,* $C_2 = \{(0,1),(1,2),\ldots,(4,0)\}$*,* $C_3 = \{(0,2),(1,3),\ldots,(5,0)\}$*,* $C_4 = \{(0,3),\ldots(4,2)\}$*, and* $C_5 = \{(0,4),\ldots,(4,3)\}$.

So far, we have played with the quasigroups Q_n and abelian groups. In the following example we consider $Q = S_3$. To simplify the notation, we will write $(1, 123)$ for $((1),(123))$.

Example 2.5.6 *Considering $Q = S_3$, the multiplication group (Section 3.1.2) is $G = S_3 \times S_3$, and the action is on $Q \times Q$, i.e. in this case, it is $S_3 \times S_3$ as well.There is no geometry to help describe the three quasi conjugacy classes for S_3 in this case. The first of which is the trivial one C_1 which contains the elements of the form (g, g) where $g \in S_3$. The second is the following*

$$C_2 = \{(1, 123), (12, 13), (13, 23), (23, 12), (123, 132), (132, 1),$$
$$(12, 23), (1, 132), (132, 123), (123, 1), (23, 13), (13, 12)\}.$$

The other 18 elements are in the third class.

2.5.2 Direct and Semidirect Products of Quasigroups

The direct product is a standard algebraic construction that allows one to create larger and more complex structures from smaller, simpler ones. It would be natural to ask if one can talk about such a construction in the context of quasigroups. Here is the definition we want:

Definition 2.5.7 *[41] Let Q and R be quasigroups. The* **direct product** *of Q and R is the set $Q \times R$ equipped with componentwise multiplication and divisions.*

Unlike in the case of groups, the direct product $Q \times R$ need not have subquasigroups isomorphic to Q or R [6, 30].

Given my background in semidirect product of groups, it was always of interest to me to find the generalization of the notion of semidirect product to quasigroups. There is not much done in that direction, but a semidirect product is defined as:

Definition 2.5.8 *[38, 18] A quasigroup Q is called the semidirect product of two quasigroups R and S, if there is a (quasigroup) homomorphism $\phi : Q \to S$ such that $\ker(\phi) = R$, and that when restricting ϕ to S, we have $\phi|_S$ is the identity function on S. Q is then denoted by $R \rtimes S$.*

The family of quasigroups Q_n shares a lot of similarities with cyclic groups $\mathbb{Z}_n$, and one thing that we would like to know is: Can Q_n be defined as the direct or semidirect product of Q_m and Q_k where $n = mk$?

To create a list of possible questions to pursue in the near future, we formulate the above formally as:

Question 2.5.9 *For integers n, m, k such that $n = mk$, and m and k are coprime is it true that $Q_n \cong Q_m \times Q_k$? If not, can we say that $Q_n \cong Q_m \rtimes Q_k$?*

Now, let $(G, \cdot)$ be a group and let $\phi, \psi \in \mathrm{Aut}(G)$. Theorem 2.1.13 ensures that $Q = (G, *)$ where $g * h = \phi(g) \cdot \psi(h)$ for all $g, h \in G$ is a quasigroup. A question to pose here:

Question 2.5.10 *What properties will be shared by the quasigroup $Q = (G, *)$ and the original group $(G, \cdot)$?*

Chapter 3

Multiplication Groups

We have already defined the multiplication group of a quasigroup in Section 2.4.1 when talking about certain special subquasigroups of a given quasigroup. In this chapter, we study multiplication groups in their own right. We begin with the basic definitions and examples (Section 3.1). Next we explore the implications of these definitions for quasigroups which are actually groups and see how things change when we move to the broader context of quasigroups that are not necessarily groups (Section 3.2). Then we explore connections between certain standard operations on Latin squares and the corresponding changes in the multiplication groups of the associated quasigroups (Section 3.3) and finally we look more specifically into the connections between the multiplication groups of conjugate quasigroups (Section 3.4).

Multiplication groups provide a way to connect a quasigroup to its multiplication group structurally. It might be easier to understand a quasigroup by studying its multiplication group. [38].

3.1 Preliminaries

We start by recalling the definition of the multiplication groups and the relative multiplication groups of a given quadigroup.

Definition (2.4.8) *We call the group generated by left and right multiplications by elements of Q the* **multiplication group** *of Q, we'll denote it by $\mathrm{Mul}(Q)$. We can write $\mathrm{Mul}(Q) = \langle R_q, L_q \mid q \in Q \rangle$ where R_q and L_q denote the right and left multiplication by $q \in Q$, respectively.*

The group generated by the right multiplication maps R_q is called the **right multiplication group** of Q, and similarly, the group generated by L_q is the **left multiplication group** of Q. We will respectively denote these two groups by $\mathrm{RMul}(Q)$ and $\mathrm{LMul}(Q)$. Although the left and right multiplication groups of a quasigroup might be isomorphic, this is not true in general.

Example 3.1.1 *The multiplication group, right multiplication group and left multiplication group of $\mathbb{Z}_n$ are all isomorphic to $\mathbb{Z}_n$.*

Definition (2.4.9) *Let Q be a quasigroup and let P be a nonempty subquasigroup of Q. The groups $\mathrm{LMul}_Q(P) = \langle L_p \mid p \in P \rangle$, $\mathrm{RMul}_Q(P) = \langle R_p \mid p \in P \rangle$ and $\mathrm{Mul}_Q(P) = \langle L_p, R_p \mid p \in P \rangle$ respectively define the* **relative left, relative right and relative multiplication** *groups of P in Q.*

We can also define the **relative multiplication group**, **relative left multiplication group** and **relative right multiplication group** by a single element $q \in Q$ in the same way.

Example 3.1.2 *Let $G = S_3$. The multiplication group of G is $S_3 \times S_3$, while the right multiplication and left multiplication groups of G are both isomorphic to G itself.*

Note that although $\mathrm{Mul}(G) \cong \mathrm{RMul}(G) \times \mathrm{LMul}(G)$ for $G = S_3$, this is not true in general. In Example 3.1.1, $\mathrm{RMul}(\mathbb{Z}_n) \times \mathrm{LMul}(G) \cong \mathbb{Z}_n \times \mathbb{Z}_n$, which is clearly not isomorphic to $\mathbb{Z}_n$.

Example 3.1.3 *Let $Q = (\mathbb{Z}_4, -)$, the set of integers modulo 4 under subtraction. The relative left multiplication group by the element $1 \in Q$ is $L_Q(1) = \langle L_1 \rangle \cong \mathbb{Z}_2$.*

Example 3.1.4 *Let $G = K_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$. Since G is abelian,* $\mathrm{LMul}(G) \cong \mathrm{RMul}(G) \cong G$ *(Theorem 3.2.1), but $G \times G$ is a group of order* 16 *which is definitely not isomorphic to* $G \cong \mathrm{Mul}(G)$.

Example 3.1.5 *As we have already seen, the integers under subtraction is a quasigroup. Its multiplication group is generated by the maps $L_a(x) = a - x$ and $R_a(x) = x - a$. The order of L_a is two as $L_a(L_a(x)) = a - (a - x) = x$, for integers a and x. On the other hand, R_a has infinite order as $R_a^n(x) = x - na$ for integers a, n and x.*

Before starting our discussion on multiplication groups of quasigroups, we recall the following useful tool.

Theorem 3.1.6 *Let G be a group generated by the elements g and h with $g^n = 1$ for $n \geq 3$, $h^2 = 1$ and $hgh^{-1} = g^{-1}$. Then there is a surjective homomorphism $\phi : D_{2n} \to G$. Furthermore, if $|G| = 2n$, then ϕ is also injective.*

Proof: The facts $g^n = 1$ and $h^2 = 1$ respectively imply $|g|$ divides n and $|h|$ is either 1 or 2. Since G is generated by g and h, we may right

$$\begin{aligned} G &= \langle g, h \mid g^n = h^2 = 1, hgh^{-1} = g^{-1} \rangle \\ &= \{1, g, \ldots, g^{n-1}, h, hg, hg^{n-1}\} \end{aligned}$$

Let $\phi : D_{2n} \to G$ be defined by $\phi(s^i r^j) = h^i g^j$. To see that ϕ is a well defined map, write $s^i r^j = s^{i+2k} r^{j+n\ell}$ for integers i, j, k and ℓ. Then

$$\phi(s^{i+2k} r^{j+n\ell}) = h^{i+2k} g^{j+n\ell} = (h^2)^k h^i (g^n)^\ell g^j = h^i g^j = \phi(s^i r^j).$$

Next, let $x, y \in D_{2n}$. For integers i, j, k and ℓ we can write $x = s^i r^j$ and $y = s^k r^\ell$. Computing

$$\begin{aligned} \phi(xy) = \phi(s^i r^j s^k r^\ell) = \phi(s^{i+k} r^{\ell - j}) = h^{i+k} g^{\ell - j} = h^i h^k g^{-j} g^\ell \\ = h^i g^j h^k g^\ell = \phi(s^i r^j)\phi(s^k r^\ell) = \phi(x)\phi(y), \end{aligned}$$

showing that ϕ is a homomorphism. It is clear that this map is surjective. Further, if $|G| = 2n = |D_{2n}|$ and ϕ is surjective, then ϕ is also injective. $\square$

We note that if $g^n = 1, h^2 = 1$ and $hgh^{-1} = g^{-1}$ are assumed to be the only relations, that will be enough to conclude that $G \cong D_{2n}$ without the need of the condition on the map ϕ.

Before looking at some of the known results about quasigroups, we note the following easy to observe facts:

Theorem 3.1.7 *Let Q be a quasigroup. Then*

1. *If Q is a commutative quasigroup, then* $\mathrm{LMul}(Q) = \mathrm{Mul}(Q)$.

2. *If Q is not commutative, then M is a nonabelian group*

Proving (a) is straightforward, since $L_q = R_q$ for any $q \in Q$. This implies $\mathrm{LMul}(Q) = \mathrm{Mul}(Q) = \mathrm{RMul}(Q)$. For (b) since Q is not commutative, there is at least one element q such that for $p \in Q$, we have $pq \neq qp$. This implies that in the multiplication group $L_q L_p \neq L_p L_q$. We add, even if a quasigroup is commutative, this does not automatically mean that the multiplication group will be abelian. The multiplication group of a quasigroup is abelian if the quasigroup is abelian, in which case the quasigroup is an abelian group. See Theorem 4.2.8.

Example 3.1.8 *The multiplication group of the commutative quasigroup whose multiplication table is given below is isomorphic to S_4.*

$*$	1	2	3	4
1	4	1	2	3
2	1	4	3	2
3	2	3	1	4
4	3	2	4	1

3.1.1 Some Known Results About Multiplication Groups of Quasigroups

We end this section with results from [19] describing what kind of groups are isomorphic to the multiplication group of a quasigroup. Recall that as mentioned in Chapter 1, a loop is

a quasigroup with an idenitty element.

Theorem 3.1.9 *Let Q be a quasigroup of order q and let $M = \mathrm{Mul}(Q)$. If $|M| = m$, then $q|m$ and $m|(q!)$. Also $q = m$ if and only if Q is an abelian group.*

This theorem gives lower and upper bounds on the order of the multiplication group of a quasigroup. For example, if $|Q| = q$, then the multiplication group will be at least of that order, or of order that is divisible by q but no more than $q!$. Based on this, If Q has order 4, then its multiplication group is of order $4, 8, 12$ or 24.

Theorem 3.1.10 *A permutation group G is isomorphic to the multiplication group of a quasigroup if and only if there is a loop $(Q, +)$ and there are permutations L and R of Q such that $G = \langle \mathrm{Mul}(Q, +), R, L\rangle$ on Q. In this case $G = \mathrm{Mul}(Q, \cdot)$ for the quasigroup operation $\cdot$ on Q defined by*

$$x \cdot y = R(x) + L(y).$$

If we take for example $Q = (\mathbb{Z}_4, -)$ which has multiplication group isomorphic to D_8. Let $P = (\mathbb{Z}_4, +)$ which is a group (i.e. a loop) with multiplication group isomorphic to $(\mathbb{Z}_4, +)$. Then choosing $L = (14)(23)$ and $R = (1)$ we get $G = \langle \mathrm{Mul}(Q, +), L, R\rangle \cong D_8 \cong \mathrm{Mul}(Q)$. The operation in this case is $x \cdot y = x + L(y)$ which is equivalent to subtraction on $\mathbb{Z}_4$.

Corollary 3.1.11 *A permutation group G is isomorphic to the multiplication group of a quasigroup $(Q, \cdot)$ if and only if there is a binary operation $+$ on Q such that $(Q, +)$ is a loop and there are permutations L and R such that $G = \langle \mathrm{LMul}(Q, +), R, L\rangle$ on Q. In this case $G = \mathrm{Mul}(Q, \cdot)$ for the quasigroup operation $\cdot$ on Q defined by*

$$x \cdot y = R(x) + L(y).$$

Back to the example following 3.1.10, since $(\mathbb{Z}_4, +)$ is an abelian group and $\mathrm{LMul}(\mathbb{Z}_4, +) = \mathrm{Mul}(\mathbb{Z}_4, +)$, it follows by Corollary 3.1.11 $G = \langle \mathrm{LMul}(Q, +), R, L\rangle \cong D_8$ for the same choice of L and R.

Corollary 3.1.12 *A permutation group G is isomorphic to the multiplication group of a finite quasigroup Q if there are permutations R, L and C such that C cyclically permutes all elements of Q. In this case $G = \langle R, L, C \rangle$.*

Let's consider $(\mathbb{Z}_4, -)$, one more time. Let $C = (1234)$, $L = (1)$ and $R = (12)(34)$, Corollary 3.1.12 ensures $G = \langle (1234), (12)(34) \rangle \cong D_8$.

The following gives a list of possible multiplication groups of quasigroups.

Theorem 3.1.13 *All finite dihedral, symmetric, alternating, general linear, projective general linear groups and all the Mathieu-groups M_{11} and M_{23} are isomorphic to multiplication groups of quasigroups.*

3.1.2 Constructing the Multiplication Group of the Quasigroup Consisting of nth Roots of Unity

In this section, we'll consider in some details the multiplication groups of the family of quasigroups Q_n. We start by illustrating the construction of the multiplication group of Q_3, Q_4 and Q_5. Then we show that the multiplication group of Q_n is the dihedral group of order $2n$.

We start by looking at Q_3, which is by definition

$$\mathrm{Mul}(Q_3) = \langle R_q, L_q \mid q \in Q \rangle = \{R_1, L_1, R_\omega, L_\omega, R_{\omega^2}, L_{\omega^2}\}.$$

The six maps are defined for $x \in Q_3$, are as follow:

$$L_1(x) = 1 \circ x = \bar{1}x = x \qquad R_1(x) = x \circ 1 = \bar{x}1 = \bar{x}$$

$$L_\omega(x) = \omega \circ x = \bar{\omega}x = \omega^2 x \qquad R_\omega(x) = x \circ \omega = \bar{x}\omega = \omega\bar{x}$$

$$L_{\omega^2} = \omega^2 \circ x = \bar{\omega^2}x = \omega x \qquad R_{\omega^2}(x) = x \circ \omega^2 = \omega^2\bar{x}$$

Note: Since ω and x are complex numbers, $\omega x = x\omega$.

Then the multiplication table for the group $\mathrm{Mul}(Q_3)$ is shown in Table 3.1. One can check that L_ω and R_ω generate $\mathrm{Mul}(Q_3)$, L_ω has order 3 and R_ω is an element of order 2.

Further, it is straightforward to verify

$$L_\omega \circ R_\omega = R_\omega \circ L_\omega^{-1}.$$

Table 3.1: Multiplication table of $\mathrm{Mul}(Q_3)$

$\circ$	L_1	L_ω	L_{ω^2}	R_1	R_ω	R_{ω^2}
L_1	L_1	L_ω	L_{ω^2}	R_1	R_ω	R_{ω^2}
L_ω	L_ω	L_{ω^2}	L_1	R_{ω^2}	R_1	R_ω
L_{ω^2}	L_{ω^2}	L_1	L_ω	R_ω	R_{ω^2}	R_1
R_1	R_1	R_ω	R_{ω^2}	L_1	L_ω	L_{ω^2}
R_ω	R_ω	R_{ω^2}	R_1	L_{ω^2}	L_1	L_ω
R_{ω^2}	R_{ω^2}	R_1	R_ω	L_ω	L_{ω^2}	L_1

Finally, since the order of $\mathrm{Mul}(Q_3)$ is 6, Theorem 3.1.6 ensures

$$\mathrm{Mul}(Q_3) \cong D_6.$$

Similarly, the group $G = \mathrm{Mul}(Q_4)$ has 8 elements, which are defined for $x \in Q_4$ as follows:

$$L_1(x) = x \qquad R_1(x) = \bar{x}$$

$$L_{-1}(x) = -x \qquad R_{-1}(x) = -\bar{x}$$

$$L_i(x) = -ix \qquad R_i(x) = i\bar{x}$$

$$L_{-i}(x) = ix \qquad R_{-i}(x) = -i\bar{x}.$$

The multiplication table of the group $\mathrm{Mul}(Q_4)$ is given in Table 3.2 below. A simple calculation shows that i generates Q_4 and therefore L_i and R_i generate of Q_4 such that:

$$L_i \circ R_i = R_i \circ L_i^{-1}$$

Since $|L_i| = 4$, $|R_i| = 2$ and $\mathrm{Mul}(Q_4)$ has 8 element, we conclude

$$\mathrm{Mul}(Q_4) \cong D_8.$$

The multiplication table of Q_5 is the Latin square given in Table 3.3. It can be shown in the same way that

$$\mathrm{Mul}(Q_5) \cong D_{10}.$$

Now we are ready to prove the following:

Table 3.2: Multiplication table of $\mathrm{Mul}(Q_4)$

$\circ$	L_1	L_{-1}	L_i	L_{-i}	R_1	R_{-1}	R_i	R_{-i}
L_1	L_1	L_{-1}	L_i	L_{-i}	R_1	R_{-1}	R_i	R_{-i}
L_{-1}	L_{-1}	L_1	L_{-i}	L_i	R_{-1}	R_1	R_{-i}	R_i
L_i	L_i	L_{-i}	L_{-1}	L_1	R_{-i}	R_i	R_1	R_{-1}
L_{-i}	L_{-i}	L_i	L_1	L_{-1}	R_i	R_{-i}	R_{-1}	R_1
R_1	R_1	R_{-1}	R_i	R_{-i}	L_1	L_{-1}	L_i	L_{-i}
R_{-1}	R_{-1}	R_1	R_{-i}	R_i	L_{-1}	L_1	L_{-i}	L_i
R_i	R_i	R_{-i}	R_{-1}	R_1	L_{-i}	L_i	L_1	L_{-1}
R_{-i}	R_{-i}	R_i	R_1	R_{-1}	L_i	L_{-i}	L_{-1}	L_1

