2017

On free quasigroups and quasigroup representations

Stefanie Grace Wang
Iowa State University

On free quasigroups and quasigroup representations

by

Stefanie Grace Wang

A dissertation submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Major: Mathematics

Program of Study Committee:
Jonathan D.H. Smith, Major Professor
Jonas Hartwig
Justin Peters
Yiu Tung Poon
Paul Sacks

The student author and the program of study committee are solely responsible for the content of this dissertation. The Graduate College will ensure this dissertation is globally accessible and will not permit alterations after a degree is conferred.

Iowa State University

Ames, Iowa

2017

DEDICATION

I would like to dedicate this dissertation to the Integral Liberal Arts Program. The Program changed my life, and I am forever grateful. It is as Aristotle said, "All men by nature desire to know." And Montaigne was certainly correct as well when he said, "There is a plague on Man: his opinion that he knows something."

TABLE OF CONTENTS

LIST OF TABLES vi

LIST OF FIGURES vii

ACKNOWLEDGEMENTS viii

ABSTRACT x

CHAPTER 1. INTRODUCTION 1

1.1 Preliminaries 1

1.2 Combinatorial Multiplication Groups 4

1.3 Outline of the Dissertation 5

CHAPTER 2. ISOMORPHISM INVARIANTS FOR LINEAR PIQUES . . . 7

2.1 Introduction 7

2.1.1 Outline of the chapter 8

2.1.2 Related invariants 8

2.1.3 Conventions 9

2.2 Linear Piques 9

2.2.1 Quasigroups and piques 9

2.2.2 Linear piques 10

2.2.3 Equivalent representations 10

2.2.4 Permutational similarity 12

2.2.5 Ordinary characters of $\mathbb{C}$-linear piques 13

2.3 Linear Piques on Finite Cyclic Groups 14

2.3.1 Permutation characters 14

2.3.2 Linear piques on small cyclic groups 15

2.3.3 Cyclic groups of prime power order . . . 16
2.3.4 Cyclic groups of order not divisible by 8 . . . 17
2.3.5 Linear piques on $\mathbb{Z}/_5$ . . . 18
2.4 Linear Piques Defined on $\mathbb{Z}/_{2^k}$ . . . 19
2.4.1 The case of $\mathbb{Z}/_8$ . . . 19
2.4.2 Computing permutations for automorphisms of $\mathbb{Z}/_{2^k}$ . . . 20
2.4.3 Linear piques on $\mathbb{Z}/_{16}$ . . . 21
CHAPTER 3. PERI-CATALAN NUMBERS . . . 24
3.1 An Introduction to Catalan Numbers and Their History . . . 24
3.1.1 Triangulating regular convex polygons . . . 25
3.1.2 Lattice paths . . . 25
3.1.3 Rooted binary trees . . . 26
3.1.4 Well-formed parentheses . . . 27
3.2 Magma Words and Rooted Binary Trees . . . 28
3.3 Quasigroup Words and Rooted Binary Trees . . . 29
3.4 Peri-Catalan Numbers . . . 30
3.5 Mirror Symmetry . . . 30
3.6 The Inductive Process . . . 33
3.7 Root Vertex Cancellations . . . 34
3.7.1 Cancellations in unbalanced trees . . . 35
3.7.2 Cancellations in balanced Trees . . . 38
3.8 Refining the Recursive Formula . . . 38
3.8.1 Counting the cancellations . . . 39
CHAPTER 4. DERIVATION AND THE FREE QUASIGROUP . . . 48
4.1 Introduction . . . 48
4.2 Centrality . . . 49
4.3 Nonassociative Integers . . . 52

CHAPTER 5. FUTURE WORK 56

5.1 Permutational Intertwinings 56

5.1.1 Linear piques on elementary abelian groups 56

5.2 Peri-Catalan Numbers 57

5.2.1 A generating function 58

5.2.2 Words in n generators 58

5.3 A Faithful Representation of the Free Quasigroup 59

APPENDIX A. FIXED POINTS FOR LINEAR PIQUES ON $\mathbb{Z}/_{2^n}$ 60

APPENDIX B. CHARACTER TABLES 62

APPENDIX C. CALCULATIONS FOR SMALL PERI-CATALAN NUMBERS 64

BIBLIOGRAPHY 66

LIST OF TABLES

Table 1.1 Two 3×3 Latin squares. 2

Table 2.1 Permutation characters for linear piques on $\mathbb{Z}/_3$ 15

Table 2.2 Permutations for the automorphisms of $\mathbb{Z}/_5$ 18

Table 2.3 Permutations for the automorphisms of $\mathbb{Z}/_8$ 20

Table 2.4 Partial character table for linear piques on $\mathbb{Z}/_8$ 20

Table 2.5 Automorphisms of $\mathbb{Z}/_{16}$: permutations and fixed point counts 21

Table 2.6 Partial character table for linear piques on $\mathbb{Z}/_{16}$ 22

Table 2.7 Conjugation relations of elements in $(\mathbb{Z}/_{16})^*$ 22

Table 3.1 The first ten peri-Catalan numbers 47

Table 4.1 A finite quasigroup generated by a single element 51

Table 5.1 The first ten peri-Catalan numbers and their ratios. 58

Table B.1 Full character table for linear piques defined on $\mathbb{Z}/_3$ 62

Table B.2 Full character table for linear piques defined on $\mathbb{Z}/_4$ 62

Table B.3 Full character table for linear piques defined on $\mathbb{Z}/_5$ 62

Table B.4 Partial character table for linear piques defined on $\mathbb{Z}/_{32}$. 63

LIST OF FIGURES

Figure 3.1 Triangulations of regular convex polygons up to $n = 4$. 25

Figure 3.2 A non-monotone and monotone path on a 3×3 lattice grid. 25

Figure 3.3 The Deathly Hallows. 26

Figure 3.4 A rooted binary tree 27

Figure 3.5 Full rooted binary trees, up to 4 leaves 27

Figure 3.6 Properly writings n pairs of parentheses 28

Figure 3.7 Mirror-symmetric rooted binary trees with four leaves 31

Figure 3.8 Triality symmetry of the quasigroup operations. 32

Figure 3.9 A tree exhibiting the necessary format for the (IR) cancellation. 39

Figure 3.10 Trees exhibiting the necessary format for the (SR) and (DR) cancellations. 40

Figure 3.11 A tree exhibiting the necessary format for the (SR) cancellation on the left branch. 42

Figure 3.12 A tree exhibiting the necessary format for the (IR) cancellation on the left branch. 43

Figure 3.13 A tree exhibiting the necessary format for the (DR) cancellation on the left branch. 44

Figure C.1 The trees for P_2. 64

Figure C.2 All possible trees with 3 arguments 65

ACKNOWLEDGEMENTS

There were many components that lent to the making of this dissertation, including an exorbitant amount of cheesecake. This was a long journey, and thanks will be given in mostly chronological order.

I am thankful for my advisor, Dr. Jonathan D. H. Smith, a purveyor of the boots-and-turtleneck hipster mathematician lifestyle. I drank the Kool-Aid and you ate the hummus. It was a delight and privilege to work with Jonathan. Not only did he provide guidance, support, and encouragement critical to my development as a mathematician, he contributed a fair share of sassy quips in our research meetings. I hope the walls in Carver aren't as thin as I fear, because the sass ran amok at times.

Two major sources of early inspiration were my high school precalculus and calculus teachers, Mrs. Lee and Mrs. Nicholson. These were two of my favorite classes in high school, and I found inspiration to pursue math largely due to my experiences in their classrooms. A peer once described to me, "You can have a pulse in Mrs. Nicholson's calculus class and fail, but still manage to pass the AP exam. That's how good she is." I thought Mrs. Lee was one of the coolest (because she had a Masters in math) and nicest teachers around. I did not understand the importance of seeing women holding higher degrees in mathematics at the time. Now I see that having role models provided subtle and subliminal encouragement that these things were possible for me. Without them, I would not have started college dead set on earning some kind of degree in math.

