5-2021

Algebraic Structures and Variations: From Latin Squares to Lie Quasigroups

Erik Flinn
eflinn@nmu.edu

Algebraic Structures and Variations: From Latin Squares to Lie Quasigroups

By

Erik Flinn

THESIS

Submitted to

Northern Michigan University

In partial fulfillment of the requirements

For the degree of

MASTER OF SCIENCE

Office of Graduate Education and Research

May 2021

SIGNATURE APPROVAL FORM

ALGEBRAIC STRUCTURES AND VARIATIONS: FROM LATIN SQUARES TO LIE QUASIGROUPS

This thesis by Erik Flinn is recommended for approval by the student's Thesis Committee, the Department Head of the Department of Mathematics and Computer Science, and the Dean of Graduate Education and Research.

Date 4/1/21

Committee Chair: Daniel Rowe, Assistant Professor

Date 4-1-21

First Reader: J.D. Phillips, Professor, Department Head

Joshua Thompson Date 4/1/21

Second Reader: Joshua Thompson, Associate Professor

Date 4-1-21

Department Head: J.D. Phillips

Lisa Eckert Date 04/15/2021

Dean of Graduate Education and Research: Dr. Lisa Eckert

ABSTRACT

Algebraic Structures and Variations: From Latin Squares to Lie Quasigroups

By

Erik Flinn

In this Master's Thesis we give an overview of the algebraic structure of sets with a single binary operation. Specifically, we are interested in quasigroups and loops and their historical connection with Latin squares; considering them in both finite and continuous variations. We also consider various mappings between such algebraic objects and utilize matrix representations to give a negative conclusion to a question concerning isotopies in the case of quasigroups.

DEDICATION

For my family and all the friends I've made along the way. Thank you!

ACKNOWLEDGMENTS

I express my sincerest gratitude for the exceptional support of the Faculty in the Computer Science and Mathematics Department at Northern Michigan University. Whether I have taken a course with them or not, there has always been words that they have said, or advice they have given me to inspire to work harder and be better than I already am.

Of course I am honored to have Dr. Phillips be my department head and begin to guide me towards the exciting worlds that algebra has to offer. However, being fully advised under Dr. Rowe has been an incredible opportunity to re-visualize and in certain cases even re-contextualize my understanding of the things I thought I knew. To them, and to both of my advisors of my teaching responsibilities, Dr. Lawton and Dr. Thompson, I owe an immense debt of gratitude.

I would also like to thank my fellow peers within the graduate program in this department. I never felt like I truly had a group in which I belonged until I met all of them, and it is paramount to me that I acknowledge how much their support has meant to me over the last two years.

And finally, the support given to me by my family, especially my mother, is a treasured asset. I know since none of them are mathematicians, that this will not make much sense after this point, so I want to let you all know here: I could not have done this without all that you have done for me over the course of my life.

Citations are done in Chicago Style.

TABLE OF CONTENTS

List of Figures

SYMBOLS AND ABBREVIATIONS

$\in$	Signifies an element is contained within...
$\exists$	Short hand for "There exists"
$\forall$	Short hand meaning "for all"
s.t.	Short hand meaning "such that"
$\cong$	Signifies Isomorphic Relation
$\approx$	Signifies Isotopic Relation
$\longrightarrow$	Short hand for "Maps to"
$\leq$	Is a Subset of
$\subseteq$	Set contained in Set
$\leftrightarrow$	Equivalence of two statements
$\mathbb{R}$	Real Numbers

1 Introduction

The world of algebra is one filled with beauty. One that we are unable to see until we learn enough to gain a greater understanding and comprehension of it all. And yet, in this beauty, we become too focused. Eventually we lose the forest for the trees. Undergraduate mathematics curriculum will often strongly consider, above any other algebraic structure, the idea of a group. Groups are well structured, well-researched, interesting and rather incredible when you stop to consider it. The very first math we learn as kids, to add and subtract whole numbers, is indicative of a group, the integers under addition. Everything from that addition through complex calculus is us merely observing the structure created by specific groups.

Sometimes, the undergraduate will also get a small sample of some furthered structured algebraic objects, for example rings and ideals, but there is seldom time in the undergraduate curriculum to consider algebras with less structure then the ones aforementioned. That being comprised of magmas, quasigroups, semigroups, loops, and so on. In fact, these structures as a whole have received much less attention from mathematicians themselves, and the work that has been done is often scattered and sometimes even repeated.

This leads, in some cases, to some mathematicians thinking of these structures as near incomprehensible objects, despite being more simplistic in nature than the ones they have already mastered. Considering how important the concept of generalizing is to mathematics, the concepts of these "lesser" algebras, their definitions, and certain theorems pertaining to them should be better systemized, summarized, and presented somewhere in totality. This thesis does not seek to detail every last theorem concerning these structures, however, it does aim to give a comprehensive overview of some important concepts to these algebraic structures. This is in an attempt to give the reader a fundamental understanding of the larger algebraic world than merely groups.

We shall summarize key algebras with less structure than or equal structure to a group, define mappings between algebraic structures, relating them to other objects such as Latin squares, and give an introduction to Lie Theory and how we can begin to generalize the axioms of Lie Group into something resembling what could be considered a "Lie Quasigroup". Along the way, we plan to report on the solutions to various research problems that were considered, such as a negative result, via counter example, concerning a question involving isotopies of finite quasigroups.

2 Groups

2.1 Introduction.

Definition 2.1. A *Group* (G, $\cdot$) is a non-empty set, closed under a binary operation, satisfying the axioms listed below. However, the operation symbol will often omitted for simplicity.

1. *Identity*: There is an element e, where operating it with an element on either side results in the same element.

   i.e. for $x \in$ G: $ex = xe = x$

2. *Associativity*: Rearranging the parantheses in a given expression does not change the outcome.

   i.e. for $a, b, c \in$ G: $a(bc) = (ab)c$

3. *Inverse*: For each element, a, there exists an element, a^{-1} such that the operation of it with a, on either side, is equal to the identity element.

   i.e. $\forall$ $a \in$ G: $\exists$ $a^{-1} \in$ G s.t. $a^{-1}a = aa^{-1} = e$

There has been extensive research written about groups which we will not discuss here, however, there are key elements of the theory of groups to highlight for our purposes moving forward. We will be defining important terms, key concepts, and specific groups that will be important for this work.

2.2 Key Terms and Concepts.

To start, we refer to the size, or number of elements a group has, as its *order*. While groups can contain an infinite number of elements, such as the integers under addition $(\mathbb{Z}, +)$, the groups and other algebraic structures we consider will be finite in size in the first portion of this thesis.

Definition 2.2. The *order* of a particular element, is the number of times that element operates on itself to reach the identity. For example, if m is the smallest integer s.t. $a^m = e$, then a has order m.

Definition 2.3. A group (H) is a *subgroup* ($H \leq G$) if:

1. H is a subset of G (i.e. $H \subseteq G$)

2. H is closed under the group operation.

3. Every element in H has an inverse in H.

   i.e. $\forall\, h \in H \Rightarrow h^{-1} \in H$

Based on these axioms, each group has at least two subgroups called the *trivial subgroup*, where $H = \{e\}$, and the whole group, $H = G$.

Another important class of subgroups are *normal subgroups* ($N \leq G$):

$$N = \{n \in G \,|\, gng^{-1} \in N \;\forall\, g \in G \text{ and } n \in N\}.$$

or the *center of a group* ($Z(G)$):

$$Z(G) = \{z \in G \,|\, gz = zg \;\forall\, g \in G\}.$$

The above property of the center of a group is that the elements of $Z(G)$ *commute* with the elements of G. Meaning that the order in which you perform the group operation on any two elements yields the same product.

A group itself will be called *commutative* if for all $x, y \in G$: $xy = yx$.

2.3 Basic Examples of Groups.

Definition 2.4. A *permutation* is a different ordering of the elements of a set. These are the basis for many other groups we will discuss below:

1. *Symmetric Groups*: Denoted S_n, are groups of all permutations of n elements. Every S_n has order $n!$ and every finite group is equivalent to some subgroup of S_n.

2. *Cyclic Groups*: Denoted C_n are groups generated by a single element. They are also denoted $\mathbb{Z}_n$.

$C_n =< a >= \{e, a, a^2, ..., a^{n-1}\}$ when n is the order of a and is the order of the group itself.

3. *Permutation Groups*: Subgroups of S_n via Cayley's Theorem, which states all finite groups, G are equivalent to some subgroup of S_n with order n.

4. *Abelian Groups* Groups satisfying the commutative property, meaning that $\forall$ a, b $\in G$, $ab = ba$

5. *Dihedral Groups*: Denoted: D_n for the n-gon, groups representing the symmetries of a particular polygon, generated by a single rotation($\rho = \frac{2\pi}{n}$) and a reflection, R.