Table 3.3: Multiplication table of $\mathrm{Mul}(Q_5)$

$\circ$	L_1	L_ω	L_{ω^2}	L_{ω^3}	L_{ω^4}	R_1	R_ω	R_{ω^2}	R_{ω^3}	R_{ω^4}
L_1	L_1	L_ω	L_{ω^2}	L_{ω^3}	L_{ω^4}	R_1	R_ω	R_{ω^2}	R_{ω^3}	R_{ω^4}
L_ω	L_ω	L_{ω^2}	L_{ω^3}	L_{ω^4}	L_1	R_{ω^4}	R_1	R_ω	R_{ω^2}	R_{ω^3}
L_{ω^2}	L_{ω^2}	L_{ω^3}	L_{ω^4}	L_1	L_ω	R_{ω^3}	R_{ω^4}	R_1	R_ω	R_{ω^2}
L_{ω^3}	L_{ω^3}	L_{ω^4}	L_1	L_ω	L_{ω^2}	R_{ω^2}	R_{ω^3}	R_{ω^4}	R_1	R_ω
L_{ω^4}	L_{ω^4}	L_1	L_ω	L_{ω^2}	L_{ω^3}	R_ω	R_{ω^2}	R_{ω^3}	R_{ω^4}	R_1
R_1	R_1	R_ω	R_{ω^2}	R_{ω^3}	R_{ω^4}	L_1	L_ω	L_{ω^2}	L_{ω^3}	L_{ω^4}
R_ω	R_ω	R_{ω^2}	R_{ω^3}	R_{ω^4}	R_1	L_{ω^4}	L_1	L_ω	L_{ω^2}	L_{ω^3}
R_{ω^2}	R_{ω^2}	R_{ω^3}	R_{ω^4}	R_1	R_ω	L_{ω^3}	L_{ω^4}	L_1	L_ω	L_{ω^2}
R_{ω^3}	R_{ω^3}	R_{ω^4}	R_1	R_ω	R_{ω^2}	L_{ω^2}	L_{ω^3}	L_{ω^4}	L_1	L_ω
R_{ω^4}	R_{ω^4}	R_1	R_ω	R_{ω^2}	R_{ω^3}	L_ω	L_{ω^2}	L_{ω^3}	L_{ω^4}	L_1

Theorem 3.1.14 *Let $Q_n = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$ equipped with the operation $\circ$ defined for $a, b \in Q_n$ by $a \circ b = \bar{a}b$. Let $\mathrm{Mul}(Q_n)$ be the multiplication group of Q_n, then*

$$\mathrm{Mul}(Q_n) \cong D_{2n}.$$

Proof: Let L_1 denote the identity element of $\mathrm{Mul}(Q_n)$. Following the same idea explained in the discussion above, we compute

$$R_\omega(R_\omega(x)) = R_\omega(\omega\bar{x}) = \omega\bar{x} \circ \omega = \bar{\omega}\bar{\bar{x}}\omega = x = L_1(x)$$

which shows that $|R_\omega| = 2$. Also, for $1 \leq k \leq n$ calculate

$$L_\omega^k(x) = \omega^{kn-k}x,$$

and the smallest k such $L_\omega^k = L_1$ is n implying $|L_\omega| = n$. Next, for $x \in Q_n$ we have

$$\begin{aligned}(L_\omega \circ R_\omega)(x) &= L_\omega(R_\omega(x)) = L_\omega(\omega\bar{x}) = \bar{\omega}(\omega\bar{x}) \\ &= (\bar{\omega}\bar{x})\omega = R_\omega(\omega x) = R_\omega(L_{\bar{\omega}}(x)) = (R_\omega \circ L_\omega^{-1})(x).\end{aligned}$$

That is $L_\omega \circ R_\omega = R_\omega \circ L_\omega$. Finally since L_ω and R_ω generate $\mathrm{Mul}(Q_n)$, we conclude by Theorem 3.1.6

$$\mathrm{Mul}(Q_n) \cong D_{2n}.$$

□

At the end of this section we pose the following two questions:

Question 3.1.15 *What other quasigroups have D_{2n} as their multiplication group? What can be said about this class of quasigroups?*

The more general question below is likely to be a much harder problem:

Question 3.1.16 *Given a group G, what are all the quasigroups having the group G as their multiplication group?*

3.2 Multiplication Groups of Quasigroups that are also Groups

In trying to get more understanding of the relation between a quasigroup and its multiplication group, we start by exploring the this relation in the case of quasigroups that are groups. For instance, Q_n has D_{2n} as its multiplication group. What will be the multiplication group of the multiplication group of Q_n? Let's start by stating the following well-known result:

Proposition 3.2.1 *Let G be an abelian group and $\mathcal{M} = \mathrm{Mul}(G)$. Then $G \cong \mathcal{M}$.*

Proof: Since G is abelian, $L_g = R_g$ for any g. We can define a map $\phi : G \to \mathcal{M}$ by $\phi(g) = L_g$ for any $g \in G$, which is an isomorphism. □

As we'll see later on, some quasigroups might have isomorphic multiplication groups while the quasigroups are not isomorphic. This is not the case for groups.

Theorem 3.2.2 *Let G and H be group. Let* $\mathrm{LMul}(G)$ *and* $\mathrm{LMul}(H)$ *be their left multiplication groups, respectively. Suppose* $\mathrm{LMul}(G) \cong \mathrm{LMul}(H)$*, then* $G \cong H$*.*

Proof: Let L^G denote the left multiplication maps by elements of G and let e_H denotes the identity element of H. Let $f : \mathrm{LMul}(G) \to \mathrm{LMul}(H)$ be a group isomorphism. Define $\phi : G \to H$ by

$$\phi(g) = f(L_g^G)(e_H)$$

If $g_1 = g_2$, then clearly $L_{g_1}^G = L_{g_2}^G$ and therefore $\phi(g_1) = \phi(g_2)$. Hence ϕ is well-define.

Let $g_1, g_2 \in G$, and calculate

$$\begin{aligned}\phi(g_1 g_2) &= f(L_{g_1 g_2}^G)(e_H) = f(L_{g_1}^G L_{g_2}^G) = f(L_{g_1}^G) f(L_{g_2}^G) \\ &= f(L^G(g_1))(e_H)\ f(L^G(g_2))(e_H) = \phi(g_1)\phi(g_2),\end{aligned}$$

showing that ϕ is a group homomorphism. Now suppose that $\phi(g_1) = \phi(g_2)$, then $f(L_{g_1}^G) = f(L_{g_2}^G)$. Since f is one-to-one, it follows that $g_1 = g_2$ and, consequently, ϕ is injective. If G and H are assumed to be finite, the proof is done. Otherwise, for $h \in H$, let L_h^H denote the left multiplication translation in H. Since f is surjective, for $g \in G$ there exists $h \in H$ such that $f(L_g^G) = L_h^H$. Thus,

$$\phi(g) = f(L_g^G)(e_H) = L_h^H(e_H),$$

showing that ϕ is also surjective and therefore $G \cong H$. □

We now prove analogues result for right multiplication groups.

Theorem 3.2.3 *Let G and H be two groups. Let* $\mathrm{RMul}(G)$ *and* $\mathrm{RMul}(H)$ *be their right multiplication groups, respectively. Suppose* $\mathrm{RMul}(G) \cong \mathrm{RMul}(H)$*, then* $G \cong H$*.*

Proof: Denote the right multiplication by elements of G by R^G and let e_H be the identity H. Let $f : \mathrm{RMul}(G) \to \mathrm{RMul}(H)$ be a group isomorphism and define $\phi : G \to H$ by

$$\phi(g) = f(R_{g^{-1}}^G)(e_H).$$

Since $g_1 = g_2$, it follows $f(R^G_{g_1^{-1}}) = f(R^G_{g_2^{-1}})$ which in turns means $R^G_{g_1^{-1}} = R^G_{g_2^{-1}}$ in $\mathrm{RMul}(G)$. Now, let $g_1, g_2 \in G$, then

$$f(R^G_{(g_1g_2)^{-1}}) = f(R^G_{g_2^{-1}g_1^{-1}}) = f(R^G_{g_1^{-1}}R^G_{g_2^{-1}}) = f(R^G_{g_1^{-1}})f(R^G_{g_2^{-1}})$$

when acting on e_H we have $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$, showing that ϕ is a homomorphism. Next, suppose that $\phi(g_1) = \phi(g_2)$, then

$$f(R^G_{g_1^{-1}})(e_H) = f(R^G_{g_2^{-1}})(e_H) \quad \Rightarrow f(R^G_{g_1^{-1}}) = f(R^G_{g_2^{-1}})$$

But f is one-to-one, and so $R^G_{g_1^{-1}} = R^G_{g_2^{-1}}$, and thus $g_1 = g_2$, and hence ϕ is also one-to-one. Since f is surjective, it follows that ϕ is also surjective, completing the proof. □

The above two theorems are not true for general quasigroups. Here is an example

Example 3.2.4 *The left multiplication groups of the two quasigroups $Q = \mathbb{Z}_3$ and P defined respectively by the below given Latin squares are both isomorphic to $\mathbb{Z}_3$. However, the two quasigroups are not isomorphic.*

Q	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

P	1	2	3
1	1	2	3
2	3	1	2
3	2	1	3

An interesting observation about the multiplication groups of finitely generated groups is the ability to study them through the generators and relations in the original group. Looking from this prospective, we can see that the multiplication groups of such groups are also finitely generated. We illustrate with the following examples:

Example 3.2.5 *The cyclic group $G = (\mathbb{Z}_n, +)$ is generated by the element $1 \in G$. The multiplication group of G will be generated by L_1. Since G is abelian Theorem 3.2.1 guarantees* $\mathrm{Mul}(G) \cong G$.

Example 3.2.6 *Consider the group $G = D_6$. Calculating the multiplication group of G starting with the generators and relations in G, a GAP calculation shows that* $\mathrm{Mul}(D_6) \cong D_6 \times D_6$. *See A.6.1.*

Next, let $G = S_4$ which can be represented

$$G = \langle g, h \mid g^2 = h^4 = (gh)^3 = (1) \rangle, \tag{3.2.1}$$

where $g = (12)$ and $h = (1234)$. The multiplication group turns out to be isomorphic to $S_4 \times S_4$.

From the above two examples, we observe that the multiplication group of a finitely-generated group is generated by left and right multiplication maps by the generators. We formulate this in the following theorem.

Theorem 3.2.7 *Let G be a finitely generated group with generators $g_1, g_2, \ldots, g_k$. The multiplication group of G is generated by L_{g_i}, R_{g_i} for $i = 1, 2, \ldots, k$, where L_{g_i} and R_{g_i} respectively denote the left and right multiplications by the element g_i.*

Proof: Let G be a finitely generated group. Then for any element $h \in G$, we can write

$$h = g_1^{\alpha_1} g_2^{\alpha_2} \ldots g_k^{\alpha_k} \tag{3.2.2}$$

The left and right multiplication by h evaluated at an element $x \in G$ are given by

$$L_h(x) = L_{g_1^{\alpha_1} g_2^{\alpha_2} \ldots g_k^{\alpha_k}} = g_1^{\alpha_1} g_2^{\alpha_2} \ldots g_k^{\alpha_k} x = (L_{g_1} \circ L_{g_2} \circ \cdots \circ L_{g_k})(x) \tag{3.2.3}$$

$$R_h(x) = R_{g_1^{\alpha_1} g_2^{\alpha_2} \ldots g_k^{\alpha_k}}(x) = x g_1^{\alpha_1} g_2^{\alpha_2} \ldots g_k^{\alpha_k} = (R_{g_k} \circ R_{g_{k-1}} \circ \cdots \circ R_{g_1})(x) \tag{3.2.4}$$

This implies any $L_, R_h \in \mathrm{Mul}(G)$ can be expressed in terms of the generators L_{g_i}, and R_{g_i}, for $i = 1, 2, \ldots, k$. Thus $\langle L_{g_i}, R_{g_i} \rangle = \mathrm{Mul}(G)$. □

As a consequence of the above theorem, the relations between the generators of G will yield relations in terms of the generators of $\mathrm{Mul}(G)$.

Corollary 3.2.8 *The relations between the generators of a finitely generated group G will be translated to relations in the generators of* $\mathrm{Mul}(G)$.

Proof: This follows directly from Theorem 3.2.7. □

To prove the next results about the multiplication group of dihedral groups, recall that the multiplication group of $D_6 \cong S_3$ is $D_6 \times D_6$ (Example 3.1.2). Let's also look at the

following example and observe the similarities and differences in the multiplication groups of dihedral groups.

Example 3.2.9 *The multiplication group of $G = D_{10}$ is generated by L_s, L_r, R_s, and R_r. These generators satisfy the relations:*

$$L_s^2 = L_r^5 = R_s^2 = R_r^5 = L_1, L_r L_s = L_s L_r^{-1}, R_r R_s = R_s R_r^{-1}.$$

In addition to those, right multipliaction and right multiplication by elements of D_{10} commutes. Therefore, the multiplication group of D_{10} is $D_{10} \times D_{10}$.

Comparing the above to the case of $G = D_8$ (Example 3.2.12), we see that the multiplication group of a dihedral group is not always isomorphic to its direct product. However, this is true for any D_{2n} for an odd integer $n \geq 3$. We'll later give a formula for all dihedral groups. Before we present the theorem, we make the following remark.

Remark 3.2.10 *In terms of its generators, $G = D_{2n} \times D_{2n}$ can be represented as:*

$$\langle s_1, r_1, s_1, s_2 \mid r_i^n = s_i^2 = e, r_i s_i = s_i r_i^{-1}, r_i r_j = r_j r_i, s_i r_j = r_j s_i, s_i s_j = s_j s_i \rangle \tag{3.2.5}$$

where $r_1 = (r, 1)$, $r_2 = (1, r)$, $s_1 = (s, 1)$, $s_2 = (1, s)$, $i \neq j$, and $e = (1, 1)$ is the identity element in G.

Theorem 3.2.11 *Let $n \geq 3$ be an odd integer. The multiplication group of $G = D_{2n}$ is $M = D_{2n} \times D_{2n}$.*

Proof: Write $G = D_{2n} = \langle r, s | r^n = s^2 = 1, rs = sr^{-1} \rangle$. We first begin by noting that $\mathrm{Mul}(G)$ has four generators, namely L_r, R_r, L_s, R_s. Now observe that L_r and R_r are both of order n whereas L_s and R_s are order two elements. Since G is a group, associativity implies

$$L_r R_r = L_r R_r, \quad L_r R_s = R_s L_r, \quad L_s R_r = R_r L_s, \quad L_s R_s = R_s L_s.$$

Finally, since $rs = sr^{-1}$ in G it follows that

$$L_r L_s = L_s L_r^{-1}, \quad R_r R_s = R_r^{-1} R_s.$$

These are the same relations as in Remark 3.2.10, therefore $\mathrm{Mul}(G) \cong D_{2n} \times D_{2n}$. □

In case n is even, the group $G = D_{2n}$ has a nontrivial center which results in having some "repetition" in the relations and generators of its multiplication group. Namely, since $r^{n/2} \in Z(G)$, we have $R_{r^{n/2}} = L_{r^{n/2}}$. As a result, the multiplication group will be quotiented out by a copy of $Z(G)$, the center of G.

Example 3.2.12 *$G = D_8$ has a nontrivial center, $Z(G) = \{1, r^2\}$. The relations among the generators of the multiplication group $M = \mathrm{Mul}(G)$ are almost the same as in the case of D_6 with the exception of the central relation $R_{r^2} = L_{r^2}$, or equivalently $R_r^2 = L_r^2$. The multiplication group of D_8 turns out to be isomorphic to its inner holomorph, $\mathrm{Innholm}(D_8)$, which can be represented as:*

$$\langle x, y, z, a, b \,|x^2 = y^2 = z^2 = a^2 = b^2 = e, xy = yx, xz = zx, yz = zy, ax = xa,$$
$$bx = xb, az = zb, aya^{-1} = xy, bzb^{-1} = xz, byb^{-1} = xy\rangle. \tag{3.2.6}$$

We can now generalize Theorem 3.2.11.

Theorem 3.2.13 *Let n be a positive integer. The multiplication group of $G = D_{2n}$ is $\mathrm{Mul}(G) \cong (G \times G)/K$, where $K \cong \{(g, g^{-1}) \mid g \in Z(G)\}$.*

Proof: Let $\phi : G \times G \to \mathrm{Mul}(G)$ be defined by $\phi(x, y) = L_x R_y$, which is well-defined. Let $(x, y), (a, b) \in G \times G$. Then

$$\phi((x, y)(a, b)) = \phi(xa, yb) = L_{xa}R_{yb} = L_x L_a R_y R_b = L_x R_y L_a R_b = \phi(x, y)\phi(a, b),$$

showing that ϕ is a group homomorphism. By the First Isomorphism Theorem, it follows

$$\mathrm{Mul}(G) \cong (G \times G)/\ker(\phi).$$

Remain to show that $\ker(\phi) = \{(g, g^{-1}) \mid g \in Z(G)\}$. By definition of ϕ,

$$\ker(\phi) = \{(x, y) \in G \times G \mid \phi(x, y) = L_e\},$$

where e is the identity of G. For $g \in G, \phi(x, y) \in \ker(\phi)$ if $\phi(x, y)(g) = g$ for all $g \in G$. That

is, if $xgy = g$ for all $g \in G$. In particular, $xey = e$ which implies $y = x^{-1}$. Thus,

$$\begin{aligned}\ker(\phi) &= \{(g, g^{-1}) \mid ghg^{-1}, \forall h \in G\} \\ &= \{(g, g^{-1} \mid gh = hg, \forall h \in G\} \\ &= \{(g, g^{-1}) \mid g \in Z(G)\}.\end{aligned}$$

Therefore, $\mathrm{Mul}(G) \cong (G \times G)/K$. □

Before we turn the dihedral groups page, we observe that the multiplication group of the dihedral group of order $2n$ has at least one "copy" of D_{2n} embedded into its multiplication group. This can be formally stated as follows:

Corollary 3.2.14 *Let $G = D_{2n}$, then*

$$\mathrm{LMul}(G) \cong \mathrm{RMul}(G) \cong G.$$

Proof: The proof follow by applying Corollary 3.2.8. □

We add one last note about dihedral groups as the multiplication groups of the family of quasigroups Q_n. From the multiplication tables of Q_3, Q_4 and Q_5 we notice that $|R_q| = 2$ for all $q \in Q$. As for the left multiplication maps, it is easy to check that all left multiplication maps are generated by L_ω. These two observation leads us to the following:

Theorem 3.2.15 *Let $Q = Q_n$ equipped with the operation defined for $a, b \in Q_n$ by $a \circ b = \bar{a}b$. Then*

$$\mathrm{LMul}(Q) \cong \mathbb{Z}_n \quad \textit{and} \quad \mathrm{RMul}(Q) \cong D_{2n}$$

Proof: The fact that $\mathrm{LMul}(Q) \cong \mathbb{Z}_n$ follows immediately from the discussion above. For the right multiplication group, as we already know, $|R_\omega| = 2$. Also, for $x \in Q$ we note

$$R_\omega R_{\omega^2}(x) = R_\omega(\bar{x}\omega^2) = \omega\overline{\bar{x}\omega^2} = x\omega^{n-1} = L_\omega(x).$$

That is, $L_\omega \in \mathrm{RMul}(Q)$, and consequently $L_q \in \mathrm{RMul}(Q)$ for all $q \in Q$. We conclude $\mathrm{RMul}(Q) \cong D_{2n}$. □

Now we consider finite groups in general. The two results given in Theorem 3.2.11 and Theorem 3.2.13 can be generalized to finite groups. We first look at finite groups with trivial center.