I was so dead set on being a math major in college that I did not anticipate the siren call of the Integral Liberal Arts Program. I have made arbitrary and bold choices in my life, but none so serendipitous as my choice to study in the Integral Program. I met some of the best people in my life through the Program. My undergraduate advisor Jim Sauerberg was a tremendous support both in Integral and in graduate school. Thank you for googling with me

"how do math minors go to grad school" and providing encouragement throughout grad school. The too-infrequent summer visits to Theo Carlile, Jim Smith, S. A. Cortright, Ted Tsukahara, and the infamous MR. RILEY were respites from the vortex of specialization. The grit and determination that got me through graduate school were first honed in the halls of Dante and Galileo. The zest and vibrancy you all have for life and learning pull me through. Thank you for seeing something in me. Thank you for everything.

My friends and professors in the Smith College post-baccalaureate program have a special place in my heart. A supportive and empowering environment for women in mathematics was the perfect place to transition from humanities to STEM. My advisor Ruth Haas is simply the best. Your unwavering encouragement and support in the post-bac program and beyond made a tremendous impact on my life. No matter how busy you were, you always found time for me. I am especially grateful for your input and support with my first job hunt. To all my friends in the post-bac program, thank you. You're all the best, and that's all there is to it.

The department at Iowa State has been a home for the last five years. I am grateful for the many friends, staff, and professors that helped me along my journey. I would like to thank my committee members for their time and commitment. Justin Peters, especially, has been a advocate and mentor. Thank you for your support, hilarious jokes, and appreciation of gerbils in compact spaces. Michael Young, you have been my Ruth-equivalent at Iowa State. Thank you for all the opportunities you provided and the (spookily accurate) encouragement. Heather Bolles, Elgin Johnston, and Barb Licklider inspired me to be a better teacher and learner, and provided the tools to do so.

My final thanks goes to my family and friends in California. The original source of the grit and determination that got me through graduate school came from my family. Thank you for ingraining the strength and determination I needed to achieve my goals. To Jim, thank you for believing in me and encouraging me every step of the way. I am thankful to have so many people I can always count on to celebrate my successes with me and to see me through difficult times.

ABSTRACT

This work consists of three parts. The discussion begins with *linear quasigroups*. For a unital ring S, an S-linear quasigroup is a unital S-module, with automorphisms ρ and λ giving a (nonassociative) multiplication $x \cdot y = x^{\rho} + y^{\lambda}$. If S is the field of complex numbers, then ordinary characters provide a complete linear isomorphism invariant for finite-dimensional S-linear quasigroups. Over other rings, it is an open problem to determine tractably computable isomorphism invariants. The paper investigates this isomorphism problem for $\mathbb{Z}$-linear quasigroups. We consider the extent to which ordinary characters classify $\mathbb{Z}$-linear quasigroups and their representations of the free group on two generators. We exhibit non-isomorphic $\mathbb{Z}$-linear quasigroups with the same ordinary character. For a subclass of $\mathbb{Z}$-linear quasigroups, equivalences of the corresponding ordinary representations are realized by permutational intertwinings. This leads to a new equivalence relation on $\mathbb{Z}$-linear quasigroups, namely permutational similarity. Like the earlier concept of central isotopy, permutational similarity is intermediate between isomorphism and isotopy. The story progresses with a representation of the free quasigroup on a single generator. This provides the motivation behind the study of *peri-Catalan numbers*. While Catalan numbers index the number of length n magma words in a single generator, peri-Catalan numbers index the number of length n reduced form quasigroup words in a single generator. We derive a recursive formula for the n-th peri-Catalan number. This is a new sequence in that it is not on the Online Encyclopedia of Integer Sequences.

CHAPTER 1. INTRODUCTION

1.1 Preliminaries

The work in this dissertation is motivated by the study of quasigroups, which are nonassociative algebras. A common joke among mathematicians is that basic tasks such as arithmetic (and sometimes calculus) are more error-prone than highly abstract mathematics. Perhaps this is why the subject of nonassociativity inspires trepidation to the uninitiated. However, dear reader, if you have subtracted correctly in your life, you have worked with a nonassociative binary operation. This chapter will provide an introduction to two nonassociative algebras and lead up to the definition of quasigroups. Small examples will be given in this chapter to help illuminate some definitions and concepts for quasigroups. These examples were chosen for their relevance to later chapters.

Definition 1.1.1. A *magma* $(M, \cdot)$ is a set equipped with a single nonassociative binary operation $\cdot : M \times M \to M$.

One familiar example of a magma is the integers $(\mathbb{Z}, +)$. Addition is associative, so this may seem a strange example. While one may read "nonassociative binary operation" as an binary operation that is strictly *not* associative, realize that a magma is not particularly discriminatory with its binary operation. Those who have taken one semester of introductory abstract algebra will know there are many more labels we can place on $(\mathbb{Z}, +)$ than simply "magma." However, for the time being, we focus on binary operations. The integers, as we will soon see, provide a rich source of examples and stepping stones for the later chapters in this dissertation.

The following magma with a non-associative binary operation is a personal favorite.

Example 1.1.2. Let

$$- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}; (x, y) \mapsto x - y$$

the binary multiplication defined on the integers. We refer to this magma as the *integers under subtraction*, denoted $(\mathbb{Z}, -)$.

Alternatively, we can look at the following.

Example 1.1.3. The integers under an "opposite" subtraction $*$ with

$$* : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}; (x, y) \mapsto y - x$$

forms another non-associative magma.

Magmas serve a key role in the next part of the discussion.

Definition 1.1.4. A *Latin square* is an $n \times n$ array of n elements such that each element appears once in each row and column.

Consider the following 3×3 arrays:

Table 1.1 Two 3×3 Latin squares.

a	b	c
c	a	b
b	c	a

0	1	2
1	2	0
2	0	1

Filling in the borders for the second array, the Cayley table for $(\mathbb{Z}/3, +, 0)$ emerges.

$x + y$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Remark 1.1.5. The Cayley table of a finite group forms a Latin square.

A magma $(Q, \cdot)$ possesses the *Latin square property* if for any $x, y, z \in Q$, knowing any two arguments in the equation $x \cdot y = z$ uniquely specifies the third.

Example 1.1.6. Consider the integers under subtraction. Let x, y, z in $(\mathbb{Z}, -)$. Knowing any two arguments in the equation $x - y = z$ uniquely specifies the third term.

Definition 1.1.7. A *(combinatorial) quasigroup* $(Q, \cdot)$ is a magma that obeys the Latin square property.

The Latin square property of a quasigroup gives rise to left and right divisions. Let $(Q, \cdot)$ be a quasigroup and $x, y, z \in Q$. Consider the problem of solving for x in the equation $x \cdot y = z$. We introduce the symbol / and use it as follows:

$$\begin{aligned} x \cdot y &= z \\ (x \cdot y)/y &= z/y \\ x &= z/y \end{aligned}$$

The element x is multiplied on the right by y, so dividing by y on the right will isolate x. We refer to / as right division and read z/y as "z divided by y."

Similarly, if we solved for y in the equation $x \cdot y = z$, we use the symbol $\backslash$ to represent division on the left. We have

$$y = x\backslash z$$

We refer to $\backslash$ as left division. We read $x\backslash z$ as "x dividing z." Since a combinatorial quasigroup obeys the Latin square property, this is equivalent to saying right and left inverses are unique in a quasigroup.

While Definition 1.1.7 is a serviceable definition that builds up from magmas and the Latin square property, it does not sufficiently capture the structure of a quasigroup. The homomorphic image of a combinatorial quasigroup need not be a quasigroup [13, Ex. 1.10.2]. The uniqueness of right and left inverses may not be preserved in the homomorphic image. We rely on an equational definition for a quasigroup, formulated as follows:

Definition 1.1.8. A *quasigroup* $(Q, \cdot, /, \backslash)$ is a set equipped with three binary operations, multiplication $\cdot$, right division /, and left division $\backslash$ such that for all $x, y \in Q$, the following identities are satisfied:

$$\begin{aligned} &\text{(SL)} \quad x \cdot (x\backslash y) = y\,; \qquad \text{(SR)} \quad y = (y/x) \cdot x\,; \\ &\text{(IL)} \quad x\backslash(x \cdot y) = y\,; \qquad \text{(IR)} \quad y = (y \cdot x)/x\,. \end{aligned} \tag{1.1}$$

We explain the labels (SL), (SR), (IL), and (IR) in Section 1.2.