   $D_n =< \rho, R \mid \rho^n = 1, R^2 = 1, R\rho = \rho^{-1}R >$

   Has order $2n$. Note: n is the number of sides/vertices of the polygon.

2.4 Cayley Tables of Groups.

Definition 2.5. A *Cayley table*, named after Arthur Cayley, describes the structure of an underlying algebraic object by arranging all potential products of the elements with respect to the group operation.

The outer border of the table is arranged such that every element is mentioned once in the outer column and outer row, and the interior is filled in to represent the binary operation between those elements, where the element rc is contained in the r^{th} row and c^{th} column. We can use Cayley tables to represent groups.

	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

Figure 1: An example of a Cayley table representing C_5

Observe, that in row two, column three that $ab = c$, or row three, column five: $bd = a$. The row is the first letter mentioned in the operation, followed by the letter representing the column.

Some examples of groups expressed as Cayley tables are written below:

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Figure 2: Cayley table of $\mathbb{Z}_3$

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Figure 3: Klein-Four Group (K_4)

We can also use numbers in place of letters, often with 1 as the identity element.

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

Figure 4: Also $\mathbb{Z}_3$

Cayley tables have different restrictions corresponding to the algebraic structure they represent. We will see examples of this in the section 3.

2.5 Mappings of Groups.

2.5.1 Homomorphisms.

Definition 2.6. A *mapping*, f, is a function from a set, A_1 to another set A_2. Often denoted:

$$f\colon A_1 \longrightarrow A_2 \text{ read as "} f \text{ maps } A_1 \text{ to } A_2 \text{".}$$

A map f will be:

1. Injective (One-to-One): $\forall\, a, b \in A_1$ if $f(a) = f(b)$, then $a = b$.

   This means that every element $a \in A_1$ maps to a unique element $f(a) \in A_2$

2. Surjectivie (Onto): $\forall\, b \in A_2$, $\exists\, a \in A_1$ s.t. $f(a) = b$.

   This means, that every element in the set A_2 has at least one corresponding element in A_1.

Definition 2.7. Any map f is called, *bijective*, if it is both injective and surjective.

Defintion 2.8. A *homomorphism* between two groups $f\colon (G_1, \cdot) \longrightarrow (G_2, \circ)$ is a mapping that satisfies the following:

$$f(a) \circ f(b) = f(a \cdot b)$$

Note there may be different group operations for G_1 and G_2 and they are therefore denoted differently.

Definition 2.9. An *isomorphism* is defined as a bijective homomorphism. We will then say that two groups are *isomorphic* ($G_1 \cong G_2$) if there exists at least one isomorphism between them.

For groups, the idea of an isomorphism is often used as a notion of equivalence, meaning that the structures of the two isomorphic groups should be considered as the same.

2.5.2 Permutations and the Symmetric Group.

Permutations of a finite set are bijections, or reorderings, of the elements of a given set. For example, if you wanted to permute the items $a, b, c \in A_1$ you could make them $b, a, c \in A_2$ by simply swapping the first and second elements. This is also a mapping from A_1 to A_2 via the permuation P, denoted $(a\ b)$:

$$a \longrightarrow b$$

$$b \longrightarrow a$$

$$c \longrightarrow c$$

And any permutation falls into one of the following categories:

1. Transpositions: Swapping any two elements $(a\ b)$

2. Simple Transpositions: Swapping two consecutive elements $(a\ a+1)$

3. k-Cycles: k elements are mapped in a cycle of length k.

   For example: $(a\ b\ c\ d)$ would be a 4 cycle in which:

$$
\begin{aligned}
a &\longrightarrow b \\
b &\longrightarrow c \\
c &\longrightarrow d \\
d &\longrightarrow a
\end{aligned}
$$

Having a cycle of n elements generates the group C_n we mentioned earlier. Meanwhile the combination of cycles and transpositions is what generates a Symmetric group S_n or one of its subgroups, depending on which of the permutations are used.

Theorem 2.1 *Any cycle can be written as a product of transpositions.*

Proof

If $k = 1$ a 1-cycle can be written as $(a_i) = (a_i\ a_{i+1})\ (a_{i+1}\ a_i)$.

if $k \geq 2$, then: $(a_1\ a_2 \cdots a_k)$ = $(a_1\ a_k)\ (a_1\ a_{k-1}) \cdots (a_1\ a_3)\ (a_1\ a_2)$. ■

Theorem 2.2 *Any transposition can be rewritten as a product of of simple transpositions.*

Proof Any $(a\ b)$ can be expressed as:

$\big(a\,(a+1)\big)\big((a+1)\,(a+2)\big) \cdots \big((b-1)\,b\big)\big((b-1)\,(b-2)\big) \cdots \big((a+2)\,(a+1)\big)\big((a+1)\,a\big)$ ■

Corollary 2.2.1 *Any cycle can be written as a product of simple transpositions.*

Proof

Combine theorem 2.1 and 2.2. ■

Corollary 2.2.2 *S_n is generated by simple transpositions.*

Proof

Any permutation in S_n can be written as product of disjoint cycles. Any cycle can be rewritten as a product of simple transpositions, therefore S_n is generated by simple transpositions. ■

Building on this, one of the most fundamental and important theorems in the theory of groups is Cayley's theorem.

Theorem 2.3 *Every group, G of order n is isomorphic to a subgroup of S_n*

Proof Let G be a group of order n. We will then define the map:

$$f_g : G \longrightarrow G \text{ s.t. } x \rightarrow gx, \text{ where } x, g \in G$$

Since f is defined as an operation between two elements, it has a simple to find inverse:

$$f_g^{-1} : G \longrightarrow G \text{ s.t. } x \rightarrow g^{-1}x, \text{ where } x, g^{-1} \in G$$

Therefore f_g acts as a permutation on G, meaning f_g is a member of S_n.

We can then define a group $H = \{f_g \mid g \in G\} \subseteq S_n$. And a map, $T : G \longrightarrow S_n$ such that $T(g) = f_g$.

T is a homomorphism:

$$f_g \cdot f_{g'} = f_g\Big(f_{g'}(x)\Big) = fg(g'x) = gg'x = f_{gg'}(x)$$

for all $x \in G$, therefore:

$$T(g \cdot g') = T(g)T(g')$$

T is injective since $gx = g'x$ implies $g = g'$.

Therefore, G is isomorphic to the image of T which is H itself.

$$G \cong H \subseteq S_n \text{ ■}$$

Since G is isomorphic to a subgroup of S_n, and S_n is generated by transpositions. Thus, any finite group is generated by simple transpositions.

3 Sets with a Single Binary Operation

An binary operation that turns a set into a group endows that set with a great deal of structure, so much so that many mathematicians have spent their entire academic careers studying groups. It is also interesting, however, to consider and discuss less-structured algebraic objects, such as magmas, semigroups and quasigroups and loops.

3.1 Magmas.

Definition 3.1. A *magma* (M, ·) is defined as a non-empty set closed under a binary operation. They are also well known as *groupoids* in some sources. Magmas are the algebraic objects that contain very little structure. As a result, Cayley tables of magmas have no additional properties.

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

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

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

Figure 5: Examples of magmas

All of the Cayley tables above are representative of various magmas, but may or may not be representative of any other algebraic structure in particular. For instance, the first is the cyclic-3 group.

Some magmas we will discuss that have additional structure include:

1. *Semigroups*: Magmas with associativity

2. *Monoids*: Semigroups with a two-sided identity element

3. *Quasigroups*: Magmas with the property that $x \cdot y = z$ has a unique solution given knowledge of any two.

4. *Loops*: Quasigroups that contain a two-sided identity element

5. *Groups*: Associative loops

3.2 Semigroups and Monoids.

Definition 3.2. A *semigroup* $(S,\cdot)$ is a set closed under a binary operation satisfying the associative law: $(a\cdot b)\cdot c = a\cdot(b\cdot c)$. While more structured than a basic magma, a semigroup lacks the identity element and inverses that we commonly have with groups.

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

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

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

Figure 6: Examples of semigroups

Definition 3.3. A *monoid* is a semigroup that also contains a two-sided identity element. The first of the three above is also an example of a monoid.

3.3 Quasigroups.

A quasigroup can be defined as a magma, where knowledge of any two elements in the equation $x\cdot y = z$, will uniquely determine the third. This however, was not how quasigroups were first defined. Birkhoff was the first mathematician to formally define a quasigroup.

Defintion 3.4. See Birkhoff.[1] A *Quasigroup* $(Q,\cdot,\ \backslash,/)$ is a set closed under three different binary operations, referred to as multiplication $(\cdot)$, left division $(\backslash)$ and right division$(/)$ satisfying the conditions:

1. $x\cdot(x\backslash y) = y$

2. $(y/x)\cdot x = y$

3. $x\backslash(x\cdot y) = y$

4. $(y\cdot x)/x = y$

[1] Garrett Birkhoff, *Lattice Theory* (American Mathematical Society 307 Colloquium Publications, 1948), ISBN: 978-0-8218-1025-5.