Theorem 3.2.16 *Let G be a finite group with a trivial center, $Z(G) = \{e\}$. Let $\mathcal{M} = \mathrm{Mul}(G)$ be the multiplication group of G. Then*

$$\mathcal{M} \cong G \times G.$$

Proof: Let $\phi : G \times G \to \mathcal{M}$ be defined by $\phi(g,h) = L_g R_{h^{-1}}$, which is a well-defined map. Next, to show that ϕ is a homomorphism, let $(x,y),(g,h) \in G \times G$, then

$$\phi(xg, yh) = L_{xg} R_{(yh)^{-1}} = L_{xg} R_{(h^{-1}y^{-1})} = L_x L_g R_{y^{-1}} R_{h^{-1}}$$
$$= L_x R_{y^{-1}} L_g R_{h^{-1}} = \phi(x,y)\phi(g,h).$$

Noting that $L_g R_{y^{-1}} = R_{y^{-1}} L_g$ since G is a group. Now to show that ϕ is injective, let $(x,y) \in \ker(\phi)$. Then for all $g \in G$

$$xgy^{-1} = g.$$

In particular, it holds for $g = e$. Thus, $x = y$, and

$$\ker(\phi) = \{(x,y) \in G \times G \mid xg = gx, \forall g \in G\} = \{(e,e)\}.$$

Thus, ϕ is injective and therefore is bijective. Hence $\mathrm{Mul}(G) \cong G \times G$. □

When G has a nontrivial center, a similar situation to that of D_{2n} with n even will result in having a subgroup of $G \times G$ as the multiplication group G. We give a couple of examples followed by the generalization of Theorem 3.2.16.

Example 3.2.17 *Let $G = D_6 \times \mathbb{Z}_3$ which has a nontrivial center $Z(G) \cong C_3$. G is generated by $\bar{c} = (1,c)$, $\bar{r} = (r,1)$, each of order 3, and $\bar{s} = (s,1)$, of order 2. In terms of these generators, G can be represented by*

$$G = \langle \bar{r}, \bar{s}, \bar{c} | \bar{r}^3 = \bar{s}^2 = \bar{c}^3 = 1, \bar{r}\bar{s} = \bar{s}\bar{r}^2, \bar{r}\bar{c} = \bar{c}\bar{r}, \bar{s}\bar{c} = \bar{c}\bar{s} \rangle.$$

The multiplication group of G can be represented by

$$\mathrm{Mul}(G) = \langle L_{\bar{r}}, L_{\bar{s}}, L_{\bar{c}}, R_{\bar{r}}, R_{\bar{s}} \mid L_{\bar{r}}^3 = L_{\bar{s}}^2 = L_{\bar{c}}^3 = R_{\bar{r}}^3 = R_{\bar{s}}^2 = 1, L_{\bar{r}} L_{\bar{s}} = L_{\bar{s}} L_{\bar{r}}^2,$$
$$L_{\bar{r}} L_{\bar{c}} = L_{\bar{c}} L_{\bar{r}}, L_{\bar{r}} R_{\bar{r}} = R_{\bar{r}} L_{\bar{r}}, L_{\bar{r}} R_{\bar{s}} = R_{\bar{s}} L_{\bar{r}}, L_{\bar{s}} L_{\bar{c}} = L_{\bar{c}} L_{\bar{s}}, L_{\bar{s}} R_{\bar{r}} = R_{\bar{r}} L_{\bar{s}},$$
$$L_{\bar{s}} R_{\bar{s}} = R_{\bar{s}} L_{\bar{s}}, L_{\bar{c}} R_{\bar{r}} = R_{\bar{r}} L_{\bar{c}}, L_{\bar{c}} R_{\bar{s}} = R_{\bar{s}} L_{\bar{c}}, R_{\bar{r}} R_{\bar{s}} = R_{\bar{s}} R_{\bar{r}}^2 \rangle \cong D_6 \times D_6 \times \mathbb{Z}_3.$$

Example 3.2.18 *Let K_4 denote the Klein four group, $G = D_6 \times K_4$, and let $\bar{s} = (s,1,1)$, $\bar{r} =$*

$(r,1,1)$, $\bar{c}_2 = (1,c,1)$, *and* $\bar{c}_3 = (1,1,c)$. *Since* $L_{\bar{c}_2} = R_{\bar{c}_2}$, *and* $L_{\bar{c}_3} = R_{\bar{c}_3}$ *the multiplication group of* G *can be defined*

$$\begin{aligned}\mathrm{Mul}(G) =&\langle L_{\bar{r}}, L_{\bar{s}}, L_{\bar{c}_2}, L_{\bar{c}_3}, R_{\bar{r}}, R_{\bar{s}} \mid L_{\bar{r}}^3 = L_{\bar{s}}^2 = L_{\bar{c}_2}^2 = L_{\bar{c}_3}^2 = R_{\bar{r}}^3 = R_{\bar{s}}^2 = 1,\\ &L_{\bar{r}}L_{\bar{s}} = L_{\bar{s}}L_{\bar{r}}^2, L_{\bar{r}}L_{\bar{c}_2} = L_{\bar{c}_2}L_{\bar{r}}, L_{\bar{r}}L_{\bar{c}_3} = L_{\bar{c}_3}L_{\bar{r}}, L_{\bar{r}}R_{\bar{r}} = R_{\bar{r}}L_{\bar{r}}, L_{\bar{r}}R_{\bar{s}} = R_{\bar{s}}L_{\bar{r}},\\ &L_{\bar{s}}L_{\bar{c}_2} = L_{\bar{c}_2}L_{\bar{s}}, L_{\bar{s}}L_{\bar{c}_3} = L_{\bar{c}_3}L_{\bar{s}}, L_{\bar{s}}R_{\bar{r}} = R_{\bar{r}}L_{\bar{s}}, L_{\bar{s}}R_{\bar{s}} = R_{\bar{s}}L_{\bar{s}}, L_{\bar{c}_2}L_{\bar{c}_3} = L_{\bar{c}_3}L_{\bar{c}_2},\\ &L_{\bar{c}_2}R_{\bar{r}} = R_{\bar{r}}L_{\bar{c}_2}, L_{\bar{c}_2}R_{\bar{s}} = R_{\bar{s}}L_{\bar{c}_2}, L_{\bar{c}_3}R_{\bar{r}} = R_{\bar{r}}L_{\bar{c}_3}, L_{\bar{c}_3}R_{\bar{s}} = R_{\bar{s}}L_{\bar{c}_3}, R_{\bar{r}}R_{\bar{s}} = R_{\bar{s}}R_{\bar{r}}^2\rangle.\end{aligned}$$

The multiplication group is isomorphic to $D_6 \times D_6 \times K_4$.

The multiplication group of a group with nontrivial center is isomorphic to its central product. The definition of the central product is given in Definition 1.1.23. The generalization of Theorem 3.2.16 is then:

Theorem 3.2.19 *Let* G *be a finite group with center* $Z = Z(G)$, *and let* $\mathcal{M} = \mathrm{Mul}(G)$. *Then*

$$\mathcal{M} \cong G \circ G.$$

Proof: Let $\phi : G \times G \to \mathcal{M}$ be defined by $\phi(g,h) = L_g R_h$ which is well-defined. Let $(g,h),(x,y) \in G \times G$, then

$$\phi(gx,hy) = L_{gx}R_{hy} = L_g L_x R_h R_y = L_g R_h L_x R_y = \phi(g,h)\phi(x,y).$$

Therefore, ϕ is a group homomorphism. By the First Isomorphism Theorem we have

$$\mathcal{M} \cong (G \times G)/\ker(\phi).$$

We will show that the $\ker\phi \cong Z$. Let $(x,y) \in \ker(\phi)$, then for all $g \in G$

$$\phi(x,y)(g) = g.$$

In particular, this holds for the identity element of G which implies $xy = e$ i.e. $y = x^{-1}$. Therefore,

$$\ker(\phi) = \{(x,y) \in G \times G \mid \phi(x,y)(g) = g, \forall g \in G\} = \{(x,x^{-1}) \mid xgx^{-1} = g, \forall g \in G\}.$$

That is $\ker(\phi) \cong Z$. Therefore, $\mathcal{M} \cong G \circ G$. □

Some of the subgroup structure gets carried over to the multiplication group. The following result shows that the relative multiplication group of a normal group is normal. We state the theorem and prove it.

Theorem 3.2.20 *Let G be a finite group and let $H \trianglelefteq G$. Let $\mathcal{M} = \mathrm{Mul}(G)$ and let $\mathcal{N} = \mathrm{Mul}_G(H)$, then $\mathcal{N} \trianglelefteq \mathcal{M}$.*

Proof: Let $m \in \mathcal{M}$. We will show that $m\mathcal{N} = \mathcal{N}m$. Since G is a group associativity implies for $a, b \in G$ we have $L_a R_b = R_b L_a$, so we may write $m = L_{g_1} R_{g_2}$, for some $g_1, g_2 \in G$. We'll show that for $m \in \mathcal{M}$ we have $m\mathcal{N} = \mathcal{N}m$.

Let $\phi \in m\mathcal{N}$, then $\phi = mn$ for some $n \in \mathcal{N}$. Write $n = L_{h_1} R_{h_2}$ for some $h_1, h_2 \in H$. Then

$$mn = L_{g_1} R_{g_2} L_{h_1} R_{h_2} = L_{g_1} L_{h_1} R_{g_2} R_{h_2} = L_{g_1 h_1} R_{g_2 h_2}.$$

$g_1 h_1 \in g_1 H, g_2 h_2 \in g_2 H$, and H is normal, so there exist $h_3, h_4 \in H$ such that $g_1 h_1 = h_3 g_1$ and $g_2 h_2 = h_4 g_2$.

$\phi = L_{h_3 g_1} R_{h_4 g_2} = L_{h_3} L_{g_1} R_{h_4} R_{g_2} = L_{h_3} R_{h_4} L_{g_1} R_{g_2}$. Then, $\phi \in \mathcal{N}m$, so $m\mathcal{N} \subseteq \mathcal{N}m$. Similarly, $\mathcal{N}m \subseteq m\mathcal{N}$. Therefore, $\mathcal{N} \trianglelefteq \mathcal{M}$. □

3.3 Multiplication Groups and Natural Latin Square Operations

In this section we will be looking at the multiplication groups of reduced Latin squares (Definition 1.1.3) and see how certain natural operations on the Latin square affect the associated multiplication groups. We start with the four reduced Latin squares of order 4 presented in Example 1.1.4. Since the multiplication groups of quasigroups are permutation groups, it make sense to view their generators as permutations. For instance, for the quasigroup in Example 3.3.1, we can represent the left multiplication by 2 as the permutation $L_2 = (12)(34)$. This can easily be done by checking the second row and see where each

element is being mapped to.This idea makes obtaining the generators of the multiplication group of a quasigroup faster.

Example 3.3.1 *The first three tables in Example 1.1.4 are isotopic, but not the fourth one. We show in this example that all three in the first class have isomorphic multiplication groups. The multiplication group of the fourth table will not be isomorphic to those of the first three.*

Let's start with

Q_1	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	2	1
4	4	3	1	2

As a quasigroup, this is generated by 3. *Thus,* $\mathrm{Mul}(Q_1) = \langle L_3, R_3 \rangle$ *but since* $R_3(x) = L_3(x)$ *for any* $x \in Q_1$, *we have* $\mathrm{Mul}(Q_1) = \langle L_3 \mid L_3^4 = 1_{Q_1} \rangle \cong \mathbb{Z}_4$. *The second table in Example 1.1.4 is the multiplication group of* Z_4 *and abelian groups are isomorphic their own multiplication groups. Now consider the third table. This quasigroup is generated by* 2 *and*

Q_3	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

as in the case of Q_1, *we have* $\mathrm{Mul}(Q_3) \cong \mathbb{Z}_4$. *The fourth table, which represents a different isotopic class, is the multiplication table of* $\mathbb{Z}_2 \times \mathbb{Z}_2$ *which is an abelian group and therefore is isomorphic to its own multiplication group.*

The example above does not imply that any isotopic quasigroups have isomorphic multiplication groups. Here is an example where this fails.

Example 3.3.2 *Isotopy does not preserve multiplication groups. Take for example* $Q = \mathbb{Z}_3$ *and let* P *be the quasigroup whose multiplication table obtained from that of* $\mathbb{Z}_3$ *by swapping*

G	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

Q	1	2	3
1	1	2	3
2	3	1	2
3	2	3	1

rows 2 and 3.

$\mathrm{Mul}(\mathbb{Z}_3) \cong \mathbb{Z}_3$, *while* $\mathrm{Mul}(P) \cong S_3$.

Given an abelian group, we can define a quasigroup using a twist on the operation of the group (See Theorems 2.1.19 and 2.1.13). This process produces isotopic quasigroups to the group we started with. In the following two examples we compute the multiplication groups of each twist of $\mathbb{Z}_5$ and $\mathbb{Z}_7$.

Example 3.3.3 *Let* $\circ_i$ *be the operation defined as* $a \circ_i b = a^{-i}b$. *For* $a, b \in \mathbb{Z}_5$ *this operation is then* $a \circ_i b = -ia + b = b - ia$, *for* $i = 1, 2, 3, 4$. *We will denote* $(\mathbb{Z}_5, \circ_i)$ *by* $\mathbb{Z}_5^i$, *and* $M_i = \mathrm{Mul}(\mathbb{Z}_5^i)$. *We know that* $\mathrm{Mul}(\mathbb{Z}_5) \cong \mathbb{Z}_5$. *The quasigroup* $\mathbb{Z}_5^1$ *the multiplication group is isomorphic to* D_{10}, *while* $\mathbb{Z}_5^4$ *has a multiplication group isomorphic to* $\mathbb{Z}_5$. *The multiplication groups of* $\mathbb{Z}_5^2$ *and* $\mathbb{Z}_5^3$ *are both isomorphic to an order* 20 *group, namely the order* 20 *general afiine group.*

Example 3.3.4 *Now we consider* $\mathbb{Z}_7$, *with the operation* $\circ_i$ *is defined for* $a, b \in \mathbb{Z}_7$ *by* $a \ \phi_i \ b = a^{-i}b = -ia + b, i \in \mathbb{Z}_7$. *As in the previous example* $\mathbb{Z}_7^i$ *is used as a shorthand of* $(\mathbb{Z}_7, \circ_i)$. *It is clear* $\mathrm{Mul}(\mathbb{Z}_7) \cong \mathbb{Z}_7$. *Also, as in the case of* $\mathbb{Z}_5$, *we have* $\mathrm{Mul}(\mathbb{Z}_7^6) \cong \mathbb{Z}_7$. *The multiplication groups of* $\mathbb{Z}_7^3$ *and* $\mathbb{Z}_7^5$ *are both isomorphic to* $\mathbb{Z}_3 \times \mathbb{Z}_7$. *The multiplication groups* M_2 *and* M_4 *are isomorphic to* $\mathbb{Z}_7 \times \mathbb{Z}_6$.

One natural operation that can be applied on Latin squares is swapping rows. If we swap two rows of a Latin square, what happens to the multiplication group? The answer is described in the following theorem:

Theorem 3.3.5 *Let Q be a finite quasigroup with multiplication group* $\mathrm{Mul}(Q)$*. Let ϕ be a permutation, and let P be the quasigroup whose multiplication table is obtained from that of Q after swapping the rows according to ϕ. Then, the multiplication Group of P, $\mathcal{M} = \mathrm{Mul}(P)$, is generated by $L_{\phi(q)}$ and $R_q \cdot \phi$ where $q \in Q$.*

Proof: Let Q be a finite quasigroup and let $\phi \in S_{|Q|}$. Let P be defined as in the statement of the theorem. We want to show that $G = \langle L_{\phi(q)}, R_q \cdot \phi \rangle$, where $q \in Q$ is isomorphic to $\mathcal{M}$ (Note: $R_q \cdot \phi$ takes place in $S_{|Q|}$). Let R_a^Q denote the right multiplication by $a \in Q$ and R_a^P denote the right multiplication by $a \in P$. We will show $G = \mathcal{M}$.

Since ϕ is a permutation, for every $p \in P$ there is a $q \in Q$ such that $p = \phi(q)$. This means, that left multiplication by $a \in Q$ is equivalent to multiplying by $\phi(a) \in Q$. Thus, $\mathcal{M}$ will have the same left multiplication maps as $\mathrm{Mul}(Q)$.

For the right multiplication, in Q we have $R_a^Q(x) = xa$. After swapping the rows, the entry x will move to the row labeled $\phi(x)$. Thus, $R_a^P(x) = R_a^Q(\phi(x))$.

In other words, after swapping the rows, row x in the Latin square of Q will be placed in the row labeled $\phi(x)$ in the newly generated Latin square.

Therefore, the generators of $\mathcal{M}$ are the generators of G, thus $\mathcal{M} = G$. □

As seen in the proof, the left multiplication maps are exactly the same for both Q and P as defined in Theorem 3.3.5. This gives the following corollary:

Corollary 3.3.6 *Swapping two or more rows of the multiplication table of a quasigroup does not change the left multiplication group.*

The following two examples illustrate Theorem 3.3.5.

Example 3.3.7 *Let $Q = \mathbb{Z}_3$ and consider the Latin square obtained from that of Q after sapping the first and second row.*

*	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

*	1	2	3
1	2	3	1
2	1	2	3
3	3	1	2

Here $\phi = (12)$. *Calculating* $\mathrm{Mul}(P)$ *directly we have*

$$\mathrm{Mul}(P) \cong \langle (123), (132), (12), (13), (23) \rangle = S_3.$$

Now, using 3.3.5 the multiplication group of P *is*

$$\begin{aligned} \mathrm{Mul}(P) &\cong \langle L_{\phi(1)}, L_{\phi(2)}, L_{\phi(3)}, R_1 \cdot (12), R_2 \cdot (12), R_3 \cdot (12) \rangle \\ &= \langle (123), (1), (132), (12), (13), (23) \rangle = S_3. \end{aligned}$$

(Note: the subscripts here are viewed as elements of Q*).*

Next, let's consider $\mathbb{Z}_4$ and take $\phi = (123)$.

Example 3.3.8 *Let* $Q = \mathbb{Z}_4$*, and let* $\phi = (123)$*. Let* P *be defined by the table to the right. Calculating the multiplication group directly and using Theorem 3.3.5 yield* $\mathrm{Mul}(P) \cong S_4$.

*	1	2	3	4
1	1	2	3	4
2	2	3	4	1
3	3	4	1	2
4	4	1	2	3

*	1	2	3	4
1	3	4	1	2
2	1	2	3	4
3	2	3	4	1
4	4	1	2	3

For the calculation and the GAP code refer to Example A.6.5.

A similar result follow when swapping the columns rather than the rows. This gives the following:

Theorem 3.3.9 *Let* Q *be a finite quasigroup with multiplication group* $\mathrm{Mul}(Q)$*. Let* ϕ *be a permutation, and let* P *be the quasigroup whose multiplication table is obtained from that of* Q *after swapping the columns according to* ϕ*. Then, the multiplication Group of* P*,* $\mathcal{M} = \mathrm{Mul}(P)$*, is generated by* $L_q \cdot \phi$ *and* $R_{\phi(q)}$ *where* $q \in Q$.