Example 1.1.9. The integers under subtraction $(\mathbb{Z}, -, /, \backslash)$ form an equational quasigroup, with $x/y := x + y$ and $x\backslash y := x - y$.

$$(x \cdot y)/y = (x - y) + y = x \qquad x\backslash(x \cdot y) = x - (x - y) = y$$

Example 1.1.10. Every group is an associative quasigroup. A quick comparison of the (SL) and (SR) identities in a quasigroup and a group help demonstrate this fact.

Identity	Quasigroup	Group
(SL)	$x \cdot (x\backslash y) = y$	$x \cdot (x^{-1}y) = y$
(SR)	$y = (y/x) \cdot x$	$y = (yx^{-1}) \cdot x$

Example 1.1.11. The finite quasigroup $(\mathbb{Z}/3, -, /, \backslash)$ has $x \cdot y = x - y$, $x/y := x + y$ and $x\backslash y := x - y$ as well.

1.2 Combinatorial Multiplication Groups

Let $(Q, \cdot, /, \backslash)$ be a quasigroup and $q \in Q$. The *right multiplication map* is defined as

$$R(q) : Q \to Q; x \mapsto x \cdot q.$$

The *left multiplication map* is similarly defined as

$$L(q) : Q \to Q; x \mapsto q \cdot x.$$

The injectivity of $R(q)$ is given by the (IR) identity $y = (y \cdot x)/x$ while the surjectivity of $R(q)$ is given by the (SR) identity $y = (y/x) \cdot x$. Meanwhile, the (IL) and (SL) identities give the injectivity and surjectivity of any $L(q)$ map, respectively. We denote the set of bijections from $Q \to Q$ as $Q!$. The *(combinatorial) multiplication group* of Q, denoted $\mathrm{Mlt}Q$, is the subgroup of $Q!$ generated by $\{L(q), R(q) | q \in Q\}$.

1.3 Outline of the Dissertation

This dissertation has three main storylines. The titular characters in the first story (Chapter 2) are linear quasigroups. We saw two examples of such quasigroups in Examples 1.1.9 and 1.1.11. These quasigroups are built on top of additive abelian groups in that we define nonassociative binary operations with an additive abelian group as the underlying set.

In general, quasigroups are nonassociative. Quasigroups are not even required to possess an identity element or even be non-empty. Those that do possess an identity element are called *loops*, but this work does not involve loops. A less restrictive notion than an identity element is a quasigroup with a pointed idempotent element. An element e in a quasigroup $(Q, \cdot, /, \backslash)$ is *idempotent* if $e \cdot e = e$. The linear quasigroups featured in Chapter 2 possess idempotent elements. The structure of linear quasigroups with an idempotent element possesses strong ties to the underlying abelian groups. This allows us to use tools from group representation theory to determine a partial isomorphism invariant for linear quasigroups. The main result of this work is Theorem 2.3.10, which provides an isomorphism invariant for a class of linear quasigroups.

The study of peri-Catalan numbers in Chapter 3 is motivated by a non-faithful representation of the free quasigroup on a single generator. While this work is relatively self-contained, the deeper motivation is given in Chapter 4. Chapter 3 heavily features quasigroup identities. The definition of an equational quasigroup contains four identities, with two more hidden in the background. For elements x, y in a quasigroup $(Q, \cdot, /, \backslash)$, we have:

$$\begin{aligned} & y \cdot (y\backslash x) = x && \text{(SL)} \\ \Rightarrow \quad & (y \cdot (y\backslash x))/(y\backslash x) = x/(y\backslash x) \\ \Rightarrow \quad & y = x/(y\backslash x) && \text{(DL)} \end{aligned}$$

A similar computation yields the (DR) identity $(x/y)\backslash = y$.

Catalan numbers arise in many combinatorial problems. One application of the Catalan numbers involves length n magma words in a single generator (§3.2). The quick story is that peri-Catalan numbers count the number of length n quasigroup words in a single generator (§ 3.3 and § 3.4). Chapter 3 defines the peri-Catalan numbers in greater detail.

After the formal definition of the peri-Catalan numbers, we outline the inductive process for generating the n-th peri-Catalan number. This chapter concludes with Theorem 3.8.14 which provides a recursion for the peri-Catalan numbers.. There are many supporting results used in the proof of this theorem. We provide details for most of these proofs.

Chapter 4 revisits quasigroup representations. One can define a differential calculus on the free quasigroup on a single generator analogous to the Fox derivative for groups. Derivation is a homomorphism from the free quasigroup on a single generator to the nonassociative analogue of the integers. Derivation is faithful on magma words in a single generator, while Proposition 4.3.4 highlights how derivation is not faithful on quasigroup words.

The final chapter outlines future directions for each of the three main storylines.

CHAPTER 2. ISOMORPHISM INVARIANTS FOR LINEAR PIQUES

2.1 Introduction

Quasigroups $(Q, \cdot)$ are nonassociative analogues of groups, retaining the cancelativity of the multiplication. A pique[1] $(P, \cdot, e)$ is a quasigroup with a nullary operation that selects an idempotent element e. The inner multiplication group of a pique P is the stabilizer of e in the group of permutations of P generated by all the right and left multiplications.

For a commutative, unital ring S, an S-linear pique or S-linear quasigroup is an S-module A equipped with automorphisms ρ and λ that furnish a pique multiplication $x \cdot y = x^\rho + y^\lambda$, with 0 as the pointed idempotent. Two S-linear piques are S-isomorphic if they are isomorphic via an invertible S-linear transformation (module isomorphism).

Finite-dimensional $\mathbb{C}$-linear piques are classified up to $\mathbb{C}$-linear isomorphism by their so-called ordinary characters, obtained from the representation of the free group on two generators that they afford. Given a finite $\mathbb{Z}$-linear pique A, one may linearize the underlying combinatorial structure to obtain a $\mathbb{C}$-linear pique $\mathbb{C}A$, the so-called complexification of the $\mathbb{Z}$-linear pique A. Our primary concern is the extent to which ordinary characters of complexifications classify $\mathbb{Z}$-linear piques. The main result (Theorem 2.3.10) shows that for a large class of $\mathbb{Z}$-linear pique structures, namely on cyclic groups of order not divisible by 8, two piques that have the same complexified ordinary character are permutationally similar, i.e., the permutation actions of their respective inner multiplication groups are similar.

[1] An acronym for "Pointed Idempotent QUasigroup(E)".

2.1.1 Outline of the chapter

We begin with definitions and examples of quasigroups and linear quasigroups in Section 2.2. We define linear quasigroups and their S-linear representations for a commutative unital ring S. Theorem 2.2.12 identifies S-linear piques with the S-linear representations of the free group on two generators that they afford. This allows us to study the representations in lieu of the piques. Permutational similarity is defined in §2.2.4, while §2.2.5 defines ordinary characters and the complexifications of $\mathbb{Z}$-linear piques. Theorem 2.2.16 observes that isomorphic $\mathbb{Z}$-linear piques have the same ordinary character.

The central Section 2.3 considers isomorphism invariants for $\mathbb{Z}$-linear piques on cyclic groups of finite order not divisible by 8. Linear piques defined on $\mathbb{Z}/_n$ for $n < 5$ are classified up to isomorphism by the ordinary characters of their complexifications, the permutation characters introduced in Definition 2.3.1 (§2.3.2). However, ordinary character theory does not suffice to cover all linear piques. Indeed, Proposition 2.3.11 exhibits non-isomorphic pique structures on $\mathbb{Z}/_5$ having the same permutation character. The main result (Theorem 2.3.10) states that linear piques defined on cyclic groups of order not divisible by 8, having the same permutation character, are permutationally similar.