5. $x/(y\backslash x) = y$

6. $(x/y)\backslash x = y$

However, two of these (5) and (6) may be removed for simplicity.

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

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

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

Figure 7: Examples of Quasigroups

The above Cayley tables are all examples of quasigroups. Notice how satisfying the axioms of a quasigroup have caused each element to occur once in each column and once in each row.

In fact the only thing it gains as opposed to a magma, is the ability to divide by elements on either side. Since it lacks the associative property, however, it means the operation of division needs to be defined twice. Once for division on the left, and once for division on the right.

There are different definitions for quasigroups[2] that help better understand the underlying structure. For instance, we can define a *quasigroup* (Q, ·) as a set with a single binary operation where for $a, b \in$ Q, there exists unique solutions $x, y \in$ Q to the equations:

$$ax = b$$

$$ya = b$$

Or put simply, a *quasigroup* is a set under a binary operation where knowledge of any two elements in the equation $xy = z$ uniquely determines the third.

Under this definition, since there is no division operation on either side, mathematicians will often define a map for multiplication on the right and left. The following is the mappings for a quasigroup Q.

[2] JD Phillips D.I. Pushkashub A.V. Shcherbacovc V.A. Shcherbacov, "On Birkhoff's Quasigroup Axioms," *Journal of Algebra* 457 (2016): 7–17, https://doi.org/10.1016/j.jalgebra.2016.02.024.

$$R_x : x \longrightarrow xg \text{ for some } g \in Q$$

$$L_x : x \longrightarrow gx \text{ for some } g \in Q$$

Given this definition, it is easy to define the inverse mappings.

$$R_x^{-1} : xg \longrightarrow x \text{ for some } g \in Q$$

$$L_x^{-1} : gx \longrightarrow x \text{ for some } g \in Q$$

This is how we can define quasigroups in terms of a single operation. The afformentioned second and third operations from Birkhoff's defintion are represented in terms of the mappings R_x^{-1} and L_x^{-1}.

3.4 Loops and Loop Varieties.

Definition 3.5. A *loop* is a quasigroup that has a two-sided identity element. Notice that a loop may still lack associativity. The first of the Cayley tables in Figure 7 is representative of a loop where 2 is the identity element.

This makes a loop closer to having the structure of a group, missing only the associative law. There are many variaties of loops satisfying weaker associative properties with special names.[3]

Definition 3.6. A *Bol loop* $(L, \cdot)$ is a loop satisfying either of the two laws:

1. $a \cdot (b \cdot (a \cdot c)) = (a \cdot (b \cdot a)) \cdot c$ for each $a, b, c \in L$. (right Bol loop law).

2. $((c \cdot a) \cdot b) \cdot a = c \cdot ((a \cdot b) \cdot a)$ for each $a, b, c \in L$ (left Bol loop law).

[3] J. D. Phillips and Petr Vojtechovsky, "The Varieties of Loops of Bol-Moufang Type," *Algebra Universe* 54 (2005): 259–271, https://doi.org/10.1007/s00012-005-1941-1.

Definition 3.7. A *Moufang loop* $(L, \cdot)$ is a loop that is both a left and right Bol loop. Equivalently, a Moufang Loop is a loop satisfying any one of the four equivalent identities:

1. $a \cdot (b \cdot (a \cdot c)) = ((a \cdot b) \cdot a) \cdot c$
2. $c \cdot (a \cdot (b \cdot a)) = ((c \cdot a) \cdot b) \cdot a$
3. $(a \cdot b) \cdot (c \cdot a) = a \cdot ((b \cdot c) \cdot a)$
4. $(a \cdot b) \cdot (c \cdot a) = (a \cdot (b \cdot c)) \cdot a$

This means that if a loop satisfies one of the above axioms, then it will satisfy the other 3. For example:

(3) ⇒ (4): Assume that (3) is true.

$$(a \cdot b) \cdot (c \cdot a) = a \cdot ((b \cdot c) \cdot a)$$

And let $c = e$:

$$(a \cdot b) \cdot a = a \cdot (b \cdot a)$$

This means that our loop satisfies the *flexible law*. Thus we can redistribute the parantheses on $a \cdot ((b \cdot c) \cdot a)$ since it both begins and ends in a.

$$(a \cdot b) \cdot (c \cdot a) = a \cdot ((b \cdot c) \cdot a) = (a \cdot ((b \cdot c)) \cdot a$$

Which is the fourth axiom.

Additionally, if a loop is a Moufang loop, inverses are necessarily two-sided.

Another common loop is what is referred to as a C-loop.

Definition 3.8. A *C-loop* is a loop satisfying the following axiom:

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

The loops that most closely resemble groups however, are *extra loops*, hilariously being named for being Moufang loops with extra properties.

Definition 3.9. An *extra loop* is a Moufang loop that is also conjugacy closed, otherwise referred to as a CC-loop. Equivalently one could say an extra loop must satisfy any one of the following identities:

1. $(x \cdot (y \cdot z)) \cdot y = (x \cdot y) \cdot (z \cdot y)$
2. $(y \cdot z) \cdot (y \cdot x) = y \cdot ((z \cdot y) \cdot x)$
3. $((x \cdot y) \cdot z) \cdot x = x \cdot (y \cdot (z \cdot x))$

And once again if a given algebraic object satisfies one of those axioms it implies that it satisfies the others.

3.5 Maps of Algebraic Structures.

In addition to homomorphisms, we can define other restrictions on maps that will result in a different relationship between two algebraic objects. The following map I'll discuss in a loosening of the conditions that define homomorphisms and isomorphisms.

Definition 3.10. A *homotopism*, which is a collection of three maps λ, τ, ι from a set with a binary operation $(A_1, \cdot)$ to another $(A_2, \circ)$ with the following property:

$$\lambda(a) \circ \tau(b) = \iota(a \cdot b)$$

The above definition is a generalization of a homorphism. A homomorphism is a homotopism, where:

$$\lambda = \tau = \iota.$$

Definition 3.11. Following similar conventions, an *isotopism* is defined as a homotopism where all three of the mappings are bijective. We will then say two sets with binary operations are *isotopic* $\big((A_1, \cdot) \approx (A_2, \circ)\big)$ if there exists at least one isotopism between them.

Lets consider some isotopies of the following Quasigroup:

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

Figure 8: Our Base four element quasigroup, Q

In which the mappings are the following permutations:

$$\lambda = (1\ 2)(3)(4)$$

$$\tau = (1\ 2\ 3)(4)$$

$$\iota = (1\ 2\ 3\ 4)$$

Notice through this example that:

$$\lambda \leftrightarrow \text{Permutation of the Left Border}$$

$$\tau \leftrightarrow \text{Permutations of the Top Border}$$

$$\iota \leftrightarrow \text{Permutations of the products}$$

Therefore, applying λ yields the quasigroup:

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

Figure 9: $\lambda(Q)$

Then applying τ will give us:

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

Figure 10: $\tau\lambda(Q)$

And finally, ι:

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

Figure 11: $\iota\tau\lambda(Q)$

Note, that since these operations each function as independent permutations of the table, it is equivalent to doing the transformations in any order.

Finally, we can revisualize the λ and τ Operations in terms of the products by moving the entire row or column affiliated with the bordering element.

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

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

Figure 12: Two equivalent ways of expressing a Cayley table

Both represent the same quasigroup despite the interior being different since the corresponding binary operations are the same.

4 Latin Squares

Definition 4.1. A *Latin square* is an $n \times n$ matrix, where the numbers... $\{(1,2,..n)\}$ occur exactly once in each column and row.

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

Figure 13: General $n \times n$ Latin square

4.1 Latin Squares and Algebraic Structures.

4.1.1 Latin Squares and Quasigroups.

If we give these Latin squares a bordering, we will have a Cayley table representation of some algebraic structure. Though it may seem like a departure from quasigroups, there is actually an equivalence between the concept of a Latin square and finite quasigroups. For the purposes of this demonstration we will therefore only be discussing finite quasigroups.

$$\begin{array}{c|cccc} & 1 & 2 & \cdots & \text{n} \\ \hline 1 & a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \text{n} & a_{n1} & a_{n2} & \cdots & a_{nn} \end{array}$$

Figure 14: A bordered Latin square that determines a quasigroup

One final definition of a quasigroup, therefore, is a finite set whose internal Cayley table is represented by a Latin square. The borders of that Cayley table are the elements of the quasigroup. This definition is most commonly referred to as a combinatorial defintion of quasigroups.