Proof: First, observe that the right multiplication maps in Mul(P) and Mul(Q) are the same. For the left multiplication: In Q, we have $L_a^Q(x) = ax$. In P, after swapping the columns column x is placed in column $\phi(x)$ in the new table, thus in P this will read

$$L_a^P(x) = a\phi(x) = L_a^Q(\phi(x))$$

Thus, $L_a^P = L_a^Q \cdot \phi$. The proof is complete. □

Another way to prove this is by using Theorem 3.3.5 together with Theorem 3.4.6, which shows that two quasigroups whose Latin squares are the transposes of one another have the same multiplication groups. Analogous to Corollary 3.3.6, we have

Corollary 3.3.10 *Swapping two or more columns of the multiplication table of a quasigroup does not change the right multiplication group.*

Another natural operation is entry-wise permutation, in which a permutation $\phi \in S_n$ is applied entry by entry on an order n Latin square. The following relates the multiplication group of the quasigroups defined by these two Latin squares.

Theorem 3.3.11 *Let $\phi \in S_n$, and let Q be a quasigroup with Latin square S. Let P be the quasigroup whose Latin square is obtained from S after applying ϕ entry-wise to S. Then* $\text{Mul}(P) = \langle \phi \cdot L_q, \phi \cdot R_q \rangle$.

Proof: Let the left and right multiplications in Mul(P) and Mul(Q) be respectively denoted by L_a^P, R_a^P and L_a^Q, R_a^Q. We first note if

$$L_a^Q : x \to y, \quad \text{i.e.} \quad ax = y,$$

then after applying ϕ to the entries in the Latin square of Q we get

$$L_a^P : x \to \phi(y),$$

which is equivalent to saying

$$\phi(L_a^Q(x)) = \phi(ax) = \phi(y).$$

Thus, $L_a^P = \phi \cdot L_a^Q$. Similarly, for the right multiplication observe that if

$$R_a^Q : z \to w,$$

then in P,

$$R_a^P : z \to \phi(w).$$

It follows

$$R_a^P = \phi \cdot R_a^Q.$$

Therefore, $\mathrm{Mul}(P) = \langle \phi \cdot L_q, \phi \cdot R_q \rangle$. □

We wrap up this section with the following remarks:

Remark 3.3.12 *If Q is a quasigroup whose multiplication table is a symmetric Latin square, then its multiplication group, left multiplication group and right multiplication group are all equal.*

Remark 3.3.13 *If the right multiplication or the left multiplication group of an order n quasigroup is isomorphic to S_n, then the multiplication group and the other side multiplication group are also isomorphic to S_n.*

3.4 Multiplication Groups of Conjugates of a Quasigroup

Each quasigroup determines six potentially different combinatorial quasigroups. [40] also gives a way to specify the equational quasigroups conjugates to a given quasigroup. This is done by applying the right multiplication action by an element of S_3 to the terms of the equation $a * b = c$. One can display the elements of S_3 as the nodes of the Cayley diagram:

$$\begin{array}{ccccc} (1) & \Longleftrightarrow & (23) & \longleftrightarrow & (123) \\ \updownarrow & & & & \Updownarrow \\ (12) & \Longleftrightarrow & (132) & \longleftrightarrow & (13) \end{array} \tag{3.4.1}$$

where the single arrow is the right multiplication by (12) and the double arrow is right multiplication by (23). The six potentially distinct quasigroups will have the following

operations for fixed a, b and c in the set Q

$$\begin{array}{ccccc} a*b=c & \Longleftrightarrow & a*c=b & \longleftrightarrow & c*a=b \\ \Updownarrow & & & & \updownarrow \\ b*a=c & \Longleftrightarrow & b*c=a & \longleftrightarrow & c*b=a \end{array} \tag{3.4.2}$$

One question is, which, if any, of the six conjugates of a quasigroup have the same multiplication table. We define the following notation of the six conjugates of a quasigroup in this context as follows:

Definition 3.4.1 *[40] The six conjugates of a quasigroup Q will be denoted by $Q_{(12)}$, $Q_{(13)}$, $Q_{(23)}$, $Q_{(123)}$ and $Q_{(132)}$. If the operation in Q, for $a, b, c \in Q$, is given by $a * b = c$, then the operation in the five conjugates can respectively be defined by $b * a = c, c * b = a, a * c = b, c * a = b$ and $b * c = a$.*

To illustrate, we look at the following example:

Example 3.4.2 *Consider $\mathbb{Z}_3$, then the conjugates of $\mathbb{Z}_3$ have the multiplication tables (omitting the head row and head column):*

$$\begin{array}{ccccc} \begin{array}{ccc} 1&2&3\\ 2&3&1\\ 3&1&2 \end{array} & & \begin{array}{ccc} 1&2&3\\ 3&1&2\\ 2&3&1 \end{array} & & \begin{array}{ccc} 1&3&2\\ 2&1&3\\ 3&2&1 \end{array} \\ \updownarrow & & & & \Updownarrow \\ \begin{array}{ccc} 1&2&3\\ 2&3&1\\ 3&1&2 \end{array} & \Longleftrightarrow & \begin{array}{ccc} 1&2&3\\ 3&1&2\\ 2&3&1 \end{array} & \longleftrightarrow & \begin{array}{ccc} 1&3&2\\ 2&1&3\\ 3&2&1 \end{array} \end{array}$$

These six table represent

$$\begin{array}{ccccc} Q & \Longleftrightarrow & Q_{(23)} & \longleftrightarrow & Q_{(123)} \\ \updownarrow & & & & \Updownarrow \\ Q_{(12)} & \Longleftrightarrow & Q_{(132)} & \Longleftrightarrow & Q_{(13)} \end{array}$$

The multiplication groups are respectively isomorphic to

$$\begin{array}{ccc} \mathbb{Z}_3 & S_3 & S_3 \\ \mathbb{Z}_3 & S_3 & S_3 \end{array}$$

It is well-know that the number of conjugates for a quasigroups Q is either 1, 2, 3 or 6. It turns out that for a given quasigroup and its conjugates the left and right multiplication groups of all conjugates are at most three different groups (up to isomorphism).

Example 3.4.3 *Let $Q = \mathbb{Z}_3$, then the multiplication group, right and left multiplication groups of Q are all $\mathbb{Z}_3$. The right multiplication group of $Q_{(23)}$ is S_3. That is, the right multiplication groups of two conjugates are not necessarily isomorphic. The same thing can be said about left multiplication groups and therefore multiplication groups of two conjugates.*

Let Q be a quasigroup and let Q_σ denote one of the six conjugates of Q. As we already mentioned, the left and right multiplications group of each of the six conjugates is one of three possible groups. If we let G_1 and G_2 to be respectively the left and right multiplication groups of Q, then $Q_{(23)}$ has the same left multiplication group G_1. However, the right multiplication group of $Q_{(23)}$ is not necessarily G_1 or G_2 (Example 3.4.3). We'll denote this third group by G_3. Because of the way the conjugates are defined, we note the following:

$$\begin{array}{ccccc} Q, G_1, G_2 & \Longleftrightarrow & Q_{(23)}, G_1^{-1}, G_3 & \longleftrightarrow & Q_{(123)}, G_3, G_1^{-1} \\ \Updownarrow & & & & \updownarrow \\ Q_{(12)}, G_2, G_1 & \Longleftrightarrow & Q_{(132)}, G_2^{-1}, G_3^{-1} & \longleftrightarrow & Q_{(13)}, G_3^{-1}, G_2^{-1} \end{array}$$

where each triple consists respectively the quasigroup, its left multiplication group and its right multiplication group. These observations leads us to:

Theorem 3.4.4 *Let Q be a quasigroup, and let $P = Q_{(23)}$. Then, the left multiplication group of P is isomorphic to the left multiplication of Q.*

Proof: The left multiplication group of Q is generated by the maps L_a where $a \in Q$, which when acting on an element $b \in Q$ we get $L_a(b) = c$ (since $a * b = c$). In P, the operation

is $a * c = b$, that means $L_a(c) = b$, and therefore $L_a^{-1}(b) = c$. This shows that the left multiplication group of P is generated by the inverses of the left multiplication maps by elements of Q. Therefore $\mathrm{LMul}(P) \cong \mathrm{LMul}(Q)$. □

We can't say the same about the right multiplication group of $Q_{(23)}$ in relation to that of Q. However, we can say that about the right multiplication groups the conjugate $Q_{(123)}$ and the left multiplication group of Q.

Theorem 3.4.5 *Let Q be a quasigroup, and let $P = Q_{(123)}$. Then, the right multiplication group of P is isomorphic to the left multiplication of Q.*

Proof: Noting that the right multiplication $R_a \in \mathrm{RMul}(P)$ is equal to $L_a \in \mathrm{LMul}(Q)$, the proof follows in a similar way as in Theorem 3.4.4. □

Now consider, $Q_{(12)}$. The multiplication table of which is the transpose of that of Q. The relations between their multiplication groups are therefore:

Theorem 3.4.6 *Let Q be a quasigroup, and let P be the quasigroup whose Latin square is the transpose of that of Q. Then* $\mathrm{LMul}(P) \cong \mathrm{LMul}(Q)$, $\mathrm{RMul}(P) \cong \mathrm{RMul}(Q)$, *and* $\mathrm{Mul}(P) \cong \mathrm{Mul}(Q)$.

Proof: This follows from the fact that left multiplications and right multiplication maps switch rules. □

As we have already mentioned, Theorem 3.3.9 also follows as a consequence of Theorem 3.3.5 and 3.4.6. We now formulate the idea discussed following Example 3.4.3.

Corollary 3.4.7 *Let Q be a quasigroup. Then the right and left multiplication groups of Q and its five conjugates are at most three different groups up to isomorphism.*

Proof: The proof follow from Theorems 3.4.4, 3.4.5, and 3.4.6. □

It would be interesting to know what groups will show up as this triple of groups.

Question 3.4.8 *What can be said about these groups described in Corollary 3.4.7? If we pick three arbitrary permutation groups can we find a quasigroup that will have this choice of groups as the right and left multiplication groups of the six conjugates?*

Next, we look at the conjugacy classes of all order 3 Latin squares.

Example 3.4.9 *The twelve order 3 Latin squares can be classified into 6 classes. The first one is the one that contains the multiplication table of $\mathbb{Z}_3$. This class is given in Example 3.4.2. Another class is*

$$\begin{array}{ccccc}
2\ 1\ 3 & & 2\ 1\ 3 & & 2\ 3\ 1 \\
3\ 2\ 1 & \Longleftrightarrow & 3\ 2\ 1 & \longleftrightarrow & 1\ 2\ 3 \\
1\ 3\ 2 & & 1\ 3\ 2 & & 3\ 1\ 2 \\
\updownarrow & & & & \updownarrow \\
2\ 3\ 1 & & 3\ 1\ 2 & & 3\ 1\ 2 \\
1\ 2\ 3 & \Longleftrightarrow & 1\ 2\ 3 & \longleftrightarrow & 1\ 2\ 3 \\
3\ 1\ 2 & & 2\ 3\ 1 & & 2\ 3\ 1
\end{array}$$

A third class is

$$\begin{array}{ccccc}
2\ 3\ 1 & & 3\ 1\ 2 & & 3\ 2\ 1 \\
3\ 1\ 2 & \Longleftrightarrow & 2\ 3\ 1 & \longleftrightarrow & 1\ 3\ 2 \\
1\ 2\ 3 & & 1\ 2\ 3 & & 2\ 1\ 3 \\
\updownarrow & & & & \updownarrow \\
2\ 3\ 1 & & 3\ 1\ 2 & & 3\ 2\ 1 \\
3\ 1\ 2 & \Longleftrightarrow & 2\ 3\ 1 & \longleftrightarrow & 1\ 3\ 2 \\
1\ 2\ 3 & & 1\ 2\ 3 & & 2\ 1\ 3
\end{array}$$

Each table of the following form its own conjugacy class.

$$\begin{array}{ccc}
1\ 3\ 2 & 2\ 1\ 3 & 3\ 2\ 1 \\
3\ 2\ 1 & 1\ 3\ 2 & 2\ 1\ 3 \\
2\ 1\ 3 & 3\ 2\ 1 & 1\ 3\ 2
\end{array}$$

A question that might be asked here is the following:

Question 3.4.10 *Can the natural operation on Latin squares be used to get a better understanding of the multiplication groups of quasigroups and its conjugates?*

In the following, MidMul denotes the **middle translation multiplication group** of a quasigroup. This group is generated by what is called the middle translation which is defined by $I_q(x) = x\backslash q$ or equivalently $x \cdot I_q(x) = q$. The group generated by left, right and middle translations, all together, is called the **full multiplication group** and is denoted by FMul.

Theorem 3.4.11 *[38] Let G be a group with center $Z = Z(G)$. Let $\mathcal{M} = \mathrm{Mul}(Q)$ then*

$$\mathrm{LMul}(G) \cong G, \quad \mathcal{M}/Z \cong G/Z \times G/Z, \quad \mathrm{FMul}(G) \cong \mathcal{M}\lambda\mathbb{Z}_2, \quad \mathrm{FMul}(Q,\cdot) \cong \mathrm{MidMul}(Q,\cdot).$$

Example 3.4.12 *Consider $(Q_3, \circ)$, the middle translation maps satisfy*

$$x \circ I_1(x) = 1, \qquad x \circ I_\omega(x) = \omega, \qquad x \circ I_{\omega^2}(x) = \omega^2.$$

As permutations, $I_1 = (1)$, $I_2 = (123)$ and $I_3 = (132)$. Thus,

$$\mathrm{MidMul}(Q_3) \cong \mathbb{Z}_3 \cong \mathrm{LMul}(Q_3).$$

The same can be said about the family of quasigroups Q_n. This is formulated in the the following theorem:

Theorem 3.4.13 *Let $Q = (Q_n, \circ)$ with the usual operation where for $a, b \in Q_n$, we define $a \circ b = \bar{a}b$. Then*

$$\mathrm{MidMul}(Q) \cong \mathrm{LMul}(Q) \cong \mathbb{Z}_n.$$

Proof: Let $q \in Q$, and consider the middle translation map I_q. Then for $x \in Q$ we have

$$x \circ I_q(x) = q$$

or equivalently

$$\bar{x} I_q(x) = q.$$

Thus,

$$I_q(x) = xq = qx = \bar{q} \circ x = L_{\bar{q}}(x).$$

Therefore, $I_q = L_{\bar{q}}$ and hence $\mathrm{LMul}(Q) \cong \mathrm{MidMul}(Q)$. Theorem 3.2.15 then implies that $\mathrm{MidMul}(Q) \cong \mathbb{Z}_n$. □

Definition 3.4.14 *[38] Let $(Q, \cdot)$ be a groupoid and let $q \in Q$. The element q is* **left (middle, right) nuclear** *element in $(Q, \cdot)$ means that $L_{qx} = L_q L_x \Leftrightarrow qx \cdot y = q \cdot xy$ ($L_{xq} = L_x L_q \Leftrightarrow xq \cdot y = x \cdot qy, R_{xq} = R_q R_x \Leftrightarrow y \cdot xq = yx \cdot q$) for all $x, y \in Q$.*

If q is a left, middle and right nuclear, then we say q is a **nuclear** in $(Q, \cdot)$.

Definition 3.4.15 *[38] Let $(Q, \cdot)$ be a groupoid. The left nucleus N_ℓ (middle nucleus, N_m, right nucleus N_r) of $(Q, \cdot)$ is the set of all left (middle, right) nuclear elements in $(Q, \cdot)$ and the nucleus is given by $N = N_\ell \cap N_r \cap N_m$.*

The sets above can be described by

$$\begin{aligned} N_\ell &= \{a \in Q \mid a \cdot xy = ax \cdot y, x, y \in Q\} \\ N_m &= \{a \in Q \mid xa \cdot y = x \cdot ay, x, y \in Q\} \\ N_r &= \{a \in Q \mid xy \cdot a = x \cdot ya, x, y \in Q\} \end{aligned} \tag{3.4.3}$$

R. H. Bruck defined a center of a loop $(Q, \cdot)$ as $Z(Q, \cdot) = N \cap C$, where $C = \{a \in Q \mid a \cdot x = x \cdot a, \forall x \in Q\}$. [38]

Example 3.4.16 *In the case of groups, all nucleus are equal to the group itself, associativity. Therefore, the definition of a center in a group is the usual definition $Z(G) = \{g \in G \mid gh = hg, \forall h \in G\}$.*

Now consider the quasigroup $P = Q_{(23)}$ from Example 3.4.2. Note that $1 \in N_\ell$, since $\forall x, y \in Q$ it holds that $1 \cdot (x \cdot y) = (1 \cdot x) \cdot y$. However, $2 \cdot (1 \cdot 1) \neq (2 \cdot 1) \cdot 1$ and $3 \cdot (1 \cdot 1) \neq (3 \cdot 1) \cdot 1$ respectively show that $2, 3 \notin N_\ell$. Both inequalities also show that $1 \notin N_r$ and therefore $N_r \cap N_\ell = \emptyset$. Also, since $1 \cdot 2 \neq 2 \cdot 1$ in Q, it follows that the center of Q, according to the definition above, is empty.

Theorem 3.4.17 *[38] For a loop (even for a groupoid)* $Z = N_\ell \cap N_r \cap C$.

This theorem is saying that the middle nucleus can be disregarded when computing the center of a groupoid.

Definition 3.4.18 *[38] M. D. Kitaroage gives the following definition of nuclei of a quasi-group*

$$\begin{aligned} N_\ell(h) &= \{a \in Q \mid ax \cdot y = a \cdot L_h^{-1}(hx \cdot y), \forall x, y \in Q\} \\ N_m(h) &= \{a \in Q \mid R_h^{-1}(xa) \cdot y = x \cdot L_h^{-1}(ay), \forall x, y \in Q\} \\ N_r(h) &= \{a \in Q \mid yx \cdot a = R_h^{-1}(y \cdot xh) \cdot a, \forall x, y \in Q\}. \end{aligned} \tag{3.4.4}$$

Chapter 4

Loops and their Multiplication Groups

In this chapter we focus on loops and their multiplication groups. A loop is a quasigroup with an identity element. As such, loops are closer to being groups than an arbitrary quasigroup, but they need not be associative or to have a two-sided inverse. We begin in Section 4.1 with the basic definitions and examples of loops and some of their generalizations. In Section 4.2 we present some of the known results about loops and their generalizations. Finally in Section 4.3, we explore the properties of the multiplication groups of loops and their generalizations.

4.1 Definitions and Examples

We start this section by defining two special kind of quasigroups.

Definition 4.1.1 *[49] A quasigroup Q with a single idempotent element is called* **pique** *("pointed idempotent quasigroup").*

Definition 4.1.2 *[39] A quasigroup is said to be* **idempotent** *if every element $q \in Q$ is idempotent. That is, $q^2 = q$ for all $q \in Q$.*

Example 4.1.3 *The table below gives an example of a pique that is not an idempotent quasigroup nor a loop.*

*	1	2	3
1	3	2	1
2	1	3	2
3	2	1	3

Example 4.1.4 *The Latin square given below represents the multiplication table of an idempotent quasigroup. One can easily check conditions (i) and (ii) of Definition 2.1.1 to see that*

*	1	2	3
1	1	3	2
2	3	2	1
3	2	1	3

this is indeed a quasigroup. Also, the condition $q^2 = q$ hold for each of the elements of the quasigroup.

A quasigroup need not have an identity element. A quasigroup with an identity element is called a loop.

Definition 4.1.5 *A* **loop** *is a quasigroup with an identity element, e such that for all $q \in Q$*

$$q \star e = e \star q = q \tag{4.1.1}$$

The identity element of a loop, e, is unique, and since $e^2 = e$ it follows that every loop has at least one idempotent element and therefore every loop is a pique. Example 4.1.3 gives the multiplication table of a non-loop piques.