The concluding Section 2.4 examines the classification of $\mathbb{Z}$-linear pique structures on $\mathbb{Z}/_{2^n}$ for $n \geq 3$. We exhibit pique structures on the cyclic group of order 16, with the same permutation character, which are neither isomorphic nor permutationally similar (Theorem 2.4.2).

2.1.2 Related invariants

Given a commutative, unital ring S and an S-module A, the S-linear piques constructed on A are all isotopic to the abelian group $(A, +, 0)$. As such, their classification up to isomorphism may be regarded as a special case of the main problem considered by Drápal in [5], namely the isomorphism problem for isotopes of a given (not necessarily abelian) group. However, the general solution to the isomorphism problem offered by [5] is computationally intractable, leaving open the search for less powerful but more accessible invariants. This situation is analogous to that prevailing in knot theory, where the existence of complete invariants does

not preclude the continuing search for weaker invariants with a lower computational complexity.

2.1.3 Conventions

The paper follows the general algebraic convention of placing a function to the right of its argument, either on the line or as a superfix. This convention allows composites of functions to be read in natural order from left to right, and serves to minimize the occurrence of brackets, which otherwise proliferate when one studies non-associative structures.

2.2 Linear Piques

2.2.1 Quasigroups and piques

Definition 2.2.1. A *quasigroup* $(Q, \cdot, \backslash, /)$ is an algebra with three binary operations, multiplication $\cdot$, left division $\backslash$, and right division $/$, such that for all $x, y \in Q$,

$$y\backslash(y \cdot x) = x = (x \cdot y)/y \tag{2.1}$$

$$y \cdot (y\backslash x) = x = (x/y) \cdot y \tag{2.2}$$

are satisfied.

Definition 2.2.2. A *pique* $(Q, \cdot, /, \backslash, e)$ is a quasigroup with a pointed idempotent element e such that $e \cdot e = e$.

Definition 2.2.3. [13§2.4] Let $(Q, \cdot, /, \backslash, e)$ be a pique. The stabilizer of e in the group of permutations of Q generated by all the right multiplications $R(q)\colon x \mapsto x \cdot q$ and left multiplications $L(q)\colon x \mapsto q \cdot x$ (for $q \in Q$) is called the *inner multiplication group* of the pique.

A pique is a pointed set, where the idempotent element serves as the basepoint. Maps between pointed sets send basepoint to basepoint. For pique homomorphisms, the pointed idempotent element of the domain maps to the pointed idempotent element of the codomain.

Example 2.2.4. Each group is an associative pique, with the identity element as the pointed idempotent element. The inner multiplication group is the inner automorphism group.

Example 2.2.5. Integers under subtraction form a nonassociative pique, with 0 as the pointed idempotent. The unique nontrivial element of the inner multiplication group is negation.

2.2.2 Linear piques

Definition 2.2.6. Suppose that S is a commutative, unital ring. A pique $(A, \cdot, /, \backslash, 0)$ is said to be *S-linear* if there is a unital S-module structure $(A, +, 0)$, with automorphisms λ and ρ such that

$$x \cdot y = x^{\rho} + y^{\lambda},\ x/y = (x - y^{\lambda})^{\rho^{-1}}, \text{and } x\backslash y = (y - x^{\rho})^{\lambda^{-1}} \tag{2.3}$$

for $x, y \in A$.

We identify λ, ρ as the left and right multiplications by the pointed idempotent 0. For a finite S-linear quasigroup, we can read off ρ and λ from the multiplication table. The first row gives us left multiplication by 0 and the first column gives us right multiplication by 0.

Example 2.2.7. On the one hand, the quasigroup $(\mathbb{Z}/_4, x \circ_1 y)$ with the nonassociative multiplication $x \circ_1 y = x(1\ 2\ 3) + y(1\ 2)$ is a pique with 0 as the pointed idempotent element. However, neither $(1\ 2\ 3)$ nor $(1\ 2)$ is an automorphism of $\mathbb{Z}/_4$. On the other hand, the quasigroup $(\mathbb{Z}/_4, x \circ_2 y)$ with the nonassociative multiplication $x \circ_2 y = x(1\ 3) + y(1\ 3)$ is also a pique with 0 as the pointed idempotent element. More importantly, the permutation $(1\ 3)$ corresponds to the automorphism of $\mathbb{Z}/_4$ defined by $x \mapsto 3x$, so $(\mathbb{Z}/_4, x \circ_2 y)$ is a $\mathbb{Z}$-linear pique.

Example 2.2.8. [14§3] Linear representations of two-generated groups are equivalent to piques.

Remark 2.2.9. Linear piques, and their shifted versions $x \cdot y = x^{\rho} + y^{\lambda} + c$ (also described as "T-quasigroups" [2, 9]), have been studied for potential applications in cryptography and related fields [1].

2.2.3 Equivalent representations

Throughout this section, S will denote a commutative, unital ring.

Definition 2.2.10. Let $\langle R, L \rangle$ be the free group on the doubleton $\{R, L\}$.

(a) Let $(A, \cdot, /, \backslash, 0)$ be an S-linear pique with $x \cdot y = x^{\rho} + y^{\lambda}$. Then the group homomorphism

$$\alpha \colon \langle R, L \rangle \to \mathrm{Aut}_S(A, +, 0); R \mapsto \rho\,,\ L \mapsto \lambda$$

is described as the *S-linear representation* that is *afforded* by $(A, \cdot, /, \backslash, 0)$.

(b) Consider two S-modules $(A,+,0)$ and $(B,+,0)$. Then corresponding S-linear representations $\alpha\colon \langle R,L\rangle \to \mathrm{Aut}_S(A,+,0)$ and $\beta\colon \langle R,L\rangle \to \mathrm{Aut}_S(B,+,0)$ are *equivalent* whenever there exists an S-module isomorphism $f : A \to B$ such that for all a in A and g in $\langle R,L\rangle$, the diagram

$$\begin{array}{ccc} A & \xrightarrow{g^\alpha} & A \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ B & \xrightarrow[g^\beta]{} & B \end{array} \tag{2.4}$$

commutes. We call f the *intertwining*.

Note that the pair of equations

$$R^\alpha f = fR^\beta \qquad \text{and} \qquad L^\alpha f = fL^\beta \tag{2.5}$$

is equivalent to the commuting of (2.4). Alternatively, one may require that the diagram

$$\begin{array}{ccccc} A & \xleftarrow{L^\alpha} & A & \xrightarrow{R^\alpha} & A \\ {\scriptstyle f}\downarrow & & {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ B & \xleftarrow[L^\beta]{} & B & \xrightarrow[R^\beta]{} & B \end{array} \tag{2.6}$$

commutes.

Lemma 2.2.11. *Suppose that $f\colon (A,\circ_1) \to (B,\circ_2)$ is a pique isomorphism between S-linear piques $(A,\circ_1)$ and $(B,\circ_2)$. Let α and β be the respective S-linear representations that they afford. Then the equations (2.5) hold.*

Proof. One has

$$aR^\alpha f = (a \circ_1 0)^f = a^f \circ_2 0 = a^f R^\beta \quad \text{and}$$
$$aL^\alpha f = (0 \circ_1 a)^f = 0 \circ_2 a^f = a^f L^\beta.$$

for each element a of A. □

Theorem 2.2.12. *Let $(A,\circ_1)$ and $(B,\circ_2)$ be two S-linear piques. Then they are isomorphic by an S-linear transformation $f\colon A \to B$ if and only if the S-linear representations they afford are equivalent.*

Proof. Let $f\colon (A,\circ_1) \to (B,\circ_2)$ be an S-linear pique isomorphism. Suppose that $\alpha\colon \langle R,L\rangle \to \mathrm{Aut}(A,+,0)$ and $\beta\colon \langle R,L\rangle \to \mathrm{Aut}(B,+,0)$ are the respective S-linear representations afforded by the S-linear piques. By Lemma 2.2.11, the equations (2.5) hold. It follows that f is an intertwining witnessing the equivalence of α and β.