Theorem 4.1 *Every Cayley table of a finite quasigroup is a Latin square and conversely, any Latin square with a bordering is representation a of a quasigroup.*

Proof

Let (a_1, a_2, ... , a_n) be the elements of the quasigroup, (Q, $\cdot$) with its Cayley table expressed below. The entry a_{rs} refers to the element that occurs in the r-th row of the s-th column and represents the product $a_r a_s \in$ Q. If the same entry occurred twice in row r, say in both columns: s and t, meaning: $a_{rs} = a_{rt} = b$. Therefore, we would have two solutions to the equation $a_r x = b$ which is a contradiction to our definition of quasigroups. Similarly, if the same entry occurred twice in the column s, we would have two solutions to the equation $ya_s = c$ for some $c \in$ Q.

Thus, the conclusion is that each element of the quasigroup occurs exactly once in each row and once in each column of the unbordered Cayley table (which is an $n \times n$ lattice) is a Latin square. ■

Additionally, a quasigroup has more than one affiliated Cayley table, since it is possible to permute the rows and columns of the table along with their bordered counterparts. Therefore it is possible to represent a given quasigroup with multiple Latin squares, or conversely, a given Latin square defines the Cayley table for more than one quasigroup, subject to different borderings.

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

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

Figure 15: Both tables represent the same quasigroup

The only difference between them, is that the Latin square/bordering are given in a different way. However, they still represent the same quasigroup. Therefore both Latin squares are indicative of the same quasigroup.

Meanwhile a loop's Cayley table needs to incorporate a two sided identity element (e). Meaning one element repeats the given bordering whether it is represented via the row or column.

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

Figure 16: Above 1 = e

4.1.2 Latin Squares and Groups.

Further more, using this explanation we can more accurately describe a Cayley table's relation to groups as well.

A given Cayley table will represent a group (not just a quasigroup) if it satisfies both of the following:

1. The interior is a Latin square.
2. The quadrangle criterion holds.[4] *That is to say for indices:* i, j, k, l *and* i', j', k', l'*, if* $a_{ik} = a_{i'k'}, a_{il} = a_{i'l'}$ *and* $a_{jk} = a_{j'k'}$*, then* $a_{jl} = a_{j'l'}$*.*

4.1.3 Latin Squares and Semigroups.

Because the axioms of a semigroup do not guarantee that their Cayley table will define a Latin square , the relationship between the two is nonexistant.

[4] Petr Vojtechovsky, "Reconstruction of Group Multiplication Tables by Quadrangle Criterion," *European Journal of Combinatorics*, 2007, https://doi.org/10.1006/eujc.2001.0548.

4.2 Mappings Between Latin Squares.

Because mappings can act on any set, we will see their effect when applied to quasigroups, and more explicitly see how these mappings affect the representative Cayley tables of those quasigroups.

Theorem 4.2 *Two Latin squares, L_1 and L_2 are isotopic if there are bijective maps between the columns, rows and symbols of L_1 onto the columns, rows and symbols of L_2*

Proof Application of their one-to-one correspondence to quasigroups and the isotopy definition of quasigroups. ■

$$\begin{vmatrix} 2 & 3 & 1 & 4 \\ 1 & 4 & 2 & 3 \\ 4 & 2 & 3 & 1 \\ 3 & 1 & 4 & 2 \end{vmatrix} \qquad \begin{vmatrix} 1 & 4 & 2 & 3 \\ 2 & 3 & 1 & 4 \\ 4 & 2 & 3 & 1 \\ 3 & 1 & 4 & 2 \end{vmatrix} \qquad \begin{vmatrix} 3 & 2 & 1 & 4 \\ 4 & 1 & 2 & 3 \\ 2 & 4 & 3 & 1 \\ 1 & 3 & 4 & 2 \end{vmatrix}$$

Figure 17: Isotopic Latin squares by row and column permutations

The above Latin squares are isotopic because you are able to do a row swap of rows 1 and 2 of the first to get the second, and column swaps of columns 1 and 2 of the first to get the third. We can also have bijections on the symbols of the Latin squares, for example:

$$\begin{vmatrix} 2 & 3 & 1 & 4 \\ 1 & 4 & 2 & 3 \\ 4 & 2 & 3 & 1 \\ 3 & 1 & 4 & 2 \end{vmatrix} \qquad \begin{vmatrix} 1 & 3 & 2 & 4 \\ 2 & 4 & 1 & 3 \\ 4 & 1 & 3 & 2 \\ 3 & 2 & 4 & 1 \end{vmatrix}$$

Figure 18: Isotopic Latin squares via permutations of the symbols

Anywhere there was a 1 in the starting square, there is now a 2. Conversly, anywhere there was a 2 there is now a 1.

Because Latin squares are representative of quasigroups, it means we can apply this concept to the quasigroups themselves.

Consider the Mappings λ, τ, ι such that:

$$\lambda = \text{Row Operations}$$

$$\tau = \text{Column Operations}$$

$$\iota = \text{Symbol Operations}$$

Then we have an algebraic represention of the transformations for these Latin squares, namely:

$$\lambda(x)\ \tau(y) = \iota(xy)$$

Some sources give the mappings as permutations of the border elements instead of row/column operations. That definition is equivalent. Therefore we will consistently use the standard bordering of $1,...,n$.

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

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

Figure 19: The first gives the bordering while the seconds omits it for simplicity

Above, both Latin squares are equivalent at every element, but the bordering of the first has been omitted from the second.

Therefore, two finite quasigroups will be consider isotopic if there exists permutations of the rows (λ), columns (τ), symbols (ι) of their associated Latin square, and λ, τ, ι are bijective.

We are, however, unable to do this for quasigroups of infinite size, due to the inability to represent them as Latin squares. However there is an interesting conclusion we can create in the finite case.

Theorem 4.3 *Any quasigroup is isotopic to a loop of the same size.*

Proof Row and column permutations create isotopic quasigroups. There is always a way to permute the rows and columns such that one row is equivalent to the its corresponding numbered column. ■

For example, using the example above, we merely can swap columns 2 and 3

$$\begin{vmatrix} 1 & 3 & 2 & 4 \\ 2 & 4 & 1 & 3 \\ 3 & 2 & 4 & 1 \\ 4 & 1 & 3 & 2 \end{vmatrix} \qquad \begin{vmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 2 & 1 \\ 4 & 3 & 1 & 2 \end{vmatrix}$$

Figure 20: Quasigroup (left) with its loop isotope (right) where 1 is the identity

4.3 Isotopy Classes of Latin Squares/Quasigroups.

Now that we have determined what quasigroups are isotopic to one another we can define what various isotopy classes based on which quasigroups are isotopic to each other.

And while it is possible to find the isotopies by hand, the process can be shortened by taking note of two qualities that present in every Latin square: Their transversals and intercalates.[5]

Definition 4.2. A *transversal* is an instance where the symbols $\{1,...,n\}$ each occur once in a distinct row and distinct column. An example is listed below:

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{vmatrix}$$

Figure 21: Latin square with 8 transversals

[5] Francisco Javier Zaragoza Mart´inez, “Intercalate Matrices and Algebraic Varieties,” *Morfismos* 2, no. 01 (1998): 67–81.

$$\begin{vmatrix} 1 & & & \\ & & 4 & \\ & & & 2 \\ & 3 & & \end{vmatrix} \quad \begin{vmatrix} 1 & & & \\ & & & 3 \\ & 4 & & \\ & & 2 & \end{vmatrix} \quad \begin{vmatrix} & 2 & & \\ & & & 3 \\ & & 1 & \\ 4 & & & \end{vmatrix} \quad \begin{vmatrix} & 2 & & \\ & & 4 & \\ 3 & & & \\ & & & 1 \end{vmatrix}$$

$$\begin{vmatrix} & & 3 & \\ 2 & & & \\ & 4 & & \\ & & & 1 \end{vmatrix} \quad \begin{vmatrix} & & 3 & \\ & 1 & & \\ & & & 2 \\ 4 & & & \end{vmatrix} \quad \begin{vmatrix} & & & 4 \\ 2 & & & \\ & & 1 & \\ & 3 & & \end{vmatrix} \quad \begin{vmatrix} & & & 4 \\ & 1 & & \\ 3 & & & \\ & & 2 & \end{vmatrix}$$

Figure 22: All 8 transversals...

Definition 4.3. An *intercalate* is a 2x2 sub Latin square. An example is listed below:

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{vmatrix}$$

Figure 23: Latin square with 4 intercalates

$$\begin{vmatrix} 1 & & 3 & \\ & & & \\ 3 & & 1 & \\ & & & \end{vmatrix} \quad \begin{vmatrix} & 2 & & 4 \\ & & & \\ & 4 & & 2 \\ & & & \end{vmatrix} \quad \begin{vmatrix} & & & \\ & 3 & & 1 \\ & & & \\ & 1 & & 3 \end{vmatrix} \quad \begin{vmatrix} & & & \\ 2 & & 4 & \\ & & & \\ 4 & & 2 & \end{vmatrix}$$

Figure 24: The 4 intercalates

Both of these qualities are *Isotopy Invariant*. This means if $L_1 \approx L_2$ (isotopic) then the number of transversals of L_1 is the same as the number of transversals of L_2. Similarly for intercalates.