Note that piques (Definition 4.1.1) make up a large family of quasigroups that includes all idempotent quasigroups (Definition 4.1.2), and the family of all idempotent quasigroups includes all loops (Definition 4.1.5).

A loop that is associative is a group. A group can have a non-associative pique isotope, but it cannot have a nonassociative loop isotope. A loop can't be isotopic to a quasigroup which is not a loop, take for instance the table in Example 4.1.3.

The formal beginning of loop theory was after defining the two most important classes of loops which are Moufang loops (Definition 4.2.9) and Bol loops (Definition 4.2.10). The term

"loop" was first introduced by Albert in his 1943 papers Quasigroups. I [2] and Quasigroups. II [3].

Example 4.1.6 *Every group is a quasigroup has an identity element, and therefore every group is a loop. The converse is not true.*

We may define a loop using the following identities

$$\begin{aligned} q \cdot (q\backslash p) &= p \\ (p/q) \cdot q &= p \\ q\backslash(q \cdot p) &= p \\ (p \cdot q)/q &= p \\ q/q &= p\backslash p \end{aligned} \tag{4.1.2}$$

A loop given by (4.1.2) is an equational loop.

Definition 4.1.7 (Equational Loop) *[38] A groupoid $(Q, \cdot)$ is a loop if there are operations "$\backslash$" and "$/$" such that in the algebra $(Q, \cdot, \backslash, /)$ the identities in (4.1.2) hold.*

A **subloop** of a loop is a subset that forms a loop under the operation on the loop. A **normal subloop** can be defined as a subloop N of the loop Q that is the kernel of some loop homomorphism. In this case the expected properties hold: N is a normal subloop of the loop Q precisely when set multiplication gives a well-defined coset multiplication and the quotient loop Q/N is canonically isomorphic to the image of any homomorphism with kernel N. [17, 7]

In Theorem 3.2.20 we showed that the relative multiplication group of a normal subgroup of a group is a normal subgroup of the multiplication group.

Question 4.1.8 *Is the relative multiplication group of a normal subloop a normal subgroup of the multiplication group of the original loop? If so, can that be generalized to normal subquasigroups?*

4.2 Known Results about Loops

The following is a known result regarding loops.

Theorem 4.2.1 *[40] Let Q be a quasigroup. Then Q is a loop if and only if Q satisfies the identity*

$$x(y/y) \cdot z = x \cdot (y/y)z. \tag{4.2.1}$$

In a loop Q, every element $q \in Q$ has a unique left inverse denoted $q^\lambda = e/q$ that satisfies $q^\lambda q = e$, where e is the identity element. Also, $q \in Q$ has a unique right inverse $q^\rho = q\backslash e$ with $qq^\rho = e$. If $q^\lambda = q^\rho$ we say q has two sided inverse in which case we denote it by q^{-1}. The elements in a loop may satisfy one or more properties when considering inverses of an element. The following define these properties.

Definition 4.2.2 *[49] Let Q be a loop, then we say Q has the* **left inverse property** *if $q^\lambda(qr) = r$ for all $q, r \in Q$. It has the* **right inverse property** *if $(rq)q^\rho = r$ for all $q, r \in Q$. If Q has both the right and left inverse properties, Q is said to have the* **inverse property**. *If $(rq)^\lambda = q^\lambda r^\lambda$, or, equivalently, $(rq)^\rho = q^\rho r^\rho$ for all $q, r \in Q$, we say Q has the* **antiautomorphic inverse property**. *We say Q has the* **weak inverse property** *when $(qp)r = e$ if and only if $q(pr) = e$. Equivalently, $(pq)^\lambda p = q^\lambda$ or $p(qp)^\rho = q^\rho$.*

Example 4.2.3 *Each element in the loop in Example 4.2.4 has itself as its inverse since each element is the right and left inverse of itself. However, this loop doesn't have the right nor the left inverse property. For example, $a * (a * b) = a * c = d \neq b$ and $(b * a) * a = d * a = c \neq b$. Further, the loop in Example 4.2.4 does not have the antiautomorphic property either, as $(a * b)^{-1} = c$ while $b^{-1} * a^{-1} = b * a = d$. This loop, however, does have the weak inverse property as for any elements x, y, z it holds that $(x * y) * z = 1$ if and only if $x * (y * z) = 1$.*

In Example 4.2.6, the left and right inverse are not the same for any element. This loop does not satisfy any of the loop inverse properties. One can verify that $2 * (3 * 4) \neq 4, (3 * 4) * 2 \neq 3, (5 * 3)^\lambda \neq 3^\lambda * 5^\lambda$, and $(4 * 2)^\rho \neq 2^\rho * 4^\rho$.

Example 4.2.4 *Referring to the Latin square from Example 2.2.10 . Let L be the quasigroup with multiplication table:*

*	1	a	b	c	d
1	1	a	b	c	d
a	a	1	c	d	b
b	b	d	1	a	c
c	c	b	d	1	a
d	d	c	a	b	1

Since $1 * q = q * 1 = q$ for all $q \in L$, $e = 1$ is the identity element of L, i.e. L is a loop. However, this is not a group since

$$(a * a) * b = b \neq d = a * (a * b).$$

Recall that L_q^{-1} and R_q^{-1} for q in a quasigroup Q are always defined. For an element $p \in Q$ we have $L_q^{-1}(p) = q\backslash p$ and $R_q^{-1}(p) = p/q$. In a loop Q with the left inverse property, each $q \in Q$ has a left inverse q^λ, and thus $L_q^{-1} = L_{q^\lambda}$. If Q has the right inverse property then $R_q^{-1} = R_{q^\rho}$, where q^ρ is the right inverse of q. In a loop with the inverse property, $q^{-1} = q^\lambda = q^\rho$, and it follows that $L_q^{-1} = L_{q^{-1}}$ and $R_q^{-1} = R_{q^{-1}}$. Compare with equation (2.1.7).

Remark 4.2.5 *In reference to Definition 4.2.2, the left and right inverse property are respectively equivalent to saying*

$$L_q^{-1} = L_{q^\lambda} \quad or \quad q\backslash r = q^\lambda r. \tag{4.2.2}$$

$$R_q^{-1} = R_{q^\rho} \quad or \quad r/q = rq^\rho. \tag{4.2.3}$$

Example 4.2.6 [1] *The left and right inverse in a loop need not be the same for every element. For example, every nonidentity element in the loop given by the order 5 Latin square below has a left inverse that do not agree with the right inverse for that element.*

Some loops, including groups, has the property that the right and left inverses are the same. However, this is not true for all loops.

[1] Example 4.2.6 and Example 4.2.7 were found in this Stack Exchange page.

*	1	2	3	4	5
1	1	2	3	4	5
2	2	5	1	3	4
3	3	4	5	2	1
4	4	1	2	5	3
5	5	3	4	1	2

Example 4.2.7 *The below order 8 Latin square defines a loop, which is not a group, yet every element has identical left and right inverse.*

*	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	8	6	1	7	3	5	4
3	3	7	8	6	1	4	2	5
4	4	1	7	8	6	5	3	2
5	5	6	1	7	8	2	4	3
6	6	3	4	5	2	8	1	7
7	7	5	2	3	4	1	8	6
8	8	4	5	2	3	7	6	1

As mentioned before, associativity of the operation defined on a quasigroup implies that the quasigroup is a loop, and therefore is a group.

Theorem 4.2.8 *[38] Let Q be a nonempty set and let $\cdot$ be a binary operation. The following are equivalent:*

1. *$(Q, \cdot)$ is an associative quasigroup.*
2. *$(Q, \cdot)$ is an associative loop.*
3. *$(Q, \cdot)$ is a group.*

Proof: In this proof xy will be used to mean $x \cdot y$.

(1) $\Rightarrow$ (2) Assume that Q is an associative quasigroup. Let $q \in Q$, then there are unique elements $e, f \in Q$ such that $qe = q$ and $fq = q$. Since Q is associative, it follows: $qe^2 = (qe)e = qe = q$, i.e. $e^2 = e$. Let $p \in$ Q such that $ep = q$ (Q is a quasigroup), then $fep = fq = q = ep$, i.e. $fe = e = e^2$ and so $f = e$. Now, let $r \in Q$, then $er = e^2r$ and

$re = re^2$ or equivalently $re = r = er$, i.e. e is an identity element, and therefore Q is a loop.

(2) $\Rightarrow$ (3) Now suppose that Q is an associative loop. The closure and identity axioms hold by definition and associativity holds by assumption. Remain to show that the inverse axiom also holds. Let e be the identity element of Q and let $q \in Q$. By definition of quasigroup, there are unique elements $a, b \in Q$ such that $ap = e$ and $pb = e$. Then $b = eb = (ap)b = a(pb) = ae = a$. Thus, Q is a group.

(3) $\Rightarrow$ (1) Every group is an associative quasigroup.

The proof is complete. □

The identities below are called the Moufang identities:

$$\begin{aligned} q \cdot (p \cdot (q \cdot r)) &= ((q \cdot p) \cdot q) \cdot r \\ ((r \cdot q) \cdot p) \cdot q &= r \cdot (q \cdot (p \cdot q)) \\ (p \cdot q) \cdot (r \cdot p) &= p \cdot ((q \cdot r) \cdot p) \end{aligned} \tag{4.2.4}$$

Definition 4.2.9 *[38] A quasigroup is called* **Moufang loop** *if any of the identities (4.2.4) hold.*

Definition 4.2.10 *[5] A* **left Bol loop** *is a loop that satisfies (4.2.5) and a* **right Bol loop** *if it satisfies (4.2.6) for a, b, c elements of the loop.*

$$a(b(ac)) = (a(ba))c \tag{4.2.5}$$

$$((ca)b)a = c((ab)a). \tag{4.2.6}$$

Definition 4.2.11 *Let Q be a loop such that for all $p, q \in Q$ it holds that*

$$q^{-1}(qp) = p = (pq)q^{-1}.$$

Then Q is said to be an **inverse property loop**, *or* **IP-loop**.

Example 4.2.12 *The order 7 Latin square below defines the smallest nongroup IP-loop.*

Definition 4.2.11 and Example 4.2.12 are from [20].

*	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	3	1	6	7	5	4
3	3	1	2	7	6	4	5
4	4	7	6	5	1	2	3
5	5	6	7	1	4	3	2
6	6	4	5	3	2	7	1
7	7	5	4	2	3	1	6

The inner mapping group of a loop can be defined as

Definition 4.2.13 *[31] Let Q be a loop with identity element e. The stabilizer of e is called the* **inner mapping group** *of Q. It is denoted by $I(Q)$.*

It is known that the notion of inner mapping group was first introduced by Bruck in [7]. The following gives two ways to generate the inner mapping group of a loop.

Proposition 4.2.14 *[17] Let Q be a loop. Then*

(a) $I(Q) = \langle R_x R_y R_{xy}^{-1}, R_x L_y R_{yx}^{-1} \mid x, y \in Q \rangle$.

(b) $I(Q) = \langle L_y R_y^{-1}, R_x R_y R_{xy}^{-1}, L_x L_y L_{yx}^{-1} \mid x, y \in Q \rangle$.

Let's look at the following examples.

Example 4.2.15 *If Q is a group, then $I(Q)$ is the inner automorphism of Q. Using Proposition 4.2.14 we compute*

$$e(xy)^{-1}yx = ey^{-1}x^{-1}yx = e \quad \text{if and only if} \quad xy = yx,$$
$$y(e)x^{-1}y^{-1}x = e \quad \text{if and only if} \quad xy^{-1} = y^{-1}x.$$

Example 4.2.16 *Consider the order 5 loop, L, given by the table in Example 4.2.6. The multiplication group of L is isomorphic to S_5 and the inner mapping group is isomorphic to S_4.*

We end this section with:

Proposition 4.2.17 *[17] In the loop Q, the subloop N is normal if and only if it is invariant under the action of* $\mathrm{Inn}(Q)$.

4.3 Multiplication Groups of Loops

In this section we will focus on some results about multiplication groups of loops, and piques. In classifying what groups are multiplication groups of loops, Theorem 4.3.10 shows that such groups are one with H-connected transversals (See Definition 1.1.16) for a subgroup H.

Definition 4.3.1 (H-connected) *[24] Let G be a group and $H \leq G$ and let A, B be two left transversals to H in G such that $[A, B] \leq H$, then A and B are said to be H-**connected**.*

Here $[A, B] = \{aba^{-1}b^{-1} \mid a \in A, b \in B\}$. In the case where $[A, A] \leq H$, we say A is H-selfconnected. We will denote by $L_G(H)$, the core of H in G (the largest normal subgroup of G contained in H). A formal definition is the following:

Definition 4.3.2 *[44] Let H be a subgroup of G. We say K is the* **core** *of the subgroup H, if K is the maximal subgroup of H such that $K \trianglelefteq G$. It is denoted $K = L_G(H)$.*

One can note that

$$L_G(H) = \bigcap_g H^g, \quad \text{where} \quad H^g = gHg^{-1}.$$

Example 4.3.3 *Let $G = D_8$ and $H = \langle r \rangle = \{1, r, r^2, r^3\}$, then the cosets of H are H and sH, and $A = \{r, s\}$ and $B = \{r^2, sr\}$ are two left transversals. We calculate $[A, B] = \{1, r^2\} \leq H$, i.e. A and B are H-connected.*
Now take $H = \{1, r^2, s, sr^2\} \cong V_4$, Klein four-group. The left costs are H and $rH = \{r, r^3, sr, sr^3\}$. Choosing $A = \{r^2, sr\}$ and $B = \{r, sr^2\}$ we get two left transversal and since $[A, B] = \{1, r^2\} \leq H$, we have H-connected left transversals. Also, in reference to Theorem 4.3.10 we note that $\langle A, B \rangle = G$, but $L_G(H) = H$, nontrivial.

Taking H to be the trivial subgroup in the above Example 4.3.3 will not work because in this case the only transversal will be the whole group G, and there is no way to get two H-connected transversal with this choice of H. The following example discusses when the choice of H being the trivial subgroup would work.

Example 4.3.4 *To illustrate take $G = \mathbb{Z}_5$, and take $H = \{1\}$, then the only transversal is $A = G$ in which case A is H-selfconnected. This only works for abelian groups. If G is nonabelian, then we can't get $[A, A] \leq \{e\}$. For instance, if H is the trivial subgroup of $G = D_8$, then taking $A = D_8$, it is clear that $[A, A] \not\leq H = \{e\}$.*

Lemma 4.3.5 *[31] Let $H \leq G$ and A and B be H-connected transversals. Let $C \subset A \cup B$ and $K = \langle H, C \rangle$. Then $C \subset L_G(K)$.*

Proof: Let $g \in G$ and $c \in C$, we will show that $g^{-1}cg \in K$ which will mean that $C \subset L_G(K)$. If $c \in A$, we can find $b \in B$ and $h \in H$ such that $g = bh$ and then $g^{-1}cg = h^{-1}b^{-1}cbh = h^{-1}(cc^{-1})b^{-1}cbh$. Since A and B are H-connected, we know that $c^{-1}b^{-1}cb \in H$ and therefore $g^{-1}cg \in K$, and so $C \subset L_G(K)$, as intended. □

We give the following example to illustrating Lemma 4.3.5.

Example 4.3.6 *Take G, H, A and B as in Example 4.3.3, in which we showed that A and B are H-connected transversal. Now pick $C = \{s\}$, then $K = G$ and we have $C \subset L_G(K) = G$. If instead we take $C = \{r\}$, then $K = H$ and we also get $C \subset L_G(K) = H$ in this case as well.*

Definition 4.3.7 *Let $(Q, \cdot, /, \backslash, e)$ be a pique. The stabilizer of a pointed idempotent element e is called the* **inner multiplication group** *of the pique. We write*

$$\mathrm{Inn}(Q) = \{\phi \in \mathrm{Mul}(Q) \mid \phi(e) = e\}.$$

Before looking at Lemma 4.3.9, consider the following example

Example 4.3.8 *Let Q be the loop given by the table below:*

Q	1	2	3	4	5
1	1	2	3	4	5
2	2	4	1	5	3
3	3	5	4	2	1
4	4	1	5	3	2
5	5	3	2	1	4

The multiplication group is $G = \mathrm{Mul}(Q) \cong S_5$. *Let* $H = I(Q) \cong S_4$, $A = \{L_1, \ldots, L_5\} \cong \{(1), (12453), (13425), (14352), (154)(23)\}$ *and let* $B = \{R_1, \ldots, R_5\} \cong \{(1), (124)(35), (13452), (14325), (15423)\}$. *We note that* $(12453) = (12)(2453) \in (12)H$, $(13425) = (13)(3425) \in (13)H$, $(14352) = (14)(4352) \in (14)H$, $(154)(23) = (15)(23)(45) \in (15)H$, *i.e.* A *is a left transversal. We can show that* B *is a left transversal in the same way. Now we calculate* $[A, B] = \{(1), (25)(34), (245), (23)(45), (234), (235), (354), (254), (24)(35)\} \leq H$.

Lemma 4.3.9 *[31] Let* Q *be a loop,* $G = \mathrm{Mul}(Q)$ *and* $H = I(Q)$ *be the multiplication and inner mapping groups of* Q*, respectively. Let* $A = \mathrm{LMul}(Q)$ *and* $B = \mathrm{RMul}(Q)$*, then* A *and* B *are* H*-connected left transversals in* G.

Proof: We first show that A is a left transversal of H in G. Let $L_p, L_q \in A$ for some $p, q \in Q$, we will show that L_p and L_q don't belong to the same coset of H. Suppose that $L_p, L_q \in gH$ for some $g \in G$, then $L_p = gh_1$ and $L_q = gh_2$ for some $h_1, h_2 \in H$. Let $e \in Q$ denote the identity element, then $h_1(e) = h_2(e) = e$. Now $L_p(e) = p = g(h_1(e)) = g(e)$ and similarly $L_q(e) = g(e)$, that means $p = q$. This shows that A is a left transversal. Similarly, B is a left transversal of H in G.

Now, we show that A and B are H-connected. Let $L_p \in A$, $R_q \in B$ for some $p, q \in Q$, we will show that $L_p^{-1}R_q^{-1}L_pR_q \in H$. That is, $L_p^{-1}R_q^{-1}L_pR_q$ fixes the identity. Calculate:

$$L_p^{-1}R_q^{-1}L_pR_q(e) = L_p^{-1}R_q^{-1}L_p(q) = L_p^{-1}R_q^{-1}(pq) = L_p^{-1}((pq)/q) = L_p^{-1}(p) = p\backslash p = e$$

i.e. $L_p^{-1}R_q^{-1}L_pR_q \in H$. Therefore $[A, B] \leq H$ and hence A and B are H-connected. □

Theorem 4.3.10 gives a necessary and sufficient conditions for a group to be the multiplication group of a loop.

Theorem 4.3.10 *[31] A group* G *is isomorphic to the multiplication group of a loop if and only if there exists a subgroup* H *satisfying* $L_G(H) = \{1_G\}$ *and* H*-connected transversals* A *and* B *satisfying* $G = \langle A, B \rangle$.