Now let $\alpha\colon \langle R,L\rangle \to \mathrm{Aut}(A,+,0)$ and $\beta\colon \langle R,L\rangle \to \mathrm{Aut}(B,+,0)$ be equivalent S-linear representations, with an intertwining $f\colon A \to B$. Then for x,y in A, one has

$$\begin{aligned}(x \circ_1 y)f &= (xR^\alpha + yL^\alpha)f \\ &= (xR^\alpha)f + (yL^\alpha)f \\ &= xfR^\beta + yfL^\beta \\ &= xf \circ_2 yf\,,\end{aligned}$$

so that $f\colon (A,\circ_1) \to (B,\circ_2)$ is an S-linear pique isomorphism. □

2.2.4 Permutational similarity

In what follows, we will consider a modified version of the commuting diagram (2.6).

Definition 2.2.13. Let A be a finite abelian group, with $\mathbb{Z}$-linear pique structures $(A,\circ_1)$ and $(A,\circ_2)$ affording respective representations

$$\alpha_i\colon \langle R,L\rangle \to \mathrm{Aut}(A,+,0)$$

for $i = 1,2$. Then the piques $(A,\circ_1)$ and $(A,\circ_2)$, or the representations they afford, are said to be *permutationally similar*, via a permutation π of the underlying set A, if the diagram

$$\begin{array}{ccccc} A & \xleftarrow{L^{\alpha_1}} & A & \xrightarrow{R^{\alpha_1}} & A \\ {\scriptstyle\pi}\downarrow & & {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ A & \xleftarrow[L^{\alpha_2}]{} & A & \xrightarrow[R^{\alpha_2}]{} & A \end{array} \tag{2.7}$$

commutes. In other words, the permutation π conjugates both R^{α_1} to R^{α_2} and L^{α_1} to L^{α_2} within the permutation group $A!$ of the set A.

Consider two permutationally similar piques $(A,\circ_1)$ and $(A,\circ_2)$ as in Definition 2.2.13. If π is not an automorphism of the abelian group $(A,+,0)$, then the permutational similarity

of representations furnished by π is not an equivalence in the sense of Definition 2.2.10. On the other hand, since both the piques are isotopic to the abelian group A, they are mutually isotopic. Furthermore, Theorem 2.2.12 shows that if two $\mathbb{Z}$-linear piques on the abelian group A are isomorphic, then they are permutationally similar. Thus permutational similarity is a relationship intermediate between isotopy and isomorphism. As such, it is analogous to the relationship of central isotopy [13§3.4].

2.2.5 Ordinary characters of $\mathbb{C}$-linear piques

Definition 2.2.14. Let G be a group. For a complex vector space V, let $\mathsf{GL}(V)$ be its group of automorphisms.

(a) An *ordinary linear representation* of G is defined as a homomorphism $\rho : G \to \mathsf{GL}(V)$, for some finite-dimensional complex vector space V.

(b) The (*ordinary*) *character* of an ordinary linear representation $\rho\colon G \to \mathsf{GL}(V)$ is the function χ or $\chi_\rho\colon G \to \mathbb{C}; g \mapsto \mathrm{Tr}(g\rho)$.

Definition 2.2.15. Let $(A, \cdot, /, \backslash, 0)$ be a finite $\mathbb{Z}$-linear pique, affording the $\mathbb{Z}$-linear representation $\alpha : \langle R, L\rangle \to \mathrm{Aut}(A, +, 0)$. Let $\mathbb{C}A$ be the complex vector space with basis A. Then the *complexification* of $(A, \cdot, /, \backslash, 0)$ is the $\mathbb{C}$-linear pique structure $(\mathbb{C}A, \cdot, /, \backslash, 0)$ obtained by extension of the pique structure $(A, \cdot, /, \backslash, 0)$. Thus

$$\alpha_{\mathbb{C}}\colon R \mapsto (\mathbb{C}A \to \mathbb{C}A; a \mapsto aR^\alpha)\,,\ L \mapsto (\mathbb{C}A \to \mathbb{C}A; a \mapsto aL^\alpha)$$

serves to specify the $\mathbb{C}$-linear representation $\alpha_{\mathbb{C}}$ that is afforded by the complexification of $(A, \cdot, /, \backslash, 0)$.

Theorem 2.2.16. *Let $f\colon (A, \cdot, /, \backslash, 0) \to (B, \cdot, /, \backslash, 0)$ be an isomorphism of finite $\mathbb{Z}$-linear piques affording respective $\mathbb{Z}$-linear representations α and β. Then the respective $\mathbb{C}$-linear representations $\alpha_{\mathbb{C}}$ and $\beta_{\mathbb{C}}$ of their complexifications have the same ordinary character.*

Proof. The bijection $f\colon A \to B$ may be extended to a unique $\mathbb{C}$-linear isomorphism $\mathbb{C}f\colon \mathbb{C}A \to \mathbb{C}B$. By Lemma 2.2.11, one has $g^\alpha f = fg^\beta$ for all g in $\langle R, L\rangle$. By linearity, one then has

$g^{\alpha_{\mathbb{C}}}(\mathbb{C}f) = (\mathbb{C}f)g^{\beta_{\mathbb{C}}}$ for all g in $\langle R, L\rangle$. Let χ_A and χ_B be the respective characters of $\alpha_{\mathbb{C}}$ and $\beta_{\mathbb{C}}$. Then

$$\chi_B(g\beta_{\mathbb{C}}) = \mathrm{Tr}(g\beta_{\mathbb{C}}) = \mathrm{Tr}\big((\mathbb{C}f)^{-1}g^{\alpha_{\mathbb{C}}}(\mathbb{C}f)\big) = \mathrm{Tr}(g\alpha_{\mathbb{C}}) = \chi_A(g\alpha_{\mathbb{C}})$$

for each g in $\langle R, L\rangle$. □

Remark 2.2.17. Although the result will not be needed for subsequent work in the current paper, it should be noted that Theorem 2.2.12, along with Theorem 12.4 of [13], implies that finite-dimensional $\mathbb{C}$-linear quasigroups are classified, up to $\mathbb{C}$-linear isomorphism, by their ordinary characters.

2.3 Linear Piques on Finite Cyclic Groups

2.3.1 Permutation characters

The following definition provides a purely combinatorial specification for the character of the ordinary representation that is afforded by the complexification of a finite $\mathbb{Z}$-linear pique (compare [11, Exercise 2.2]).

Definition 2.3.1. Let $(A, \cdot, /, \backslash, 0)$ be a finite $\mathbb{Z}$-linear pique, affording the $\mathbb{Z}$-linear representation $\alpha : \langle R, L\rangle \to \mathrm{Aut}(A, +, 0)$. For an element g of $\langle R, L\rangle$, the *permutation character* $\chi(g)$ is the number of fixed points of the permutation g^{α} of the set A.

Although the group $\langle R, L\rangle$ is infinite, the permutation character is determined by the fixed-point numbers for each member of the finite set $\langle R, L\rangle^{\alpha}$ of permutations of A, the inner multiplication group of the pique $(A, \cdot, /, \backslash, 0)$. We generally use cycle notation for permutations of A, recognizing the number of fixed points of a permutation as the number of one-cycles in its cycle decomposition.

For $1 < n \in \mathbb{Z}$, we will consider $\mathbb{Z}$-linear piques defined on finite cyclic groups $(\mathbb{Z}/_n, +.0)$. We write $(\mathbb{Z}/_n)^*$ for the group of units of the monoid $(\mathbb{Z}/_n, \cdot, 1)$, the set of residues coprime to n. We use the isomorphism

$$(\mathbb{Z}/_n)^* \to \mathrm{Aut}(\mathbb{Z}/_n, +, 0); r \mapsto (x \mapsto rx)$$

[12, 5.7.11] to identify automorphisms of finite cyclic groups. Thus the order of the automorphism group $\mathrm{Aut}(\mathbb{Z}/_n, +, 0)$ is given by the Euler function $\varphi(n)$. We note the following for future reference.