Size	# Ltn Sqr	# Isot. Classes	Loop representative of each isotopy class	Conclusion
$n = 1$	1	1	$\begin{vmatrix} 1 \end{vmatrix}$	There is only a single Latin square of size 1.
$n = 2$	2	1	$\begin{vmatrix} 1 & 2 \\ 2 & 1 \end{vmatrix}$	Both Latin squares of size 2 are isotopic.
$n = 3$	12	1	$\begin{vmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \\ 1 & 3 & 2 \end{vmatrix}$	All Latin squares of size 3 are isotopic to one another.
$n = 4$	576	2	$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{vmatrix}, \begin{vmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{vmatrix}$	Any Latin square of size 4 that is not representative the K_4 group(First one) is isotopic to one another.
$n = 5$	161280	2	$\begin{vmatrix} 1 & 3 & 2 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \\ 2 & 4 & 5 & 1 & 3 \\ 4 & 5 & 3 & 2 & 1 \\ 5 & 2 & 1 & 3 & 4 \end{vmatrix}, \begin{vmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \\ 3 & 4 & 5 & 1 & 2 \\ 4 & 5 & 1 & 2 & 3 \\ 5 & 1 & 2 & 3 & 4 \end{vmatrix}$	One isotopy class affiliated with the cyclic-5 group and one affiliated with no groups...

Note that size 6 has 22 isotopy classes and size 7 has 564. This huge jump is due to the large jump in number of potential permutations of the elements in a given quasigroup of larger size.

$$\begin{array}{cc}
1! = 1 & 5! = 120 \\
2! = 2 & 6! = 720 \\
3! = 6 & 7! = 5040 \\
4! = 24 & 8! = 40320
\end{array}$$

As the number of permutations of the elements go, so do the number of Latin squares, isotopies and therefore, isotopy classes. This is known as a process of *combinatorial explosion*.

Transversals and intercalates can be challenging to find for larger finite quasigroups, not to mention in the inability to find them at all for infinite quasigroups since they are unable to be expressed via Latin squares. This sparks an interesting question, that so far remains unanswered. Is there an easier way to quickly identify two isotopic quasigroups, finite or infinite, without the use of these two isotopy invariant properties? More discussions on Latin squares takes place in the work of Keedwell and Dénes,[6] however, it is the extent we will cover here.

4.4 Latin Squares as Matrices.

Another important way to reinterpret Latin squares is as matrices. If we view the following equivalently:

Then, using the Latin square as matrix allows us to view the actions on a quasigroup in terms of matrix operations.

Isotopies can now be thought of using elementary matrices to simulate row and column operations, in addition to inner permutations of the entries. For a matrix, A:

[6] A. Donald Keedwell and József Dénes, *Latin Squares and their Applications* (Elsevier, 2015), ISBN: 978-0-444-63555-6.

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}$$

Figure 25: A Latin square represented as an $n \times n$ matrix consisting of $\{1, 2, ..., n\}$

.

$$R_\lambda A \leftrightarrow \text{Row Operations performed on } A$$

$$AC_\tau \leftrightarrow \text{Column Operations performed on } A$$

$$\iota(A) \leftrightarrow \text{Permutations of the entries contained in } A$$

A question we were then able to answer in our research is described below:

Question *Is it possible to express $\iota(A)$ as some combination of row and column operations?*

Equivalent Question *Are there permutation matrices, P, Q such that we can say $\iota(A) = PAQ$?*

Theorem 4.4 *For some $n \times n$ matrix, A, it is not always true that $\iota(A)$ can be expressed in terms of row and column operations.*

Proof By contradiction.

If $\iota(A) = PAQ$ for some permutation matrices, P and Q, then $det(\iota(A)) = \pm det(A)$ since row and column operations will preserve the determinant of a given matrix.

$$A = \begin{bmatrix} 3 & 1 & 4 & 2 \\ 2 & 3 & 1 & 4 \\ 4 & 2 & 3 & 1 \\ 1 & 4 & 2 & 3 \end{bmatrix}$$

Let $\iota : A \longrightarrow A$ via the permutation: (2 3)

$$\iota(A) = \begin{bmatrix} 2 & 1 & 4 & 3 \\ 3 & 2 & 1 & 4 \\ 4 & 3 & 2 & 1 \\ 1 & 4 & 3 & 2 \end{bmatrix}$$

$det(A) = 80; det(\imath(A)) = 160$

$80 \neq 160$

$\imath(A)$ is not necessarily able to be expressed solely terms of row and column operations. ■

Remark. This does leave the question open to whether or not you can express $i(A)$ in other ways, or how it is related to base matrix, A.

Since the order in which we perform the row, column or symbol permutations is irrelevant, we can say that two matrices (representative of quasigroups) A and A' are isotopic if there are permutation matrices s.t:

$$A' = R_\lambda \imath(A) C_\tau$$

And similarly, two matrices will be isomorphic via the map f if:

$$A' = R_f f(A) C_f$$

We can also rewrite this condition as either:

$$A' = R_f f(A) R_f^T \text{ or } A' = C_f^T f(A) C_f$$

This representation gives a lot of power to develop certain relationships between quasigroups. This is because you can begin to look at qualities of a matrix in addition to qualities of a Latin square and see if they are isotopy invariant. The above proof shows that the determinant is not isotopic invariant, as well as the trace of a matrix. However, there may be other properties that are.

4.5 Parastrophy Classes of Quasigroups.

4.5.1 Introduction.

In addition to belonging to a specific isotopy class, every quasigroup belongs to a parastrophe class as well. Originally, the term was referred to as adjugacy and conjugacy by various authors, but this ended up causing some confusion. The term parastrophe was first coined then by Sade.[7]

Let Q be a quasigroup. If in $(Q,\cdot)$: $xy = z$ then the parastrophic classes consist of the resulting quasigroups from a permutation of those three elements in that equation.

Definition 4.4. For every one of the six possible permutations, f of $\{x,y,z\}$, such that $f \in S_3$, there is a quasigroup Q_f such that $xy = z$ in Q if and only if $f(x)f(y) = f(z)$ in Q_f. These 6 mappings are known as the *parastrophisms* of Q. These parastrophisms, similar to isotopisms, form a group acting on the quasigroup, this time isomorphic to S_3 or one of its subgroups.

Potential quasigroup parastrophy classes, given by Krainichuk:[8]

asymmetric: All parastrophes are pairwise disjoint.

commutative: The class of parastrophes s.t. $xy = yx = z$

left-symmetric: The class of parastrophes s.t. $x(xy) = y$

right-symmetric: The class of parastrophes s.t. $(xy)y = x$

semi-symmetric: The class of parastrophes s.t. $(xy)x = y$

totally symmetric: All parastrophes coincide meaning that it satisfies both commutativity and either left/right symmetry.

If a quasigroup belongs to a given parastrophy class, then some of its parastophes may be isomorphic or isotopic to it. For example, for quasigroups in the commutative parastrophy class, their matrix representation is equivalent to its transpose ($A = A^T$), meaning their Latin square can be expressed symmetrically with the right bordering of elements. As an example:

[7] Par Albert Sade, “Quasigroupes parastrophiques. Expressions et identités,” *Mathematische Nachrichten* 20, nos. 1-2 (1959): 73–106, https://doi.org/10.1002/mana.19590200109.

[8] Halyna Krainichuk, “Classification of Group Isotopes According to their Symmetry Groups,” *Folia Mathematica* 19, no. 1 (2017): 84–98.

$$\text{For } Q = \begin{bmatrix} 3 & 1 & 2 & 4 \\ 4 & 2 & 1 & 3 \\ 1 & 4 & 3 & 2 \\ 2 & 3 & 4 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 1 & 2 & 4 \\ 4 & 2 & 1 & 3 \\ 1 & 4 & 3 & 2 \\ 2 & 3 & 4 & 1 \end{bmatrix}$$

(a) $xy = z$

$$\begin{bmatrix} 3 & 4 & 1 & 2 \\ 1 & 2 & 4 & 3 \\ 2 & 1 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix}$$

(b) $yx = z$

$$\begin{bmatrix} 2 & 3 & 1 & 4 \\ 3 & 2 & 4 & 1 \\ 1 & 4 & 3 & 2 \\ 4 & 1 & 2 & 3 \end{bmatrix}$$

(c) $xz = y$

$$\begin{bmatrix} 2 & 3 & 1 & 4 \\ 3 & 2 & 4 & 1 \\ 1 & 4 & 3 & 2 \\ 4 & 1 & 2 & 3 \end{bmatrix}$$

(d) $zx = y$

$$\begin{bmatrix} 3 & 4 & 1 & 2 \\ 1 & 2 & 4 & 3 \\ 2 & 1 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix}$$

(e) $yz = x$

$$\begin{bmatrix} 3 & 1 & 2 & 4 \\ 4 & 2 & 1 & 3 \\ 1 & 4 & 3 & 2 \\ 2 & 3 & 4 & 1 \end{bmatrix}$$

(f) $zy = x$

Above shows that Q belongs to a right-symmetric parastrophe class since matrix (a) is is the same as matrix (f). This explicitly shows us that the parastrophe group is a subgroup of S_3 with only three elements, C_3. More interesting results can then arise when we consider the group of not only parastrophes, but isotopies, as well.