Proof: Lemma 4.3.9 and the fact that $\mathrm{Mul}(Q) = \langle A, B \rangle$ where A and B as in the referred-to lemma gives most of the forward direction. To show that $L_G(H) = \{1_G\}$, let

$1 < K \leq H$, we will show that K cannot be normal in G. Suppose K is normal in G, then for all $g \in G$ we have $gkg^{-1} \in K$, i.e. $g(k(g^{-1}(1_Q))) = 1_Q$. That is, for all $g \in G$, either $k(g^{-1}(1_Q)) = g^{-1}(1_Q)$ and k fixes $g^{-1}(1_Q)$ or $g \in I(Q)$. For $g \notin I(Q)$, k fixes $g^{-1}(1_Q)$ and as g ranges over all possible elements in $G/I(Q)$, $g^{-1}(1_Q)$ will range over all possible elements in Q, which means that k is the identity map. Thus, $L_G(H) = \{1_G\}$.

Now for the backward direction, let $H \leq G$ and let A and B be H-connected left transversals of H with $L_G(H) = \{1_G\}$ and $G = \langle A, B\rangle$. Since A is a left transversal we know that for any $g \in G$ there is exactly one $f(g) \in A$ such that $f(g)H = gH$, that is $g^{-1}f(g) \in H$. Let K be the set of left cosets of H and define the operation $*$ by $(g_1H) * (g_2H) = f(g_1)g_2H$.

We first show that this is a well-defined operation. Suppose $uH = xH$, $vH = yH$ in K i.e. $u^{-1}x \in H$ and $v^{-1}y \in H$. Then

$$uH * vH = f(u)vH \qquad \text{and} \qquad xH * yH = f(x)yH$$

We want to show $f(u)vH = f(x)yH$ which is equivalent to showing $(f(x)v)^{-1}f(x)y \in H$ keeping in mind that $f(x) = f(u)$, since both $f(x)$ and $f(u)$ are representatives of the same coset in the left transversal A. Since $(f(x)v)^{-1}f(x)y = v^{-1}f(x)^{-1}f(x)y = v^{-1}y \in H$ as $vH = yH$, the operation is well-defined.

Next, we show that $(K, *)$ is a quasigroup. Let g_1H, $g_2H \in K$ we want to find elements aH, $bH \in K$ such that $g_1H * aH = g_2H$ and $bH * g_1H = g_2H$ i.e. $f(g_1)aH = g_2H$ and $f(b)g_1H = g_2H$. Taking $a = [f(g_1)]^{-1}g_2$ solves the first. For the second equation, since $f(b) \in A$ and A is a left transversal, there is exactly one $f(b) \in A$ that satisfies $bH * g_1H = g_2H$. Therefore, K is a quasigroup under the operation $*$.

We now show that K is a loop. Let $h \in A$ be the representative of H. For $b \in B$, and given that A and B are H-connected, we have $hbh^{-1}b^{-1} \in H$, then $bh^{-1}b^{-1} \in H$. As b ranges over all possible elements in B, this forces $h = 1_G$ i.e. $1_G \in A$, therefore K is a loop; as $f(1) = 1$ is the representative of H in A.

Since B is also a left transversal, for each $x \in G$ there is exactly one $g(x) \in B$ such that $xH = g(x)H$, so $(xH) * (yH) = f(x)yH = f(x)g(y)H$. Since A and B are H-connected, it

follows $f(x)g(y)H = g(y)f(x)H$.

Finally, consider the action of G on K by left multiplication. Since $L_G(H) = \{1_G\}$, the kernel of the permutation representation corresponding to the action is trivial. Therefore, $\mathrm{Mul}(K) \cong G$. □

Let's look at the following example explaining why K in the proof of 4.3.10 is a quasi-group.

Example 4.3.11 *Let $G = S_4$, $H = S_3$. Suppose $K = \{H, (14)H, (24)H, (34)H\}$, and let $A = \{(1), (14), (24), (34)\}$. Take the operation $*$ as in the proof above. For g_1H, $g_2H \in K$ we want to find the unique aH and $bH \in K$ such that $g_1H * aH = g_2H$ and $g_1H * bH = g_2H$, i.e. $f(g_1)aH = g_2H$ and $f(b)g_1H = g_2H$. For the first we get $aH = [f(g_1)]^{-1}g_2H$ (on the left) and for the later see the table on the right*

	H	(14)H	(24)H	(34)H
H	a = (1)	(14)	(24)	(34)
(14)H	(14)	(1)	(24)	(34)
(24)H	(24)	(14)	(1)	(34)
(34)H	(34)	(14)	(24)	(1)

	H	(14)H	(24)H	(34)H
H	f(b)=(1)	(1)	(1)	(1)
(14)H	(14)	(1)	(24)	(34)
(24)H	(24)	(14)	(1)	(34)
(34)H	(34)	(14)	(24)	(1)

Note, the table to the left is representing $f(g_1)*g_2H$ and the one to the right is representing $g_1H * g_2H$.

Note that Theorem 4.3.10 and Example 4.3.3 ensure that D_8, and in fact all dihedral groups, cannot be the multiplication group of a loop. However, Example 4.3.13 shows that the dihedral group D_8 can be the multiplication group of a pique.

Example 4.3.12 *The multiplication group of the commutative pique whose table is given below is D_6. One can observe $L_1 = (23)$, $L_2 = (13)$ and $L_3 = (12)$ which generate D_6.*

	1	2	3
1	1	3	2
2	3	2	1
3	2	1	3

Example 4.3.13 *$P = (\mathbb{Z}_4, -)$ is a pique. Calculating its multiplication group yields* $\mathrm{Mul}(P) \cong D_8$. *See Example A.6.6 for the GAP calculation code.*

Remark 4.3.14 *In reference to the proof of 4.3.10, for every $x \in G$ there is exactly one $g(x) \in B$ such that $xH = g(x)H$. It follows that $(xH)*(yH) = f(x)yH = f(x)g(y)H$. Since A and B are H-connected, we have $f(x)g(y)H = g(y)f(x)H$ as $f(x)^{-1}g(y)^{-1}f(x)g(y) \in H$. We note that this does not automatically mean that $(xH) * (yH) = (yH) * (xH)$.*

The following is a consequence of Theorem 4.3.10.

Theorem 4.3.15 *[31] A group G is isomorphic to the multiplication group of a commutative loop if and only if there exists a subgroup H of G satisfying $L_G(H) = \{1_G\}$ and an H-selfconnected transversal A satisfying $G = \langle A \rangle$.*

Proof: Let H, A and B be as in Lemma 4.3.9, then since L is commutative $B = A$ it follows that A is an H-selfconnected transversal and $G = \langle A \rangle$. Further, $L_G(H) = \{1_G\}$ follows from the proof of Theorem 4.3.10.

For the backward direction, suppose G is a group with the given assumptions as in the statement of the theorem. The fact that G is the multiplication group of a loop K follows as in proof of Theorem 4.3.10. Now since $A = B$, Remark 4.3.14 ensures that K is a commutative loop. □

Theorem 4.3.16 *Let Q be a loop with a cyclic inner mapping group $I(Q)$. Then Q is an abelian group if one of the following holds:*

(i) Q is finite,

(ii) Q is a group,

(iii) $I(Q)$ is a p-group for a prime p.

Hence in all cases $I(Q)$ is trivial.

Theeorem 4.3.16 and its proof can be found in [31]. Another interesting fact about the multiplication groups of loops is the following:

Theorem 4.3.17 *[2] Let Q be a loop and let $G = \mathrm{Mul}(Q)$, then the center of Q is isomorphic to the center of G.*

We state the following theorem about the multiplication groups of a loop with the proof. For the definition of transitive and semiregular group actions see Definition 1.1.20.

Theorem 4.3.18 *[17] Let Q be a loop.*

(a) $\mathrm{RMul}(Q), \mathrm{LMul}(Q)$ *and* $\mathrm{Mul}(Q)$ *are transitive subgroups of* $S_{|Q|}$.

(b) Q *is a group if and only if* $\mathrm{RMul}(Q)$ *is semiregular.*

(c) Q *is an abelian group if and only if* $\mathrm{Mul}(Q)$ *is abelian.*

Proof:

(a) Since Q is a loop, it has an identity element $e \in Q$. The right and left multiplication actions by e gives the entire loop, Q. This shows transitivity.

(b) First assume that Q is a group. Consider the action of $\mathrm{RMul}(Q)$ on Q. For any $p, q \in Q$, if $R_q(x) = R_p(x)$ then $xq = xp$, multiplying by x^{-1} from the left yields $q = p$. This means there $\mathrm{RMul}(Q)$ acts on Q semiregularly. Conversely, consider the actions on the identity e of Q: $R_{pq}(e) = pq$ and $R_q(R_p(e)) = pq$. Since the action is semiregular it follows that $R_{pq} = R_q R_p$. Thus, for $x \in Q$ we have $R_{pq}(x) = R_q(R_p(x))$ which implies $x(pq) = (xp)q$. Thus, Q is associative and therefore is a group.

(c) The multiplication group of an abelian group is itself, which makes one side of this result immediate. Refer to Theorem 3.2.1. Conversely, suppose that $\mathrm{Mul}(Q)$ is abelian. Then the action of $\mathrm{Mul}(Q)$ on Q is transitive, and since it is abelian the action is regular. Thus, by (b) Q is a group and the map $\phi : Q \to \mathrm{RMul}(Q)$ defined by $\phi(q) = R_q$ is an isomorphism, therefore Q is an abelian group.

This completes the proof. □

The following theorem gives some interesting facts about the inner mapping group of a loop.

Theorem 4.3.19 *[24] Let Q be a quasigroup.*

(a) If Q is a group, then $I(Q)$ is the group of inner automorphisms.

(b) A loop Q is an abelian group if and only if $I(Q) = \{1\}$.

(c) If Q is a finite loop with $I(Q)$ a cyclic group, then Q is an abelian group.

Proof:

(a) Let Q be a group, and let $\phi \in I(Q)$, we will show that ϕ is a conjugation action, i.e. $\phi \in \mathrm{Inn}(Q)$. Since $I(Q)$ is the stabilizer of e, and $\phi \in I(Q)$, we have $\phi(e) = e$. The fact that $\phi \in I(Q) \subset \mathrm{Mul}(Q)$ allows us to write $\phi(x) = L_p(R_q(x))$ for some $p, q \in Q$. Put together, we conclude that $p = q^{-1}$, and $\phi(x) = q^{-1}xq$, i.e. $\phi \in \mathrm{Inn}(Q)$. This shows $I(Q) \subset \mathrm{Inn}(Q)$, and since we know $\mathrm{Inn}(Q) \subset I(Q)$, we conclude that $I(Q) = \mathrm{Inn}(Q)$, when Q is a group.

(b) Let Q be an abelian group and let $e \in Q$ denote the identity element. since the only element that stabilizes e is e itself, $I(Q)$ is the trivial subgroup. Conversely, suppose that $R_p(x) = y$ and $R_q(x) = y$, then $R_p^{-1} \circ R_q(x) = x$, i.e. $(xq)p^{\rho} = x$. This imply $xq = xp$, then $p = q$ after left multiplying by left inverse of x, x^{λ}. Thus, $\mathrm{RMul}(Q)$ is semiregular and thus Q is a group. By Proposition 4.2.14 we $I(Q) = \langle R_x R_y R_{xy}^{-1}, R_x L_y R_{yx}^{-1} \mid x, y \in Q \rangle$. But $I(Q) = \{1\}$, thus $y(yx)^{-1}x = e$ i.e. $(yx)^{-1} = y^{-1}x^{-1}$, i.e. $xy = yx$ for all $x, y \in Q$. Thus, Q is an abelian group.

(c) Let Q be a finite loop such that its inner mapping group, $I(Q)$, is cyclic. We want to show that Q is an abelian group. Let $e \in Q$ be the identity element of Q, and let $\phi \in I(Q)$ be a generator of $I(Q)$. We know that the identity map sends e to e. Let $k \leq |Q|$ be the smallest integer such that such that $\phi^k \in I(Q)$. Then $\phi^k(e) = e$, but

$\phi^k = \phi^{k-1} \circ \phi$, and $\phi(e) = e$, i.e. $\phi^{k-1}(e) = e$. This forces k to be zero, i.e. $I(Q)$ is trivial and therefore, Q is an abelian group.

Concluding the proof. □

The following give some conditions on when a loop is an abelian group.

Theorem 4.3.20 *[31] Let Q be a loop such that $I(Q)$ is a cyclic group. Then Q is an abelian group provided that at least one of the following conditions holds:*

1. *Q is finite.*
2. *Q is a group.*
3. *$I(Q)$ is a p-group for a prime p.*

Hence in all these cases $I(Q)$ is trivial.

We note that (i) follows from (c) and (ii) follows from (a) of Theorem 4.3.19. The proof is given in [31].

In [31] it was mentioned that all abelian groups are naturally isomorphic to multiplication groups of loops. It is also known that for $n \geq 5$ there exists a loop Q of order n such that $\mathrm{Mul}(Q) = S_n$ [22]. For $n \geq 6$ there exists an order n loop Q such that $\mathrm{Mul}(Q) = A_n$ [23]. The following theorem from [31] gives some conditions on groups that cannot be the multiplication groups of loops.

Theorem 4.3.21 *Let G be a group and let $H \leq G$ be nontrivial. Consider the following conditions:*

(1) $L_G(H)$ is nontrivial,

(2) $HZ(G) \leq N_G(H)$,

(3) H is a cyclic p-group or H is isomorphic to the Prüfer group ,

(4) H is cyclic.

Then if all proper nontrivial subgroups of G satisfies either (1), (2) or (3), G is not isomorphic to the multiplication group of a loop. If G is finite and every proper nontrivial subgroup

of G satisfies either (1), (2) or (4) then G is not isomorphic to the multiplication group of a loop.

A list of groups that are not isomorphic to the multiplication group of a loop are given in [31]. For example, the symmetric groups S_3 and S_4, the alternating group A_4 and the dihedral groups D_{2n} are among the groups that are not isomorphic to the multiplication group of a loop.

Example 4.3.22 *[31] The multiplication group of the loop given in the table below is an order 24 nonnilpotent group, which is isomorphic to $A_4 \times \mathbb{Z}_2$ according to GAP. The inner mapping group is isomorphic to the Klein's four group.*

$*$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	4	3	6	5
3	3	4	5	6	2	1
4	4	3	6	5	1	2
5	5	6	1	2	3	4
6	6	5	2	1	4	3

Example 4.3.23 *The table below defines a loop. A quick calculation shows that $\mathrm{Mul}(Q) \cong \mathbb{Z}_4$, which means that Q is isotopic to a reduced Latin square. Also, it is straightforward to verify that $I(Q)$ is the trivial subgroup. In fact, Q is a group that is isomorphic to $\mathbb{Z}_4$.*

Q	1	2	3	4
1	4	1	2	3
2	1	2	3	4
3	2	3	4	1
4	3	4	1	2

Example 4.3.24 *Consider $Q = (\mathbb{Z}_5, -)$. It defines a pique, with a single idempotent element, namely 0. $Q = (\mathbb{Z}_5, -)$ is generated by 1, as $0, 2, 3$ and 4 are respectively the solutions to $1 - x = 1, x - 1 = 1, x - 2 = 1$ and $x - 3 = 1$. Then $\mathrm{Mul}(Q) = \langle L_1, R_1 \mid L_1^2 = R_1^5 = R_0, R_1 L_1 = L_1 R_1^4 \rangle \cong D_{10}$. The stabilizer of 0 is the inner multiplication group $\mathrm{Inn}(Q) = \{\phi \in \mathrm{Mul}(Q) \mid \phi(0) = 0\} = \{L_0, R_0\} \cong \mathbb{Z}_2$. This agrees with 4.3.19(b).*

Example 4.3.25 *The Latin square given below is the multiplication table of a loop with* $e = 2$ *as its identity.*

*	1	2	3	4	5
1	3	1	4	5	2
2	1	2	3	4	5
3	5	3	1	2	4
4	2	4	5	1	3
5	4	5	2	3	1

The multiplication group of this quasigroup is $\mathrm{Mul}(Q) = \langle L_1, R_1 \rangle$ *with both generators has order five, which turns out to be isomorphic to* $\mathbb{Z}_5 \times \mathbb{Z}_5$. *To find* $I(Q)$, *we notice that* L_2 *and* $L_1 R_5$, *for example, are in* $I(Q)$, *but not* L_3. *Since* $\mathrm{Mul}(Q)$ *has order* 25, $I(Q)$ *must be an order 5 subgroup and is therefore isomorphic to* $\mathbb{Z}_5$.

Example 4.3.26 *Let* $Q = (\mathbb{Z}_6, -)$. *Then* $\mathrm{Mul}(Q) = \langle L_1, R_1 \mid L_1^2 = R_2^6 = R_0, R_1 L_1 = L_1 R_1^5 \rangle \cong D_{12}$, *and* $I(Q) = \{L_0, R_0\} \cong \mathbb{Z}_2$.

We end this section with the two questions:

Question 4.3.27 *Applying the natural operations on the multiplication table (Latin square) described in Section 3.3 we will possibly lose the loop structure, how does that change the multiplication group?*

Question 4.3.28 *Does any of the operations (or a combination of them) produce another loop? If so, are the multiplication groups isomorphic?*

4.3.1 Piques

Piques were defined in Definition 4.1.1. Having an idempotent element, not necessarily an identity element, one would like to know what of the results about loops can be generalized to piques? We know for example, that dihedral groups are isomorphic to the multiplication group of some pique, which is not true in the case of loops.

Example 4.3.29 *The Latin square given below is the multiplication table of a commutative idempotent quasigroup (it is also a pique) that is not a loop.*

Q	1	2	3	4	5
1	1	5	2	3	4
2	5	2	4	1	3
3	2	4	3	5	1
4	3	1	5	4	2
5	4	3	1	2	5

The multiplication group of this quasigroup is $\mathrm{Mul}(Q) = \langle L_1, L_2 \rangle$ *which, according to GAP, has ID* $[20, 3]$ *(General affine group). This group can be represented as* $\langle g, h \mid g^5 = h^4 = e, hg = g^2h \rangle$.

Example 4.3.30 *The following describes a way to construct an order* 4 *pique from a quasigroup of order* 3. *Consider the quasigroup:*

$*$	1	2	3
1	2	1	3
2	1	3	2
3	3	2	1

We can obtain a pique with an idempotent element $p = 4$ *by applying one of the six 4-cycles elements of* S_4. *The first row will be obtained by applying* (1234), *for instance, to the first entry,* 2, *which gives the first row to be:* 3 4 1 2. *Applying all six 4-cycles on the above table yield the following:*

3	4	1	2		4	3	1	2		4	1	3	2
2	3	4	1		2	4	3	1		3	2	4	1
4	1	2	3		1	2	4	3		2	4	1	3
1	2	3	4		3	1	2	4		1	3	2	4

1	3	4	2	3	1	4	2	1	4	3	2
3	4	2	1	4	2	3	1	4	3	2	1
4	2	1	3	1	4	2	3	2	1	4	3
2	1	3	4	2	3	1	4	3	2	1	4

We note that the multiplication group of the original quasigroup is isomorphic to S_3. The multiplication groups of all six order six piques are isomorphic to S_4.