Lemma 2.3.2. *Let p be a prime number, and let k be a positive integer. Then an automorphism of $\mathbb{Z}/_{p^k}$ has p^j many fixed points, for some $0 < j \leq k$.*

Proof. The set of fixed points of a group automorphism forms a subgroup of the group in question. The result then follows by Lagrange's Theorem. □

2.3.2 Linear piques on small cyclic groups

We build piques on $\mathbb{Z}/_3$ by assigning automorphisms of $(\mathbb{Z}/_3, +, 0)$ to R, L. Since R, L can be 1 or 2, we have four possibilities for the binary multiplication. Here, we exhibit the permutation character table for $\mathbb{Z}$-linear representations of each linear pique defined on $\mathbb{Z}/_3$.

Table 2.1 Permutation characters for linear piques on $\mathbb{Z}/_3$

$x \cdot y$	R	L	$\chi(R)$	$\chi(L)$
$x + y$	(1)	(1)	3	3
$x + 2y$	(1)	(1 2)	3	1
$2x + y$	(1 2)	(1)	1	3
$2x + 2y$	(1 2)	(1 2)	1	1

The ordinary characters of R, L are distinct for linear piques of order 3. By Theorem 2.2.16, the four piques are all mutually non-isomorphic. Thus the permutation character completely resolves the isomorphism classes of linear piques of order 3:

Proposition 2.3.3. *Linear piques defined on $\mathbb{Z}/_3$ are classified completely up to isomorphism by their permutation characters.*

In similar vein, one obtains the following:

Proposition 2.3.4. *Linear piques defined on each of $\mathbb{Z}/_2$ and $\mathbb{Z}/_4$ are classified completely up to isomorphism by their permutation characters.*

2.3.3 Cyclic groups of prime power order

Consider a cyclic group $\mathbb{Z}/_{p^k}$, where p is a prime and k is a positive integer.

Lemma 2.3.5. *[12, 5.7.12] If p is an odd prime and k is a positive integer, or $p = 2$ and $k \in \{1, 2\}$, then $\mathrm{Aut}(\mathbb{Z}/_{p^k}, +, 0)$ is a cyclic group of order $\varphi(p^k) = p^{k-1}(p-1)$.*

Lemma 2.3.6. *Let $\mathbb{Z}$-linear representations $\alpha_i : \langle R, L\rangle \to \mathrm{Aut}(\mathbb{Z}/_{p^k})$ have equal respective permutation characters χ_i, for $i = 1, 2$. Then for each element g of $\langle R, L\rangle$, the automorphisms g^{α_1} and g^{α_2} have the same order.*

Proof. Suppose, without loss of generality, that $s = |\langle g^{\alpha_1}\rangle| \geq |\langle g^{\alpha_2}\rangle| = t$. Then $\chi_1(g^t) = \chi_2(g^t) = p^k$, so that $g^{\alpha_1 t} = g^{t\alpha_1} = 1$ and $s \leq t$. □

Lemma 2.3.7. *[4, Ex. 2.1] Two permutation representations of a finite cyclic group, with the same character, are isomorphic.*

Proposition 2.3.8. *Let p be a prime number, and let k be a positive integer. Suppose that two linear pique structures defined on $\mathbb{Z}/p^k$ have the same permutation character. Suppose that one of the three following hypotheses applies:*

(a) *Let p be an odd prime;*

(b) *Let $p = 2$ and $k \in \{1, 2\}$;*

(c) *Let $p = 2$ and $k > 2$, but assume that the inner multiplication groups of the two piques are cyclic.*

Then the corresponding representations are permutationally similar.

Proof. Suppose that the piques correspond to respective representations $\alpha_i : \langle R, L\rangle \to \mathrm{Aut}(\mathbb{Z}/_{p^k})$, for $i = 1, 2$. Suppose, without loss of generality, that $|\langle R, L\rangle^{\alpha_1}| \geq |\langle R, L\rangle^{\alpha_2}|$. Let g be an element of $\langle R, L\rangle$ whose image under α_1 generates $\langle R, L\rangle^{\alpha_1}$, so the order of g^{α_1} is $|\langle R, L\rangle^{\alpha_1}|$. Then by Lemma 2.3.6, the order of g^{α_2} is $|\langle R, L\rangle^{\alpha_1}|$. Thus $|\langle R, L\rangle^{\alpha_1}| = |\langle R, L\rangle^{\alpha_2}|$, and g^{α_2} generates $\langle R, L\rangle^{\alpha_2}$. Consider the finite cyclic group $G \cong \langle g^{\alpha_1}\rangle \cong \langle g^{\alpha_2}\rangle$, with permutation representations $\gamma_i \colon G \to \mathrm{Aut}(\mathbb{Z}/_{p^k}); g^{\alpha_i t} \mapsto g^{t\alpha_i}$ for $i = 1, 2$. The respective permutation characters are equal,

so by Lemma 2.3.7, the two permutation representations γ_i of G are isomorphic. It follows that the representations α_1, α_2 are permutationally similar. □

2.3.4 Cyclic groups of order not divisible by 8

For any positive integer m, consider a factorization

$$m = \prod_{i=1}^{s} p_i^{k_i}$$

with distinct primes $p_1 < \ldots < p_s$ for $1 \leq i \leq s$. Write $q_i = p_i^{k_i}$ for $1 \leq i \leq s$. We refer to q_i as the *p_i-part* of m. Now for $1 < n \in \mathbb{Z}$, fix the notation $n = \prod_{i=1}^{s} p_i^{k_i}$, with distinct primes $p_1 < \ldots < p_s$ and positive exponents $k_1, \ldots, k_s$, for $1 \leq i \leq s$.

Proposition 2.3.9. *[12, 5.7.3] Let A be an abelian group of order n. For $1 \leq i \leq s$, let A_i be the Sylow p_i-subgroup of A. Then* $\mathrm{Aut}(A) \cong \prod_{i=1}^{s} \mathrm{Aut}(A_i)$.

The Chinese Remainder Theorem gives a direct sum decomposition

$$c\colon \mathbb{Z}/_n \to \bigoplus_{i=1}^{s} \mathbb{Z}/_{q_i}; x \mapsto (x_1, \ldots, x_s)\,. \tag{2.8}$$

In turn, application of Proposition 2.3.9 to the cyclic group $\mathbb{Z}/_n$ yields the isomorphism

$$a\colon \mathrm{Aut}(\mathbb{Z}/_n) \to \prod_{i=1}^{s} \mathrm{Aut}(\mathbb{Z}/_{q_i}); \theta \mapsto (\theta_1, \ldots, \theta_s)\,. \tag{2.9}$$

For an automorphism θ of $\mathbb{Z}/_n$, let $\pi(\theta)$ be the number of fixed points of θ. For $1 \leq i \leq s$, let $\pi_i(\theta_i)$ be the number of fixed points of θ_i on $\mathbb{Z}/_{q_i}$. By virtue of the set isomorphism $c\colon \mathbb{Z}/_n \to \prod_{i=1}^{s} \mathbb{Z}/_{q_i}$, one has

$$\pi(\theta) = \prod_{i=1}^{s} \pi_i(\theta_i)\,.$$

Then by Lemma 2.3.2, $\pi_i(\theta_i)$ is the p_i-part of $\pi(\theta)$.

Now restrict the fixed integer n by requiring that it not be divisible by 8. In our notation, this means that $k_1 < 3$ if $p_1 = 2$. As a consequence, the automorphism groups $\mathrm{Aut}(\mathbb{Z}/_{q_i})$ are all cyclic.