4.5.2 Isotopies and Parastrophes as a Group.

Since both parastrophes and isotopies are defined in terms of permutations, we can and will define the collection of isotopies ($\mathbb{I}$) and parastrophes ($\mathbb{P}$) of a certain quasigroup, Q as a group $\mathbb{G}$. The following theorem and corollary are given by Artzy.[9]

Theorem 4.5 $\mathbb{I}$ *is a normal subgroup in* $\mathbb{G}$

Proof We will define, without loss of generality, α to be the parastrophe that swaps the first two elements and β will be the parastrophe reminiscent of a standard 3-cycle. And an arbitrary isotopy, set of three maps to be: $[\lambda, \tau, \iota]$.

Then it suffices to show that for any $[\lambda, \tau, \iota]$:

$$\mathbb{I} \leq \mathbb{G}$$

[9] R. Artzy, "Isotopy and Parastrophy of Quasigroups," *Proceedings of the American Mathematical Society* 14, no. 3 (1963): 429–431, https://doi.org/10.2307/2033814.

$$\alpha[\lambda,\tau,\iota]\alpha^{-1} \in \mathbb{I}$$
$$\beta[\lambda,\tau,\iota]\beta^{-1} \in \mathbb{I}$$

$\mathbb{I} \leq \mathbb{G}$ since any combination of isotopies is still an isotopy, therefore it is closed under the group operation, and for any isotopy we can define an inverse mapping since it is by definition bijective.

Subsequently, since α is a swapping of elements: $\alpha = \alpha^{-1}$. Therefore:

$$\alpha[\lambda,\tau,\iota]\alpha^{-1} = \alpha[\lambda,\tau,\iota]\alpha = [\tau,\lambda,\iota] \in \mathbb{I} \text{ by properties of permutations.}$$

Similarly, $\beta[\lambda,\tau,\iota]\beta^{-1} = [\iota,\lambda,\tau] \in \mathbb{I}$

Therefore, $\mathbb{I}$ is a normal subgroup of $\mathbb{G}$ ■

Corollary 4.5.1 *If Q_1 is parastrophic to Q_2 by parastrophy: p, then an isotopy of Q_1 is parastrophic to an isotopy of Q_2 by p.*

Proof Let $i(Q_1)$ be the isotopy of Q_1 and $Q_2 = p(Q_1)$

Consider $pi(Q_1)$, which is to be read as performing i on Q_1 and then subsequently performing p. Since $Q_1 = p^{-1}(Q_2)$:

$$pi(Q_1) = pip^{-1}(Q_2)$$

And by our above theorem:

$$pip^{-1} \in \mathbb{I}$$

Thus: $pip^{-1}(Q_2)$ is isotopic to Q_2. ■

5 Continuous Algebraic Structures

Here we will consider infinite sets with a single binary operation. In particular, we will focus on Lie groups, Lie quasigroups, and Lie loops.

5.1 Lie Groups.

5.1.1 Definition.

Definition 5.1. A *Lie group* is a group, G, whose underlying set is a manifold, s.t. the maps $G \times G \longrightarrow G$, where $(x,y) \to xy$ and $G \longrightarrow G$ via $x \longrightarrow x^{-1}$ are smooth maps of manifolds.

Definition 5.2. A *manifold* is a topological space that locally resembles Euclidean space, $\mathbb{R}^n$, near each point. More precisely, an n-dimensional manifold, or *n-manifold*, is a topological space with the property that each point has a neighborhood that is homeomorphic to the Euclidean space of dimension n such that on the overlaps.

Figure 27: S^1xS^1 is a Lie group, while S^2 is not, however, they are both 2-manifolds

Definition 5.3. A real-valued function on an open subset $U \subseteq \mathbb{R}^n$ is called smooth if it is infinitely differentiable. Equivalently, A function $f\colon M \longrightarrow \mathbb{R}^n$ on a manifold M is called smooth if $\forall$ charts (U, φ) the function:

$$f \circ \varphi^{-1}\colon \varphi(U) \longrightarrow \mathbb{R}^n \text{ is smooth.}$$

The set of smooth functions into the real-line $f\colon M \longrightarrow \mathbb{R}$ is denoted $C^\infty(M)$.

5.1.2 Examples.

The following matrix groups form Lie groups with respect to matrix multiplication.

1. $GL_n(\mathbb{R}) = \{\text{All } n\text{x}n \text{ matrices over } \mathbb{R} \mid \det \neq 0\}$

$GL_n(\mathbb{R})$ is a Lie group since it is an n^2-manifold and it is a group such that matrix multiplication and matrix inverses are smooth maps.

$I \in GL_n(\mathbb{R})$: since $det(I) = 1$.

For $A, B \in GL_n(\mathbb{R})$: $det(AB) = det(A)det(B) \neq 0$

$A \in GL_n(\mathbb{R}) \Rightarrow A^{-1} \in GL_n(\mathbb{R})$:

Since $det(A)det(A^{-1}) = det(I) \Rightarrow det(A^{-1}) = \dfrac{1}{det(A)} \neq 0$

Another example of smooth of a smooth map is $det : GL_2(\mathbb{R}) \longrightarrow GL_1(\mathbb{R})$.

$det : GL_2(\mathbb{R}) \longrightarrow GL_1(\mathbb{R})$ via: $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \longrightarrow ad - bc$

is a smooth map from the 4-manifold $GL_2(\mathbb{R})$ to the 1-manifold $GL_1(\mathbb{R})$.

det is a smooth mapping because the n-th derivative with respect to each variable, a, b, c, d exists and continuous for all n.

2. $SL_n(\mathbb{R}) = \{\text{All } n\text{x}n \text{ matrices over } \mathbb{R} \mid \det = 1\}$

$SL_n(\mathbb{R})$ is a Lie group since it is an $(n^2 - 1)$-dimensional manifold that forms a group.

$I \in SL_n(\mathbb{R})$: since $det(I) = 1$.

For $A,B \in SL_n(\mathbb{R})$: $det(AB) = det(A)det(B) = 1$

$A \in SL_n(\mathbb{R}) \Rightarrow A^{-1} \in SL_n(\mathbb{R})$:

Since $det(A)det(A^{-1}) = det(I) \Rightarrow det(A^{-1}) = \frac{1}{1} = 1$

3. $O_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid A^T = A^{-1}\}$

$O_n(\mathbb{R})$ is also a Lie group. In particular it is a group because:

$I \in O_n(\mathbb{R})$: since $I = I^T = I^{-1}$.

For $A,B \in O_n(\mathbb{R})$: $(AB)^T = B^T A^T = B^{-1}A^{-1} = (BA)^{-1}$

$A \in O_n(\mathbb{R}) \Rightarrow A^{-1} \in O_n(\mathbb{R})$:

Since $A^T = A^{-1}$, then $(A^T)^{-1} = (A^{-1})^T = (A^{-1})^{-1} = A$

4. $SO_n(\mathbb{R}) = \{A \in SL_n(\mathbb{R}) \mid A^T = A^{-1}\}$ is also a Lie Group.

5.1.3 Manifolds and Tangent Spaces.

Definition 5.4. Let A be any associative $\mathbb{R}$-algebra. A *derivation*, $D : A \longrightarrow A$, of A is a linear map ($D(af + by) = aD(f) + bD(g)$) such that:

$$D(fg) = D(f)g + fD(g) \; \forall \, f,g \in A$$

Definition 5.5. Let $a \in M$. The *tangent space* at a is defined to be:

$$T_a(M) = \mathrm{Der}_a(C^\infty(M,\mathbb{R}))$$

the $\mathbb{R}$-vector space of derivations at a of the algebra, $C^\infty(M,\mathbb{R})$.