In general, starting with an order n quasigroup (not necessarily a pique) we can obtain a pique of order $n+1$ by applying an n-cycle permutation on that quasigroup. The permutation is applied to the first entry of each row, and then the rest of the row is finished by finishing up the cycle. The above example illustrate how this is done. Obtaining such a quasigroup from a given quasigroup looks similar to the following:

Proposition 4.3.31 *Let Q be an idempotent quasigroup. By the addition of an identity element, 0, we can define a loop on the disjoint union $Q' = Q \cup \{0\}$ under the operation:*

$$x + y = \begin{cases} 0 & \text{if } x = y; \\ x \cdot y & \text{otherwise} \end{cases} \tag{4.3.1}$$

Example 4.3.32 *An idempotent quasigroup made into a loop with the addition of 0 as described in proposition 4.3.33.*

Q	1	2	3	4
1	1	3	4	2
2	4	2	1	3
3	2	4	3	1
4	3	1	2	4

Q'	0	1	2	3	4
0	0	1	2	3	4
1	1	0	3	4	2
2	2	4	0	1	3
3	3	2	4	0	1
4	4	3	1	2	0

The following result shows that this process indeed yields a loop.

Proposition 4.3.33 *[40] Let $Q' = Q \cup \{0\}$ where Q is an idempotent quasigroup Q. Define the multiplication on Q' by (4.3.1) in which $0 + x = x = x + 0$. Then $(Q', +, 0)$ defines a loop structure on Q'.*

Proof: Since Q is a quasigroup, its multiplication table is a Latin square. Constructing the multiplication table of Q' under the operation given in (4.3.1), we get a new table augmented by new row and new columns, both labeled 0. As per (4.3.1) the diagonal entries will all be 0. By the identity $0 + x = x = x + 0$, the first row and first column will both read $0, 1, 2, \ldots, n$. The diagonal entries in the table of Q will be moved to the first row/column. Thus, the new table we get is a reduced Latin square, which means that Q' is a loop. □

Example 4.3.34 *Let $Q = \mathbb{Z}_3$, then apply the 4-cycle (1234) to obtain the following order 4 pique*

	1	2	3	4
1	2	3	4	1
2	3	4	1	2
3	4	1	2	3
4	1	2	3	4

Piques seems to generalize the notion of loops, a lot of interesting questions raise about piques and how we can generalize what we know about loops to piques. Here are three of many questions:

Question 4.3.35 *D_8 can't be isomorphic to the multiplication group of a loop but is isomorphic to the multiplication group of a pique. Are there other such groups that cannot be multiplication groups of a loop but would work for a pique?*

Question 4.3.36 *How is the multiplication group of a quasigroup changed when we use the construction described in Example 4.3.30 to create a pique from it?*

Question 4.3.37 *Is it possible to to generalize the construction method described in Proposition 4.3.31 to construct a pique with a desired number of idempotents?*

Chapter 5

Looking Back, Looking Forward

5.1 Summary

Quasigroups are algebraic structures in which divisibility is always defined. In this thesis we investigated quasigroups by studying their multiplication groups. We showed that there are some quasigroups, Q_n, that possess similar substructure as groups. We also proved that some groups have multiplication groups isomorphic to their direct products, and then generalized that to say that the multiplication group of a group is its central product. This thesis also showed that some non-isomorphic quasigroups share the same multiplication group, some share the same left multiplication group and other quasigroups share the same right multiplication group. We studied the multiplication groups of quasigroups based on their structures and also by viewing them as the counterpart of Latin squares and showed ways to generate the multiplication group of a quasigroup by looking at their multiplication tables. We also showed that when applying natural operations on a Latin square such as row swapping, column swapping, transposing or entry relabeling, the multiplication group of the corresponding quasigroup also undergoes predictable changes; more specifically we provided a way to relate the multiplication group of the quasigroup whose table is obtained by row swapping, column swapping, transposing or entry relabeling.

Although this thesis focused on a lot of different things, the example of the family of quasigroups Q_n is one to highlight. This family of quasigroups mimic the cyclic groups in sharing a lot of similar properties. For example, Q_n is generated by a single element, $\omega = e^{2i\pi/n}$, and it has exactly one subquasigroup of order k where k is a divisor of the order of Q_n. In Theorem 3.2.15 we showed that Q_n has a left multiplication group that is isomorphic to $\mathbb{Z}_n$. The subquasigroups of Q_n turns out to be Lagrangean (Theorem 2.4.16), and when $|Q_n| = p^k m$ where p is a prime number, coprime to m, then Q_n has a Sylow p-subquasigroup.

5.2 List of Results

Theorem (2.1.10) *Let $Q = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$ be the set comprised of the nth roots of unity. Then Q is a quasigroup under the operation $a \circ b = \overline{a}b$.*

Theorem (2.1.11) *Let $Q = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$ be the set of nth roots of unity. Define $*$ on Q by $a * b = a\bar{b}$ for all $a, b \in Q$. Then Q is a quasigroup. Furthermore, the multiplication table of $(Q, *)$ is the transpose of that of $(Q, \circ)$ given in Theorem 2.1.10.*

Theorem (2.2.3) *A subquasigroup H of a group G is a subgroup of G.*

Theorem (2.2.8) *Let Q_n be the quasigroup consisting of the nth roots of unity together with the binary operation $a \circ b = \bar{a}b$, for $a, b \in Q_n$. Then Q_n has exactly one subquasigroup with k elements for every k that divides n. Furthermore, these are all the subquasigroups of Q_n.*

Theorem (2.4.16) *Let $Q = (Q_n, \circ)$ where for $a, b \in Q_n$, we have $a \circ b = \bar{a}b$. Then, the subquasigroups of Q are all right Lagrangean.*

Corollary (2.4.17) *Let $Q = (Q_n, \circ)$ where for $a, b \in Q_n$, we have $a \circ b = \bar{a}b$. Then the subquasigroups of Q_n are left Lagrangean, and therefore Lagrangean in Q.*

Corollary (2.4.26) *Let Q be as in Theorem 2.4.16. If $n = p^k \cdot m$ for a prime p coprime with m, then Q contains a Sylow p-subquasigroup.*

Theorem (3.1.7) Let Q be a quasigroup. Then

1. If Q is a commutative quasigroup, then $\mathrm{LMul}(Q) = \mathrm{Mul}(Q)$.
2. If Q is not commutative, then M is a nonabelian group

Theorem (3.1.14) *Let $Q_n = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$ equipped with the operation $\circ$ defined for $a, b \in Q_n$ by $a \circ b = \bar{a}b$. Let $\mathrm{Mul}(Q_n)$ be the multiplication group of Q_n, then*

$$\mathrm{Mul}(Q_n) \cong D_{2n}.$$

Theorem (3.2.2) *Let G and H be group. Let $\mathrm{LMul}(G)$ and $\mathrm{LMul}(H)$ be their left multiplication groups, respectively. Suppose $\mathrm{LMul}(G) \cong \mathrm{LMul}(H)$, then $G \cong H$.*

Theorem (3.2.3) *Let G and H be group. Let $\mathrm{RMul}(G)$ and $\mathrm{RMul}(H)$ be their right multiplication groups, respectively. Suppose $\mathrm{RMul}(G) \cong \mathrm{RMul}(H)$, then $G \cong H$.*

Theorem (3.2.7) *Let G be a finitely generated group with generators $g_1, g_2, \ldots, g_k$. The multiplication group of G is generated by L_{g_i}, R_{g_i} for $i = 1, 2, \ldots, k$, where L_{g_i} and R_{g_i} respectively denote the left and right multiplications by the element g_i.*

Corollary (3.2.8) *The relation between the generators of a finitely generated group G will be translated to relations in the generators of $\mathrm{Mul}(G)$.*

Theorem (3.2.11) *Let $n \geq 3$ be an odd integer. The multiplication group of $G = D_{2n}$ is $M = D_{2n} \times D_{2n}$.*

Theorem (3.2.13) *Let n be a positive integer, and let $G = D_{2n}$, then the multiplication group of G is $\mathrm{Mul}(G) = (D_{2n} \times D_{2n})/Z(G)$.*

Corollary (3.2.14) *Let $G = D_{2n}$, then*

$$\mathrm{LMul}(G) \cong \mathrm{RMul}(G) \cong G.$$

Theorem (3.2.15) *Let $Q = Q_n$ equipped with the operation defined for $a, b \in Q_n$ by $a \circ b = \bar{a}b$. Then*

$$\mathrm{LMul}(Q) \cong \mathbb{Z}_n \quad \textit{and} \quad \mathrm{RMul}(Q) \cong D_{2n}$$

Theorem (3.2.16) *Let G be a finite group with a trivial center, $Z(G) = \{e\}$. Let $\mathcal{M} = \mathrm{Mul}(G)$ be the multiplication group of G. Then*

$$\mathcal{M} \cong G \times G.$$

Theorem (3.2.19) *Let G be a finite group with center $Z = Z(G)$, and let $\mathcal{M} = \mathrm{Mul}(G)$. Then*

$$\mathcal{M} \cong G \circ G.$$

Theorem (3.2.20) *Let G be a finite group and let $H \trianglelefteq G$. Let $\mathcal{M} = \mathrm{Mul}(G)$ and let $\mathcal{N} = \mathrm{Mul}_G(H)$, then $\mathcal{N} \trianglelefteq \mathcal{M}$.*

Theorem (3.3.5) Let Q be a finite quasigroup with multiplication group $\mathrm{Mul}(Q)$. Let ϕ be a permutation, and let P be the quasigroup whose multiplication table is obtained from that of Q after swapping the rows according to ϕ. Then, the multiplication Group of P, $\mathcal{M} = \mathrm{Mul}(P)$, is generated by $L_{\phi(q)}$ and $R_q \cdot \phi$ where $q \in Q$.

Corollary (3.3.6) *Swapping two or more rows of the multiplication table of a quasigroup does not change the left multiplication group.*

Theorem (3.3.9) *Let Q be a finite quasigroup with multiplication group* $\mathrm{Mul}(Q)$. *Let ϕ be a permutation, and let P be the quasigroup whose multiplication table is obtained from that of Q after swapping the columns according to ϕ. Then, the multiplication Group of P,*

$\mathcal{M} = \mathrm{Mul}(P)$, *is generated by* $L_q \cdot \phi$ *and* $R_{\phi(q)}$ *where* $q \in Q$.

Corollary (3.3.10) *Swapping two or more columns of the multiplication table of a quasigroup does not change the right multiplication group.*

Theorem (3.3.11) *Let* $\phi \in S_n$, *and let* Q *be a quasigroup with Latin square* S. *Let* P *be the quasigroup whose Latin square is obtained from* S *after applying* ϕ *entry-wise to* S. *Then* $\mathrm{Mul}(P) = \langle \phi L_q, \phi R_q \rangle$.

Theorem (3.4.4) *Let* Q *be a quasigroup, and let* $P = Q_{(23)}$. *Then, the left multiplication group of* P *is isomorphic to the left multiplication of* Q.

Theorem (3.4.5) *Let* Q *be a quasigroup, and let* $P = Q_{(123)}$. *Then, the right multiplication group of* P *is isomorphic to the left multiplication of* Q.

Theorem (3.4.6) *Let* Q *be a quasigroup, and let* P *be the quasigroup whose Latin square is the transpose of that of* Q. *Then* $\mathrm{LMul}(P) \cong \mathrm{LMul}(Q)$, $\mathrm{RMul}(P) \cong \mathrm{RMul}(Q)$, *and* $\mathrm{Mul}(P) \cong \mathrm{Mul}(Q)$.

Corollary (3.4.7) *Let* Q *be a quasigroup. Then the right and left multiplication groups of* Q *and its five conjugates are at most three different groups up to isomorphism.*

Theorem (3.4.13) *Let* $Q = (Q_n, \circ)$ *with the usual operation where for* $a, b \in Q_n$, *we define* $a \circ b = \bar{a}b$. *Then*

$$\mathrm{MidMul}(Q) \cong \mathrm{LMul}(Q) \cong \mathbb{Z}_n.$$

5.3 Future Work

Throughout this thesis, we were able to answer many interesting questions, but there are many more that we would like to know the answer to.

The family of quasigroups Q_n was of special interest for the many similarities it shares with the family of cyclic groups. We would still like to know if we can relate the Q_n's using direct products or semidirect products (Question 2.5.9). Another possible question is whether we can do the same with other quasigroups (Question 2.5.10).

In Subsection 3.1.2, we showed that $\mathrm{Mul}(Q_n) \cong D_{2n}$; it would be good to know if there are any other quasigroup with D_{2n} as their multiplication group (Question 3.1.15). The more general question of characterizing all possible quasigroups with a fixed multiplication group is bound to be a lot more challenging (Question 3.1.16).

In Theorem 3.2.20, we showed that normality gets carried over to the multiplication group; can the same thing be said about loops and their normal subloops? (Question 4.1.8).

In Section 3.4, it was shown that up to isomorphism a quasigroup and its conjugates can have up to three distinct groups as their left and right multiplication groups. What can we say about these groups? Alternatively, picking three permutation groups can we find a quasigroup that will have this choice of groups as the right and left multiplication groups of its six conjugates? (Question 3.4.8)

Piques, as defined in Chapter 4, are quasigroups with an idempotent element. It is clear that every loop is a pique, a question might be how can the multiplication groups of piques and loops be related? Example 4.3.13 shows that D_8 can be the multiplication group of a pique. However, it is well-known that it can't be the multiplication group of a loop. Are there other such groups? (Question 4.3.35) What other results can or can't be generalized from the theory of loops to piques? Also, how is the multiplication group of a quasigroup changed when we construct a pique from it using the method described in Section 4.3.1? (Question 4.3.36) And finally, it would be interesting to figure out whether it is possible to generalize the construction method described in Proposition 4.3.31 to construct a pique with

a desired number of idempotents (Question 4.3.37).

Section 3.3 shows how the multiplication group of a Latin square (or rather the quasigroup defined by that Latin square) after applying an operation like row swapping, for instance, is related to the multiplication group of the original Latin square. Can this be generalized to all isotopies? How would that help in trying to get a better understanding of the conjugates of a given quasigroup? (Question 3.4.10) Also, can we use these ideas to construct a the multiplication table of a loop from that of another loop? (Question 4.3.28) How does that effect the multiplication group? (Question 4.3.27)

I look forward to continuing to work on these and similar problems in the near future.

Appendix A

Implementing GAP and SageMath to Help with Identifying the Multiplication Groups

A.1 What is SageMath?

SageMath (previously Sage or SAGE, "System for Algebra and Geometry Experimentation") is a computer algebra system with features covering many aspects of mathematics, including algebra, combinatorics, graph theory, numerical analysis, number theory, calculus and statistics.

A.2 On Using SageMath

Appealing to technology, I first used SageMath to calculate things like the order of a group, to generate group, character tables among other things.

Example A.2.1 *One can call any of the groups in the built-in library of the SageMath, and you can ask the software for the order of the group. The codes below will respectively generate a permutation group with the given generators, the symmetric group in five letters, and the alternating group in six letters.*

```
sage: G = PermutationGroup([[(1,2),(3,4)], [(1,2,3,4)]])
sage: G.order()
8
sage: P = PermutationGroup([[(1,2),(3,4)], [(1,2,3)]])
```

```
sage: P.order()
12
sage: D = DihedralGroup(6)
sage: D.order()
12
sage: H = SymmetricGroup(5)
sage: H.order()
120
sage: K = groups.presentation.Alternating(6)
Finitely presented group < a, b | a^3, b^5, (a*b)^4, (a*b^-1*a^-1*b)^2,
(b*a^-1*b^-1*a^-1)^3 >
sage: K.order()
360
```

It is also possible to generate things like the list of elements, the multiplication table of the group, the order of each of the elements, etc...

Example A.2.2 *Here is how one can generate the multiplication table. First, we import "Operation Table" library using the command*

```
sage: from sage.matrix.operation_table import OperationTable
```

Then, using the group P from example A.2.1, we generate the multiplication table of a group

```
sage: T = OperationTable(P, operation = operator.mul)
```

```
*  a b c d e f g h i j k l
 +-----------------------
a| a b c d e f g h i j k l
b| b a d c h j i e g f l k
c| c e f i g a b j l k h d
d| d h j g i b a f k l e c
e| e c i f j k l g b a d h
f| f g a l b c e k d h j i
g| g f l a k h d b e c i j
h| h d g j f l k i a b c e
i| i j k b l e c a h d g f
j| j i b k a d h l c e f g
k| k l e h c i j d f g a b
l| l k h e d g f c j i b a
```

Example A.2.3 *Also, SageMath allows you to get a latex code to copy and paste in your latex document.*

```
sage: T._latex_()
{\\setlength{\\arraycolsep}{2ex}\n\\begin{array}{r|*{12}{r}}\n\\
multicolumn{1}{c|}{\\ast}&a&b&c&d&e&f&g&h&i&j&k&l\\\\\\
```

```
\hline\n{}a&a&b&c&d&e&f&g&h&i&j&k&l
\\\\\n{}b&b&a&d&c&h&j&i&e&g&f&l&k\\\\\n{}c&c&e&f&i&g&a&b&j&l&k&h&d\\\\\n{}
d&d&h&j&g&i&b&a&f&k&l&e&c\\\\\n{}e&e&c&i&f&j&k&l&g&b&a&d&h\\\\\n{}
f&f&g&a&l&b&c&e&k&d&h&j&i\\\\\n{}g&g&f&l&a&k&h&d&b&e&c&i&j\\\\\
n{}h&h&d&g&j&f&l&k&i&a&b&c&e
\\\\\n{}i&i&j&k&b&l&e&c&a&h&d&g&f\\\\\n{}j&j&i&b&k&a&d&h&l&c&e&f&g\\\\\n{}
k&k&l&e&h&c&i&j&d&f&g&a&b\\\\\n{}l&l&k&h&e&d&g&f&c&j&i&b&a\\\\\n\\end{array}}'
```

Example A.2.4 *One can get some information about the group. For example, SageMath will tell you whether a group is abelian or not, it also gives the order of the group, and it lists the elements of the group.*

```
sage: D.is_abelian()
False
sage: D.order()
12
sage: elements = D.list()

[(),
 (1,6)(2,5)(3,4),
 (1,2,3,4,5,6),
 (1,5)(2,4),
 (2,6)(3,5),
 (1,3,5)(2,4,6),
 (1,4)(2,3)(5,6),
 (1,6,5,4,3,2),
 (1,4)(2,5)(3,6),
 (1,2)(3,6)(4,5),
 (1,5,3)(2,6,4),
 (1,3)(4,6)]
```

You can also call a specific element and finds its order

```
sage: d=elements[3]
sage: d.order()
2
```

Also, you can ask if a group is simple or not

```
AlternatingGroup(5).is_simple()
True
sage: SymmetricGroup(5).is_simple()
False
```

Example A.2.5 *The subgroup generated by one or more elements can be found by*

```
sage: D.subgroup([e])
Subgroup of (Dihedral group of order 12 as a permutation group) generated
by [(1,6,5,4,3,2)]
sage: K.subgroup([k,k2])
Group([ b^-1*a*b*a, b^-1*a^-1*b ])
```

Example A.2.6 *Quotient groups*

```
sage: K.subgroup([k,k2])
Group([ b^-1*a*b*a, b^-1*a^-1*b ])
sage: A4 = AlternatingGroup(4)
sage: r1 = A4("(1,2) (3,4)")
sage: r2 = A4("(1,3) (2,4)")
sage: r3 = A4("(1,4) (2,3)")
sage: L = A4.subgroup([r1, r2, r3])
sage: A4.quotient(L)
Permutation Group with generators [(1,2,3)]
```

Example A.2.7 *We can also generate a conjugacy class containing a specified element*

```
sage: g = G((1,2,3,4))
sage: G = SymmetricGroup(6)
sage: g = G((1,2,3,4))
sage: G.conjugacy_class(g)
Conjugacy class of cycle type [4, 1, 1] in Symmetric group of order 6! as a permutation
```

All the representatives of the conjugacy classes can be generated using the code

```
sage: G = SymmetricGroup(6)
sage: G.conjugacy_classes_representatives()

[(),
 (1,2),
 (1,2)(3,4),
 (1,2)(3,4)(5,6),
 (1,2,3),
 (1,2,3)(4,5),
 (1,2,3)(4,5,6),
 (1,2,3,4),
 (1,2,3,4)(5,6),
 (1,2,3,4,5),
 (1,2,3,4,5,6)]
```

A.3 What is GAP?