Theorem 2.3.10. *Let A be a finite cyclic group whose order is not divisible by 8. Then if two $\mathbb{Z}$-linear piques on A have the same permutation character, they are permutationally similar.*

Table 2.2 Permutations for the automorphisms of $\mathbb{Z}/_5$

Automorphism	1	2	3	4
Permutation	(1)	(1 2 4 3)	(1 3 4 2)	(1 4)(2 3)

Proof. By transport of structure, it suffices to examine the case where $A = \mathbb{Z}/_n$, with notation as above. Consider the representations α, α' of $\langle R, L\rangle$ corresponding to the two pique structures. Suppose that their respective permutation characters are χ and χ'. By the hypothesis, these characters coincide. In particular, for each element g of $\langle R, L\rangle$, and for each $1 \leq i \leq s$, the respective p_i-parts of $\chi_i(g)$ and $\chi'_i(g)$ of $\chi(g)$ and $\chi'(g)$ coincide.

For each $1 \leq i \leq s$, and for each element g of $\langle R, L\rangle$, define $g^{\alpha_i} = (g^\alpha)_i$ and $g^{\alpha'_i} = (g^{\alpha'})_i$ using the notation embodied in (2.9). One obtains respective representations α_i and α'_i of $\langle R, L\rangle$ on $\mathbb{Z}/_{q_i}$, with equal permutation characters $\chi_i(g)$ and $\chi'_i(g)$. By Proposition 2.3.8, it follows that these representations are permutationally similar, say by permutations $b_i \colon \mathbb{Z}/_{q_i} \to \mathbb{Z}/_{q_i}$. Then the permutation b of $\mathbb{Z}/_n$, defined by setting $xb = (x_1b_1, \ldots, x_sb_s)c^{-1}$ in the notation of (2.8), yields the desired permutation similarity between α and α'. □

2.3.5 Linear piques on $\mathbb{Z}/_5$

Now we consider an explicit example of the preceding work using linear piques defined on $\mathbb{Z}/_5$. Automorphisms of $\mathbb{Z}/_5$ are given by multiplication by non-zero elements. The following table lists the permutations for each element in $(\mathbb{Z}/_5)^*$.

Let $x \circ_1 y = x + 2y$ and $x \circ_2 y = x + 3y$. Since the identity $(xx)x = (yy)y$ holds in $(\mathbb{Z}/_5, \circ_1)$, but not in $(\mathbb{Z}/_5, \circ_2)$, the respective piques are certainly not isomorphic, even as magmas under the quasigroup multiplication.

On the other hand, the representations of $(\mathbb{Z}/_5, \circ_1)$ and $(\mathbb{Z}/_5, \circ_2)$ have the same permutation character. In each case, R maps to the identity, and L maps to a 4-cycle. Let $\{e_i \mid 0 \leq i < 5\}$

be the standard basis for $\mathbb{C}^5$. Consider the permutation matrix

$$P_{(2\ 3)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

of the permutation (2 3). Define the linear transformation

$$\tau : \mathbb{C}^5 \to \mathbb{C}^5; e_i \mapsto e_i P_{(2\ 3)}\,.$$

Since the 4-cycles (1 2 4 3) and (1 3 4 2) are conjugated by (2 3), the ordinary representations for the non-isomorphic $\mathbb{Z}$-linear piques $(\mathbb{Z}/_5, \circ_1)$ and $(\mathbb{Z}/_5, \circ_2)$ are permutationally similar. We may summarize as follows.

Proposition 2.3.11. *There is a pair of $\mathbb{Z}$-linear piques on $\mathbb{Z}/_5$ which have the same permutation character, and are permutationally similar, but which are not isomorphic.*

2.4 Linear Piques Defined on $\mathbb{Z}/_{2^k}$

As recorded in Proposition 2.3.4, linear piques defined on $\mathbb{Z}/_2$ and $\mathbb{Z}/_4$ are classified up to isomorphism by their permutation characters. In this section, we examine the classification of $\mathbb{Z}$-linear pique structures on $\mathbb{Z}/_{2^k}$ for $k \geq 3$. For each positive integer k, the group of units of the monoid of integers modulo 2^k consists of the non-zero odd residues.

2.4.1 The case of $\mathbb{Z}/_8$

Let us consider linear piques defined on $\mathbb{Z}/_8$. To construct a $\mathbb{Z}$-linear pique on $\mathbb{Z}/_8$, we must assign ρ, λ the values 1, 3, 5, or 7. The following table lists the permutations for each element in $(\mathbb{Z}/_8)^*$.

If two linear piques have the same permutation characters, then the permutations associated with R, L must have the same cycle type. The only possibilities for isomorphic ordinary representations are listed in the following table. We omit opposite quasigroups.

Table 2.3 Permutations for the automorphisms of $\mathbb{Z}/_8$

Automorphism	1	3	5	7
Permutation	(1)	(1 3)(2 6)(5 7)	(1 5)(3 7)	(1 7)(2 6)(3 5)

Table 2.4 Partial character table for linear piques on $\mathbb{Z}/_8$

$x \cdot y$	R	L	$\chi(R)$	$\chi(L)$	$\chi(L^2)$	$\chi(RL)$
$x+3y$	(1)	(1 3)(2 6)(5 7)	8	2	8	2
$x+7y$	(1)	(1 7)(2 6)(3 5)	8	2	8	2
$5x+3y$	(1 5)(3 7)	(1 3)(2 6)(5 7)	4	2	8	2
$5x+7y$	(1 5)(3 7)	(1 7)(2 6)(3 5)	4	2	8	2

The permutations for 3 and 7 are conjugated by (3 7), while those for 1 and 5 are fixed under conjugation by (3 7). Thus for equivalent complexified ordinary representations, the permutation matrix $P_{(3\ 7)}$ serves as a permutation intertwining. We may summarize as follows.

Proposition 2.4.1. *If a pair of $\mathbb{Z}$-linear piques on $\mathbb{Z}/_8$ have the same permutation character, then they are permutationally similar.*

2.4.2 Computing permutations for automorphisms of $\mathbb{Z}/_{2^k}$

For consideration of linear piques defined on $\mathbb{Z}/_{2^k}$ for $k \geq 4$, it becomes unwieldy to determine the permutations implemented by each automorphism of $\mathbb{Z}/_{2^k}$ by hand. Instead, we use a program to list the permutations, and to enumerate their fixed points. We illustrate the process by computing the permutations for automorphisms of $\mathbb{Z}/_{16}$.

The residue 1 corresponds to the identity permutation. To compute the permutation for the automorphism $x \mapsto 3x$, the program generates cycles in disjoint cycle notation as follows: $1 * 3 = 3,\ 3 * 3 = 9,\ 9 * 3 = 11,\ 11 * 3 = 1$. Once an element is congruent to the starting element of the cycle (in this case 1), the program stops the process and outputs the cycle — here (1 3 9 11). The elements that appear in this cycle are removed from the list of odd integers modulo 16. The program takes the next smallest element from the list of remaining integers modulo 16, and repeats the process. Since $2 * 3 = 6$ and $6 * 3 = 2$ modulo 16, this computation gives us the transposition (2 6). The program appends it to the first cycle, so we

have (1 3 9 11)(2 6). Then 2 and 6 are removed from the list, and the process continues. The program stops when the list of remaining integers modulo 16 is empty. Once the process is complete for a given automorphism, it moves on to the next smallest representative element of $(\mathbb{Z}/_{16})^*$, until there are no more.

For each permutation, the program computes the number of fixed points. For a given element u in $(\mathbb{Z}/_{16})^*$, the program checks if $au \equiv a \mod 16$ for each $a \in \mathbb{Z}/_{16}$. If the equation holds, then the program adds 1 to the number of fixed points for the permutation associated with u. The information is compiled into Table 2.5.