Therefore:

$$D(fg) = D(f)g(a) + f(x)D(g) \; \forall \, f,g \in C^\infty(M,\mathbb{R})$$

Let X, Y be derivations at a, where M is the sphere S^2. Then we can create the tangent plane:

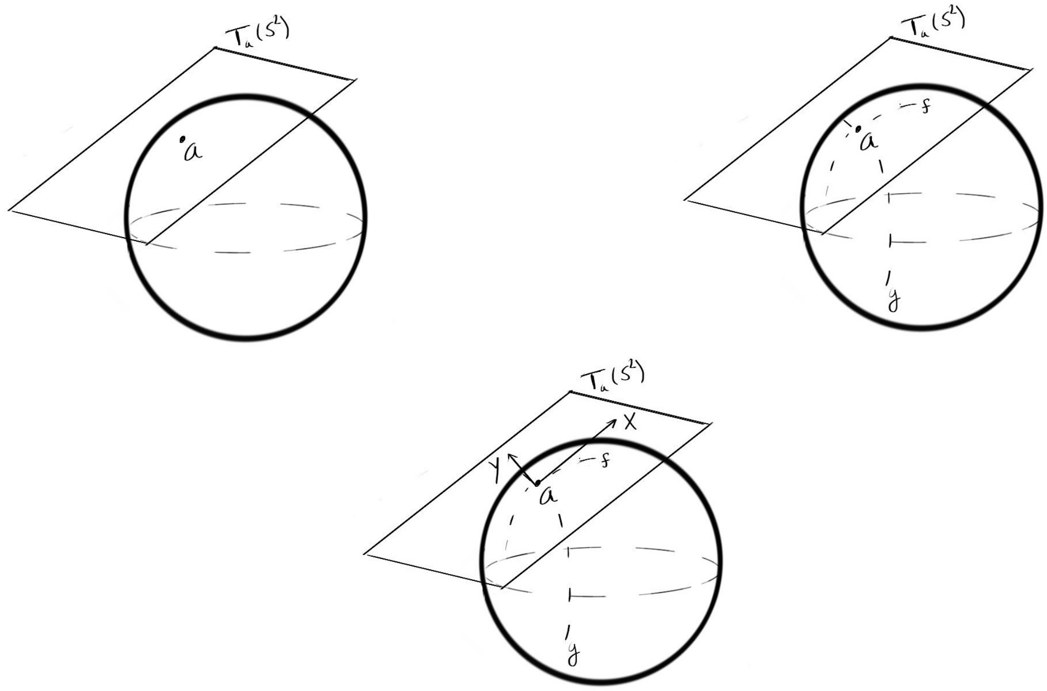

Figure 28: S^2 and its tangent plane, $T_a(S^2) = \text{span}_{\mathbb{R}}(X, Y)$

If G is a Lie group, using the tangent space at $a = e$, we encounter a fundamental object, known as Lie algebra.

5.2 Lie Algebra.

5.2.1 General Definition.

Definition 5.6. *A Lie algebra* is an $\mathbb{R}$-vector space $\mathfrak{g}$ with the binary operation $[\cdot,\cdot]$: $\mathfrak{g} \times \mathfrak{g} \longrightarrow \mathfrak{g}$, $(X,Y) \to [X,Y]$ that satisfies the following:

Bilinear: $[aX + bY, Z] = a[X,Z] + b[Y,Z]$

Skew-Symmetric: $[X,Y] = -[Y,X]$

Jacobi: $[X,[Y,Z]] + [Z,[X,Y]] + [Y,[Z,X]] = 0$

5.2.2 Tangent Space of G at the Identity.

Given that our group G is a manifold, we can define the tangent space of G at identity as:

$$\mathfrak{g} = T_e(G) = \{\text{Set of all derivations on } G \text{ at } e\}$$

where the Lie bracket operation is the commutator ($[X,Y] = XY - YX$) of the derivations X and Y that are tangent at e.

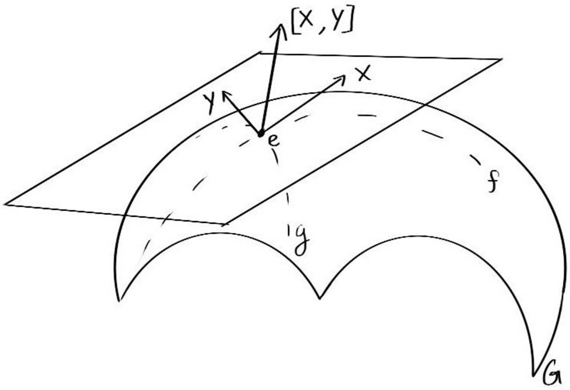

Figure 29: The commutator, $XY - YX$ of two derivations is another derivation

Let's show then, that the commutator of two derivations is, itself, a derivation. This means that:

1. $(XY - YX)(fg) = (XY - YX)(f) \cdot g + f \cdot (XY - YX)(g)$ 2. $(XY - YX)(af + bg) = a \cdot (XY - YX)(f) + b \cdot (XY - YX)(g)$

Proof of 1.

$$\begin{aligned}
(XY - YX)(fg) &= XY(fg) - YX(fg) \\
&= X[Y(f) \cdot g + f \cdot Y(g)] - Y[X(f) \cdot g + f \cdot Y(g)] \\
&= XY(f) \cdot g + Y(f)X(g) + X(f)Y(g) + f \cdot XY(g) \\
&\quad - YX(f) \cdot g - X(f)Y(g) - Y(f)X(g) - f \cdot YX(g) \\
&= [XY(f) - YX(f)] \cdot g + f \cdot [XY(g) - YX(g)] \\
&= (XY - YX)(f) \cdot g + f \cdot (XY - YX)(g) \blacksquare
\end{aligned}$$

Proof of 2.

$$\begin{aligned}
(XY-YX)(af+bg) &= XY(af)+XY(bg)-YX(af)-YX(bg) \\
&= X[Y(a)\cdot f+a\cdot Y(f)]+X[Y(b)\cdot g+b\cdot Y(g)] \\
&\quad -Y[X(a)\cdot f+a\cdot X(f)]-Y[X(b)\cdot g+b\cdot X(g)] \\
&= XY(a)\cdot f+Y(a)X(f)+X(a)Y(f)+a\cdot XY(f) \\
&\quad +XY(b)\cdot g+Y(b)X(g)+X(b)Y(g)+b\cdot XY(g) \\
&\quad -YX(a)\cdot f-X(a)Y(f)-Y(a)X(f)-a\cdot YX(f) \\
&\quad -YX(b)\cdot g-X(b)Y(g)-Y(b)X(g)-b\cdot YX(g) \\
&= a[XY(f)-YX(f)]+b[XY(g)-YX(g)] \\
&= a(XY-YX)(f)+b(XY-YX)(g) \blacksquare
\end{aligned}$$

The commutator of two derivations then is always a derivation itself, meaning that $[X,Y] \in T_e(G)$.

We can now take this example and apply it to various Lie groups.

5.2.3 Other Examples of Lie Algebras.

Here, we shall see the affect that the commutator derivation has on various Lie groups we discussed in Section 5.1.2.

1. Let $G = GL_n(\mathbb{R})$

$$T_I(G) = \mathfrak{gl}_n(\mathbb{R}) = M_n(\mathbb{R})$$

This means the tangent space of matrices with a nonzero determinant are all matrices under the bracket operation.

2. Let $G = SL_n(\mathbb{R})$

$$T_I(G) = \mathfrak{sl}_n(\mathbb{R}) = \{n\text{x}n \text{ matrices with trace } 0\}$$

Since $A,B \in \mathfrak{sl}_n(\mathbb{R})$:

$$\text{If } tr(AB) = tr(BA), \text{ then } tr(AB - BA) = tr(AB) - tr(BA) = 0$$

3. Let $G = SO(n, \mathbb{R})$

$$T_I(G) = \mathfrak{so}_n(\mathbb{R}) = \{\text{skew symmetric } n \times n \text{ matrices}\}$$

It is valuable to note here that since:

$$SO(n, \mathbb{R}) \subseteq SL_n(\mathbb{R}) \subseteq GL_n(\mathbb{R})$$

The corresponding tangent spaces have the same levels of containment.

$$\mathfrak{so}_n(\mathbb{R}) \subseteq \mathfrak{sl}_n(\mathbb{R}) \subseteq \mathfrak{gl}_n(\mathbb{R})$$

Finally, lets examine the specific case of $\mathfrak{so}_3(\mathbb{R})$ where, again, $[A, B] = AB - BA$. We know that A, B are both skew symmetric and have trace 0.

$$A = \begin{bmatrix} 0 & a & b \\ -a & 0 & c \\ -b & -c & 0 \end{bmatrix} \qquad B = \begin{bmatrix} 0 & x & y \\ -x & 0 & z \\ -y & -z & 0 \end{bmatrix}$$

Figure 30: $A, B \in \mathfrak{so}_3(\mathbb{R})$

Which gives us that all matrices $A \in \mathfrak{so}_3(\mathbb{R})$ are linear combinations of the basis (I, J, K) where:

$$I = \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \qquad J = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \qquad K = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix}$$

Figure 31: Basis of $\mathfrak{so}_3(\mathbb{R})$

This leads us to the conclusion that $\mathfrak{so}_3(\mathbb{R}) = \text{span}_{\mathbb{R}}(I, J, K)$. And lets verify that $AB - BA \in \text{span}_{\mathbb{R}}(I, J, K)$.