GAP is a system for computational discrete algebra, with particular emphasis on Computational Group Theory. GAP provides a programming language, a library of thousands of functions implementing algebraic algorithms written in the GAP language as well as large data libraries of algebraic objects. See also the overview and the description of the mathematical capabilities. GAP is used in research and teaching for studying groups and their representations, rings, vector spaces, algebras, combinatorial structures, and more. The system, including source, is distributed freely. You can study and easily modify or extend it for your special use.

Reference: https://www.gap-system.org [15]

A.4 Using GAP Through SageMath

At first, I used GAP through SageMath mostly for identifying groups using the GAP function `Id.Group(G)`. *An example follows*

Example A.4.1 *In the SageMath interface, you follow the command below to define a group and then identify the group using the GAP index.*

```
sage: G = gap('Group((1,2,3)(4,5), (3,4))')
sage: G.IdGroup()
[ 120, 34 ]
sage: G.Order()
120
```

This was my first step in using GAP, and later I used the GAP software to define groups using generators and relations. For example, the dihedral group $D_8 = \langle r, s \mid r^4 = s^2 = 1, rs = sr^{-1} \rangle$. *We can define a group in the same way (without knowing the actual group to start with) and then using Id.Group to identify the group.*

Example A.4.2 *We define a "free group" in gap with two generators, and then we define a new group as a quotient using the relations that we calculated.*

```
gap> f := FreeGroup("a", "b");;
gap> f;
<free group on the generators [ a, b ]>
gap> g := f/[f.1^4, f.2^2, (f.2*f.1^3)^2];
<fp group on the generators [ a, b ]>
gap> IdGroup(g);
[ 8, 3 ]
```

There are references where one can look and find the name of this specific group for most of the small groups. The group indexed [8, 3] is the dihedral group of order 8 defined above, D_8.

The following example is an example that I calculated the relation for myself as part of the research

Example A.4.3 *In the problem that we are working on in my research we are trying to understand the multiplication groups for groups that are finitely represented by generators and relation, like D_8. If a group has two generator, the multiplication group (at least the ones we considered so far) has four generators. Here is how we used gap feeding it the relations based on its four generators.*

```
f := FreeGroup("a", "b", "c", "d");;
gap> g := f/[f.1^4, f.2^2, f.3^4, f.4^2, f.3^3*f.1^3*f.3*f.1, f.4*f.1^3*f.4*f.1,
f.3^3*f.2*f.3*f.2, (f.4*f.2)^2, (f.2*f.1)^3, (f.3*f.4)^3];
<fp group on the generators [ a, b, c, d ]>
gap> IdGroup(g);
[ 576, 8653 ]
```

A.5 Calculating in GAP Using the Loops Package

The Loops Package, if not found in pkg/loops in the main directory, can be downloaded and added to there. To use the loops package one needs to call the command line below. This can be done anytime, it need not be called at the beginning of the GAP session.

```
gap> LoadPackage("loops");
```

Once loaded, the package can be used, among other things, for defining loops, calculating their multiplication group and other such things.

Example A.5.1 *Here is an example showing how to define a quasigroup or a loop using their multiplication table.*

```
gap> table_1 := [[2,1,3],[1,3,2],[3,2,1]];;
gap> Q:= QuasigroupByCayleyTable(table_1);;
gap> IsQuasigroup(Q);
true
```

The "IsQuasigroup" checks whether the input is a quasigroup or not. The command "MultiplicationTable" returns the rows of the multiplication table of the quasigroup Q.

```
gap> MultiplicationTable(Q);
[ [ 2, 1, 3 ], [ 1, 3, 2 ], [ 3, 2, 1 ] ]
```

Defining a loop from a Cayley table will return an error if the table is reduced.

```
L := LoopByCayleyTable(table_1);;
Error, LOOPS: <1> must be a normalized latin square.
```

When the table is reduced, we get something like

```
L := LoopByCayleyTable(table_2);;
gap> IsLoop(L);
true
```

Many other thing can be done in GAP. For example Section A.6 gives examples on how GAP is used to calculate the multiplication group, and how to recognize it using the "IdGroup" command.

A.6 Some Examples Calculations

This section will show the different ways GAP was used to do some of the calculations in this thesis.

Example A.6.1 *One way to define a group in GAP is to use the FreeGroup command. The multiplication group of D_6 (Example 3.2.6) was calculated as follow:*

```
gap> f := FreeGroup( "a", "b", "c", "d" );;
G := f/[f.1^3, f.2^2, f.3^3, f.4^2, (f.2*f.1^2)^2, f.3^2*f.1^2*f.3*f.1,
f.4*f.1^2*f.4*f.1, f.3^2*f.2*f.3*f.2, (f.4*f.2)^2, (f.4*f.3^2)^2];
gap> IdGroup(G);
[ 36, 10 ]
```

Note here $f.1 = L_r, f.2 = L_2, f.3 = R_r$ and $f.4 = R_s$. The multiplication group $\mathrm{Mul}(G)$ *has GAP-Id* $[36, 10]$ *which is the GAP Id of $D_6 \times D_6$. GAP ID for $S_4 \times S_4$ is of $G = S_4$ is* $[576, 8653]$.

The code used for calculating $\mathrm{Mul}(D_{10})$ *(Example 3.2.9) is*

```
f := FreeGroup( ""a", "b", "c", "d" );;
H := f/[f.1^5, f.2^2, f.3^5, f.4^2, (f.2*f.1^4)^2, f.3^4*f.1^4*f.3*f.1,
f.4*f.1^4*f.4*f.1, f.3^4*f.2*f.3*f.2, (f.4*f.2)^2, (f.4*f.3^4)^2];
gap> IdGroup(H);
[ 100, 13 ]
```

Next we look at D_8:

Example A.6.2 *The code for calculating* $\mathrm{Mul}(D_8)$ *(Example 3.2.12).*

```
gap> f := FreeGroup( "a", "b", "c", "d" );;
G := f/[f.1^4, f.2^2, f.3^4, f.4^2, (f.2*f.1^3)^2, f.3^3*f.1^3*f.3*f.1,
f.4*f.1^3*f.4*f.1, f.3^3*f.2*f.3*f.2, (f.4*f.2)^2, (f.4*f.3^3)^2, f.1^2*f.3^2];;
gap> IdGroup(G);
[ 32, 49 ]
```

The calculations for the twist of $\mathbb{Z}_5$ in Example 3.3.3 are given in the following example.

Example A.6.3 *For* $\mathcal{M}_1 = \mathrm{Mul}(\mathbb{Z}_5^1)$*:*

```
gap> f := FreeGroup(2);
g := f/[f.1^5, f.2^2, (f.2*f.1)^2];
gap> IdGroup(g);
[ 10, 1 ].
```

For $\mathcal{M}_2 = \mathrm{Mul}(\mathbb{Z}_5^2)$*: In GAP,*

```
gap> f := FreeGroup(2);
g := f/[f.1^5, f.2^4, f.2^3*f.1^2*f.2*f.1];
gap> IdGroup(g);
[ 20, 3 ].
```

The calculations for Example 3.3.4 are given below:

Example A.6.4 $M_2 = \langle L_1, R_1 \mid L_1^7 = R_1^6 = L_0, R_1L_1 = L_1^5R_1\rangle \cong (\mathbb{Z}_7 \rtimes \mathbb{Z}_3) \rtimes \mathbb{Z}_2$

```
gap> f:= FreeGroup(2);
<free group on the generators [ f1, f2 ]>
gap> g:= f/[f.1^7,f.2^6,f.2^5*f.1^2*f.2*f.1];;
gap> IdGroup(g);
[ 42, 1 ].
```

$\mathbb{Z}_7^3$ *has the multiplication group* $M_3 = \langle L_1, R_1 \mid L_1^7 = R_1^3 = L_0, R_1L_1 = L_1^4R_1\rangle \cong \mathbb{Z}_7 \rtimes \mathbb{Z}_9$

```
gap> p:=SemidirectProduct(au,n);;
gap> g:=f/[f.1^7,f.2^3,f.2^2*f.1^3*f.2*f.1];;
gap> IdGroup(g);
[ 21, 1 ].
```

- $\mathbb{Z}_7^4$ *has the multiplication group* $M_4 = \langle L_1, R_1 \mid L_1^7 = R_1^6 = L_0, R_1L_1 = L_1^3R_1\rangle \cong (\mathbb{Z}_7 \rtimes \mathbb{Z}_3) \rtimes \mathbb{Z}_2$.

```
gap> g:= f/[f.1^7,f.2^6,f.2^5*f.1^4*f.2*f.1];;
gap> IdGroup(g);
[ 42, 1 ].
```

- $\mathbb{Z}_7^5$ *has the multiplication group* $M_5 = \langle L_1, R_1 \mid L_1^7 = R_1^3 = L_0, R_1L_1 = L_1^2R_1\rangle \cong \mathbb{Z}_7 \rtimes \mathbb{Z}_3$

```
gap> g:= f/[f.1^7,f.2^3,f.2^2*f.1^5*f.2*f.1];;
gap> IdGroup(g);
[ 21, 1 ].
```

- ${\mathbb{Z}_7}^6$ *has the multiplication group* $M_6 \cong \mathbb{Z}_7$.

Here are the calculations for Example 3.3.8

Example A.6.5 *The multiplication group calculated according to Theorem3.3.5*

$$\mathrm{Mul}(P) \cong \langle L_{\phi(1)}, L_{\phi(2)}, L_{\phi(3)}, L_{\phi(4)}, R_1 \cdot (123), R_2 \cdot (123), R_3 \cdot (123), R_4 \cdot (123) \rangle$$

is generated by $= L_2 = (1234), L_{\phi(2)} = L_3 = (13)(24), L_{\phi(3)} = L_1 = (1), L_{\phi(4)} = L_4 = (1432)$ *and* $R_1 \cdot (123) = (123), R_2 \cdot (123) = (1234)(123) = (1324), R_3 \cdot (123) = (13)(24)(123) = (142), R_4 \cdot (123) = (1432)(123) = (34)$.

```
gap> gen := [(1,2,3,4), (1,3)(2,4), (1,4,3,2),
                (1,2,3), (1,3,2,4), (1,4,2), (3,4)];;
gap> G := Group(gen);;
gap> IdGroup(G);
    [ 24, 12 ]
```

Calculating directly (using the L_p *and* R_p *where* p *is a generator of* P*):*

```
gap> Q := QuasigroupByCayleyTable([[3,4,1,2],[1,2,3,4],[2,3,4,1],[4,1,2,3]]);;
gap> M := MultiplicationGroup(Q);; IdGroup(M);
    [ 24, 12 ]
```

[24, 12] is the GAP Id of S_4.

Calculating the multiplication group for P *from Example 4.3.13.*

Example A.6.6
```
gap> tab1 := [[1,4,3,2], [2,1,4,3], [3,2,1,4], [4,3,2,1]];;
gap> Qtab1:= QuasigroupByCayleyTable(tab1);;
gap> M := MultiplicationGroup(Qtab1);;
gap> IdGroup(M);;
[ 8, 3 ]
```
That shows theat $\mathrm{Mul}(P) \cong D_8$.

Bibliography

[1] *P. R. J. ÖSTERGARD A. HULPKE, P. KASKI. The number of latin squares of order 11. 80(274):1197–1219, 2011.* 2

[2] *A. A. Albert. Quasigroups i.* Transactions of the American Mathematical Society, *54(3):507–519, 1943.* 13, 14, 28, 74, 86

[3] *A. A. Albert. Quasigroups ii.* Transactions of the American Mathematical Society, *55(3):401–419, 1944.* 13, 74

[4] *A. C. Atkinson and R. A. Bailey. One hundred years of the design of experiments on and off the pages of biometrika.* Biometrika, *88(1):53–97, 2001.* 12

[5] *G. Bol. Gewebe und gruppen.* Mathematische Annalen, *114(1):414–431, 1937.* 78

[6] *R. H. Bruck. Some results in the theory of quasigroups.* Transactions of the American Mathematical Society, *55(1):19–52, 1944.* 26, 39

[7] *R. H. Bruck. A survey of binary systems. 1966.* 22, 74, 79

[8] *J. H. Dinitz C. J. Colbourn.* Handbook of combinatorial designs. *Chapman & Hall/-Taylor & Francis, 2 edition, 2007.* 3

[9] *Ramiro Carrillo-Catalán, Marina Rasskazova, and Liudmila Sabinina. Malcev algebras corresponding to smooth almost left automorphic Moufang loops.* J. Algebra Appl., *17(12):1850232, 10, 2018.* 13

[10] *L. Stemkoski D. Klyve. Graeco-latin squares and a mistaken conjecture of euler.* College Mathematics Journal, *37(1):2–15, 08 2006.* 12

[11] *Phullendu Das. Isotopy of abelian quasigroups. 63(2):317–323, 1977.* 29

[12] *D. S. Dummit and R. M. Foote.* Abstract algebra. Third edn. *ohn Wiley & Sons, 2004.* 4, 7, 17

[13] *G. N. Garrison. Quasi-groups.* Annals of Mathematics, *4(3):474–487, 1940.* 13, 26

[14] *D. Gorenstein.* Finite groups. Second edn. *Chelsea Publishing Co., 1980.* 8

[15] *The GAP Group. Gap reference manual, release 4.11.1, 2021.* 105

[16] *D. Guichard. An introduction to combinatorics and graph theory, 2022.* 2, 4

[17] *J. I. Hall.* Moufang loops and groups with triality are essentially the same thing. *Memoirs of the American Mathematical Society, 1947-6221 ; volume 260, number 1252. American Mathematical Society, Providence, RI, 2019.* 74, 79, 86

[18] *Mohammad Hassanzadeh and Serkan Sütlü. Matched pairs of m-invertible hopf quasigroups.* Quasigroups & Related Systems, *28(1), 2020.* 39

[19] *T. Ihringer. On multiplication groups of quasigroups.* Pacific J. Math, *5:13711–141, 1984.* 44

[20] *A. Asif J. Slaney. Generating loops with the inverse property.* CICM Workshop on Empirically Successful Automated Reasoning in Mathematics, ESARM 2008, *378:55–66, 2008.* 78

[21] *J. D. H. Smith K. W. Johnson. Characters of finite quasigroups.* European Journal of Combinatorics, *5(1):43–50, 1984.* 37

[22] *A. Donald Keedwell and József Dénes. Chapter 6 - connections between latin squares and magic squares. In A. Donald Keedwell and József Dénes, editors,* Latin Squares and their Applications (Second Edition), *pages 205–234. North-Holland, Boston, second edition edition, 2015.* 3, 12, 23, 88

[23] *Tomáš Kepka and Drápal Aleš. Alternating groups and latin squares.* European Journal of Combinatorics, *10(2):175–180, 1989.* 88

[24] *Tomáš Kepka and Markku Niemenmaa. On loops with cyclic inner mapping groups.* Archiv der Mathematik, *60:233–236, 03 1993.* 80, 87

[25] *Charles R. Leedham-Green and Susan Mckay. The structure of groups of prime power order. 2002.* 8

[26] *Charles C. Lindner. Quasigroups orthogonal to a given abelian group. 14(1):117, 1971.* 23

[27] *M. A. M. Lynch. Generating quasigroups: a group theory investigation.* International Journal of Mathematical Education in Science and Technology, *42(6):806–812, 2011.* 22

[28] *I. L. Chuang M. A. Nielsen.* Quantum Computation and Quantum Information. *Cambridge University Press., 2002.* 9

[29] *J. D. H. Smith M. K. Kinyon and Petr Vojtěchovský. Sylow theory for quasigroups ii: Sectional action.* Journal of Combinatorial Designs, *23(3):159–184, 2017.* 7

[30] *D. C. Murdoch. Quasi-groups which satisfy certain generalized associative laws.* American Journal of Mathematics, *61(2):509–522, 08 1939.* 13, 18, 39

[31] *Markku Niemenmaa and Tomas Kepka. On multiplication groups of loops.* Journal of Algebra, *135:112–122, 11 1990.* 79, 81, 82, 85, 86, 88, 89

[32] *H. O. Pflugfelder. Historical notes on loop theory. 41(2):359–370, 2000.* 12, 14, 28

[33] *J. Pieprzyk S. Bakhtiari, R. Safavi-Naini. A message authentication code based on latin squares. volume 1270, pages 194–203, 01 1997.* 12

[34] *Ali Sagheer and Makarim Abdul-Jabbar. Error correcting code using latin square.* Journal of AL-Anbar University for Pure Science, ISSN 1991-8941, *2, 01 2008.* 12

[35] *E. Schröder.* Lehrbuch der Arithmetik und Algebra fur Lehrer und Studirende. *Leipzig, B. G. Teubner, 1890.* 13

[36] *E. Schröder.* Vorlesungen über die algebra der logik (exakte logik). *Leipzig, B. G. Teubner, 1890.* 13

[37] *V. Shcherbacov.* Quasigroups in cryptology, `arXiv:1007.3572`. *2012.* 12

[38] *V. Shcherbacov.* Elements of quasigroup theory and applications. *Monographs and research notes in mathematics. CRC Press, Taylor & Francis Group, Boca Raton, FL, 2017.* 5, 14, 39, 41, 69, 70, 71, 74, 77, 78

[39] *J. D. H. Smith. Quasigroups and quandles.* Discrete Mathematics, *1-3(109):277–282, 1992.* 72

[40] *J. D. H. Smith.* An Introduction To Quasigroups and Their Representations. *Chapman & Hall/CRC, 2006.* 18, 27, 28, 29, 30, 64, 65, 75, 93

[41] *J. D. H. Smith. Four lectures on quasigroup representations, 2007.* 18, 39

[42] *J. D. H. Smith. Sylow theory for quasigroups.* Journal of Combinatorial Designs, *23(3):115–133, 2008.* 17, 32, 34, 35, 36

[43] *J. D. H. Smith. Homotopies of central quasigroups.* Communications in Algebra, *40(5):1878–1885, 2012.* 30, 31

[44] *M. Suzuki.* Group theory. *Grundlehren der mathematischen Wissenschaften ; 247-248. Springer-Verlag, Berlin ;, 1982.* 80

[45] *George Teseleanu. Cryptographic symmetric structures based on quasigroups.* Cryptologia, *pages 1–28, 2022.* 13

[46] *J. H. van Lint and R. M. Wilson.* A Course in Combinatorics. *Cambridge University Press, 2 edition, 2001.* 2

[47] *D. W. Wall. Sub-quasigroups of finite quasigroups.* Pacific J. Math, *7(4):1711–1714, 1957.* 25, 26

[48] *W. D. Wallis and J. C. George. Introduction to combinatorics.* CRC Press, *10(2):212, 2011.* 2

[49] Wikipedia. Quasigroup. 22, 72, 75

[50] R. Wilson. Combinatorics : Ancient & Modern. *Oxford Scholarship Online, Oxford, 2013.* 11, 12