We'll start by calculating both AB and BA:

$$AB = \begin{bmatrix} -(ax+by) & -bz & az \\ -cy & -(ax+cz) & -ay \\ cx & -bx & -(by+cz) \end{bmatrix}$$

$$BA = \begin{bmatrix} -(ax+by) & -cy & cx \\ -bz & -(ax+cz) & -bx \\ az & -ay & -(by+cz) \end{bmatrix}$$

Figure 32: $AB, BA \notin \mathfrak{so}_3(\mathbb{R})$

Lets now calculate $AB - BA$:

$$AB - BA = \begin{bmatrix} 0 & cy-bz & az-cx \\ bz-cy & 0 & bx-ay \\ cx-az & ay-bx & 0 \end{bmatrix}$$

$$AB - BA = \begin{bmatrix} 0 & cy-bz & az-cx \\ -(cy-bz) & 0 & bx-ay \\ -(az-cx) & -(bx-ay) & 0 \end{bmatrix}$$

Figure 33: $AB - BA \in \mathfrak{so}_3(\mathbb{R})$

Thus, $AB - BA \in \text{span}_{\mathbb{R}}(I, J, K)$.

Remarkably this matrix can be generated, via the cross product of the vectors:

$$v_1 = \begin{bmatrix} a \\ b \\ c \end{bmatrix} \qquad v_2 = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$$

$$v_1 \text{ x } v_2 = \begin{bmatrix} bz-cy \\ cx-az \\ ay-bx \end{bmatrix}$$

Therefore, $\mathfrak{so}_3(\mathbb{R})$ is isormorphic to $\mathbb{R}^3$ under the cross-product operation.

$$\mathfrak{so}_3(\mathbb{R}) \cong (\mathbb{R}, \times)$$

5.3 Lie Quasigroups and Loops.

5.3.1 Definitions.

Definition 5.7. Adapting our definition of Lie groups, we can define a quasigroup $(Q,\cdot,\backslash,/)$ to be a *Lie quasigroup* if Q is a manifold and the following are smooth maps:

$$Q\times Q \longrightarrow Q, \text{ via } (x,y)\rightarrow x\backslash y$$
$$Q\times Q \longrightarrow Q, \text{ via } (x,y)\rightarrow x/y$$
$$Q\times Q \longrightarrow Q, \text{ via } (x,y)\rightarrow x\cdot y$$

Definition 5.8. We will define a loop, $(L,\cdot)$ to be a *Lie loop* if L is a manifold and the following are smooth maps:

$$L\times L \longrightarrow L, \text{ via } x\rightarrow x^{-1} \text{ (right inverse)}$$
$$L\times L \longrightarrow L, \text{ via } x\rightarrow {}^{-1}x \text{ (left inverse)}$$
$$L\times L \longrightarrow L, \text{ via } (x,y)\rightarrow x\cdot y$$

Since loops have an identity element, e, it is more viable to consider the mappings corresponding to the left and right inverses. Where ${}^{-1}x\cdot x = e$ and $x\cdot x^{-1} = e$, however, x $\cdot\ {}^{-1}x \neq e$ and $x^{-1}\cdot x \neq e$.

5.3.2 Examples.

We can then consider many examples using operations we already know to see some Lie loops. For starters, $(\mathbb{R},\circ)$, where $x\circ y = x+y-xy$. $\mathbb{R}$ is clearly a manifold and $\circ$ acts a smooth mapping. This is because any mapping that is a polynomial in the variables is infinitely differentiable.

Therefore, all that is left is to show that it does indeed represent a loop, rather than some other algebraic structure. Firstly lets show that it does contain a two sided identity: element:

$$x+e-xe = x \Rightarrow e-xe = 0 \Rightarrow e(1-x) = 0 \Rightarrow e = 0$$
$$e+y-ey = y \Rightarrow e-ey = 0 \Rightarrow e(1-y) = 0 \Rightarrow e = 0$$

It is trivial to see that any combination of real numbers will produce a real number via the operation, as well, so to verify that this is a loop and not a group, we will need to show that there is no associative property under this operation meaning $(x \circ y) \circ z \neq x \circ (y \circ z)$:

$$\begin{gathered}
(x \circ y) \circ z = (x+y-xy) \circ z = x+y-xy+z-[(x+y-xy)z] \\
\neq \\
x \circ (y \circ z) = x \circ (y+z-yz) = x+y+z-yz-[x(y+z-yz)]
\end{gathered}$$

We can also define several Lie quasigroups and loops on matrices as well. Instead of denoting our sets as $GL_n(\mathbb{R})$ where matrix multiplication is the group operation, we will denote them as $QGL_n(\mathbb{R})$, where the underlying set is $GL_n(\mathbb{R})$ and we vary the operation to have it satisfy the Lie quasigroup axioms. We can define, then the following matrix Lie quasigroups:

1. $(QGL_2(\mathbb{R}), \circ)$, where $A \circ B = AB^{-1}$, thus:

   $A \circ B = C$ uniquely determines $C = AB^{-1}$

   $A \backslash C = B$ uniquely determines $B = C^{-1}A$

   $C/B = A$ uniquely determines $A = CB$

2. $(QGL_2(\mathbb{R}), \circ)$, where $A \circ B = AB^T$, thus:

   $A \circ B = C$ uniquely determines $C = AB^T$

   $A \backslash C = B$ uniquely determines $B = C^T(A^{-1})^T$

   $C/B = A$ uniquely determines $A = C(B^{-1})^T$

3. $(QGL_2(\mathbb{R}), \circ)$, where $A \circ B = A^{-1}B^T$, thus:

   $A \circ B = C$ uniquely determines $C = A^{-1}B^T$

   $A \backslash C = B$ uniquely determines $B = C^T A^T$

   $C/B = A$ uniquely determines $A = B^T C^{-1}$

5.4 Further Directions.

Consider the analogues of the Lie algebra for a Lie quasigroup, which is called an *Akivis algebra.* In addition to the bracket operation, $[X,Y] = XY - YX$ on $T_e(Q)$, we also consider another operation being the associator, $(X,Y,Z) = (XY)Z - X(YZ)$. If you have a Lie loop satisfying further properties (such as ones of the Bol-Moufang type we discussed in section 3.4) what are the corresponding properties of the Akivis algebra?

6 Summary and Conclusions

In summation, we have given a comprehensive review of the algebraic structure of sets with a single binary operation, and given various representations of these algebraic objects. Hopefully the reading of this Master's Thesis allows for readers to gain understanding of various algebraic objects, especially quasigroups and loops. The thesis summarizes and answers questions considering isotopies and parastrophes, namely the idea that there is no way to express the symbol mappings of a Latin square with the use of row and column permutations. The thesis then goes on to introduce certain continuous algebraic structures such as Lie groups, loops, and quasigroups as well as examples. We end on a question designed to inspire the reader for further research.

References

Artzy, R. “Isotopy and Parastrophy of Quasigroups.” *Proceedings of the American Mathematical Society* 14, no. 3 (1963): 429–431. https://doi.org/10.2307/2033814.

Birkhoff, Garrett. *Lattice Theory*. American Mathematical Society 307 Colloquium Publications, 1948. ISBN: 978-0-8218-1025-5.

Keedwell, A. Donald, and József Dénes. *Latin Squares and their Applications*. Elsevier, 2015. ISBN: 978-0-444-63555-6.

Krainichuk, Halyna. “Classification of Group Isotopes According to their Symmetry Groups.” *Folia Mathematica* 19, no. 1 (2017): 84–98.

Mart´inez, Francisco Javier Zaragoza. “Intercalate Matrices and Algebraic Varieties.” *Morfismos* 2, no. 01 (1998): 67–81.

Phillips, J. D., and Petr Vojtechovsky. “The Varieties of Loops of Bol-Moufang Type.” *Algebra Universe* 54 (2005): 259–271. https://doi.org/10.1007/s00012-005-1941-1.

Sade, Par Albert. “Quasigroupes parastrophiques. Expressions et identités.” *Mathematische Nachrichten* 20, nos. 1-2 (1959): 73–106. https://doi.org/10.1002/mana.19590200109.

Shcherbacov, JD Phillips D.I. Pushkashub A.V. Shcherbacovc V.A. “On Birkhoff’s Quasigroup Axioms.” *Journal of Algebra* 457 (2016): 7–17. https://doi.org/10.1016/j.jalgebra.2016.02.024.

Vojtechovsky, Petr. “Reconstruction of Group Multiplication Tables by Quadrangle Criterion.” *European Journal of Combinatorics*, 2007. https://doi.org/10.1006/eujc.2001.0548.