Table 2.5 Automorphisms of $\mathbb{Z}/_{16}$: permutations and fixed point counts

Autom.	Permutation	Fixed points
1	(1)	16
3	(1 3 9 11)(2 6)(4 12)(5 15 13 7)(10 14)	2
5	(1 5 9 13)(2 10)(3 5 11 7)(6 14)	4
7	(1 7)(2 14)(3 5)(4 12)(6 10)(9 15)(11 13)	2
9	(1 9)(3 11)(5 13)(7 15)	8
11	(1 11 9 3)(2 6)(4 12)(5 7 13 15)(10 14)	2
13	(1 13 9 5)(2 10)(3 7 11 15)(6 14)	4
15	(1 15)(2 14)(3 13)(4 12)(5 11)(6 10)(7 9)	2

2.4.3 Linear piques on $\mathbb{Z}/_{16}$

Linear piques on $\mathbb{Z}/_{16}$ are summarized in Table 2.6. We are only concerned with piques having non-cyclic inner multiplication groups, since the piques with cyclic inner multiplication groups are handled by Proposition 2.3.8(c). In addition, we have chosen single representatives from each pair of mutually opposite quasigroups. In the first column of the table, each pique is identified by the respective right multiplication ρ and left multiplication λ by 0.

For each pique listed, the table provides summary information on the permutation character. Note that elements in $(\mathbb{Z}/_{16})^*$ have order 1, 2, or 4, since $(\mathbb{Z}/_{16})^* \equiv C_2 \times C_4$. Thus when considering which words from $\langle R, L \rangle$ will have their permutation character displayed in Table 2.6, it suffices to take powers of R, L strictly less than 4.

For any right multiplication by 0 in a $\mathbb{Z}/_{16}$ pique, $\rho^4 = 1$, so we exclude duplicate columns

such as R^4L and L. These will yield the exact same character regardless of the pique. The choices for the columns are not unique.

Table 2.6 Partial character table for linear piques on $\mathbb{Z}/_{16}$

ρ	λ	$\chi(RL)$	$\chi(RL^2)$	$\chi(RL^3)$	$\chi(R)$	$\chi(R^2)$	$\chi(R^3)$	$\chi(L^2)$
5	3	2	4	2	4	8	4	8
5	11	2	4	2	4	8	4	8
13	3	2	4	2	4	8	4	8
13	11	2	4	2	4	8	4	8
13	7	2	4	2	4	8	4	16
13	15	2	4	2	4	8	4	16
5	7	2	4	2	4	8	4	16
5	15	2	4	2	4	8	4	16
9	7	2	8	2	8	16	8	16
9	15	2	8	2	8	16	8	16
11	7	4	2	4	2	8	2	16
3	15	4	2	4	2	8	2	16
3	7	4	2	4	2	8	2	16
11	15	4	2	4	2	8	2	16
7	15	8	2	8	2	16	2	16

Table 2.7 lists the permutations that fix or conjugate elements in $(\mathbb{Z}/_{16})^*$.

Table 2.7 Conjugation relations of elements in $(\mathbb{Z}/_{16})^*$

Permutation	Fixes	Conjugates
$\sigma = (3\ 11)(7\ 15)$	5, 13, 9	3 and 11, 7 and 15
$\tau = (7\ 15)(5\ 13)$	3, 11, 9	5 and 13, 7 and 15

The top four rows of the body of Table 2.6 exhibit four linear piques that yield the same permutation character. Since we want to consider a pair of piques, we have 6 options. Take the permutations $\sigma = (3\ 11)(7\ 15)$ and $\tau = (7\ 15)(5\ 13)$. If the two piques in the pair have identical ρ or identical λ, they will yield permutations that can be simultaneously conjugated by σ or τ. Thus four pairings of the linear piques in the top four rows of the body of Table 2.6 have representations that are permutationally similar.

Now consider the two linear piques $(\mathbb{Z}/_{16}, \circ_1)$ with $x \circ_1 y = 5x + 3y$ and $(\mathbb{Z}/_{16}, \circ_2)$ with

$x \circ_2 y = 13x + 11y$. The right and left multiplications cannot be simultaneously conjugated by σ or τ. In the conjugation of 3 and 11, 5 and 13 are fixed points. In the conjugation of 5 and 13, 3 and 11 now become fixed points. If there exists $\pi \in S_{16}$ that simultaneously conjugates these pairs of permutations, π needs both to fix and to interchange 3 and 11, 5 and 13 in the respective permutations. This is impossible. Hence, the piques $(\mathbb{Z}/_{16}, \circ_1)$ and $(\mathbb{Z}/_{16}, \circ_2)$ are not permutationally similar. The pair of linear piques with multiplications given by $5x + 11y$ and $13x + 3y$ displays the same behavior. Summarizing, we have obtained the following negative result to contrast with the positive results obtained earlier, along with Proposition 2.3.11.

Theorem 2.4.2. *There are pairs of $\mathbb{Z}$-linear piques on $\mathbb{Z}/_{16}$ which have the same permutation character, but which are neither isomorphic nor permutationally similar.*

CHAPTER 3. PERI-CATALAN NUMBERS

3.1 An Introduction to Catalan Numbers and Their History

Catalan numbers appear in a variety of combinatorial questions. Though the sequence is named after the Belgian mathematician Eugène Charles Catalan (1814-1894), Leonhard Euler (1707-1783) was one of the first European mathematicians to discover and study the sequence. According to [10], the Catalan numbers were well-studied by a plethora of mathematicians, though the sequence remained unnamed for a large portion of time. Notable mathematicians studied Catalan numbers, including Christian Goldbach (1690-1764), Joseph Louiville (1809-1882), and Arthur Cayley (1821-1895). In older papers, this sequence was referred to as *Segner numbers* or *Euler-Segner numbers*. The modern name *Catalan numbers* arose from an American combinatorialist John Riordan (1903-1988) in his 1968 monograph *Combinatorial Identities* [10].

Regardless of its naming history, Catalan was the first mathematician to prove the familiar closed form formula for the n-th Catalan number. For a positive integer n, we have $C_n = \frac{1}{n}\binom{2n-2}{n-1}$. While many sources start the index at $n = 0$, we start the index at $n = 1$. In a paper motivated by the study of Fermat curves and modular curves, Long and Smith introduced a new class of loops, called *Catalan loops* [7]. A *loop* is a quasigroup equipped with an identity element 1. The Catalan loops were so named because the Catalan numbers appear as coefficients in a recursive solution in the proof that Catalan loops are two-sided loops. Here, the indexing naturally started at 1.

The following subsections will briefly introduce some applications of Catalan numbers. For the remainder of this chapter, the application with rooted binary trees will play the largest role in the study of peri-Catalan numbers.

3.1.1 Triangulating regular convex polygons

Euler characterized the n-th Catalan number as the number of ways to triangulate a convex regular $(n+1)$-gon [10]. If the indexing started at $n = 0$, then the triangulations would start with $(n+2)$-gons. Minimal shifts in the index and number of sides is an added benefit of starting the index at $n = 1$.

Given a regular convex polygon, a *triangulation* of the polygon divides the polygon into triangular segments by drawing non-intersecting lines between the vertices. The figure below illustrates the triangulations of a regular $(n+1)$-gon from $n = 1$ to $n = 4$.

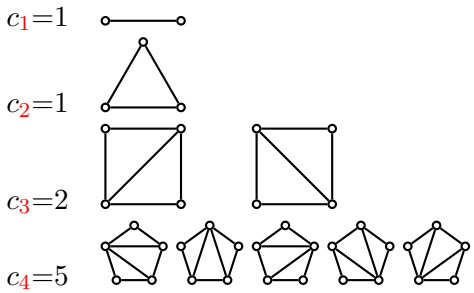


Figure 3.1 Triangulations of regular convex polygons up to $n = 4$.

Catalan studied the number of ways to write a non-associative product of n variables.

3.1.2 Lattice paths

Given an $n \times n$ lattice grid, a path along the grid lines from the bottom left corner to the top right corner is *monotone* if the path only consists of steps going right and up. Catalan numbers arise when counting the number of monotone lattice paths below the diagonal on an $n \times n$ lattice grid.

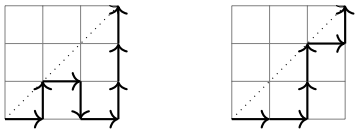
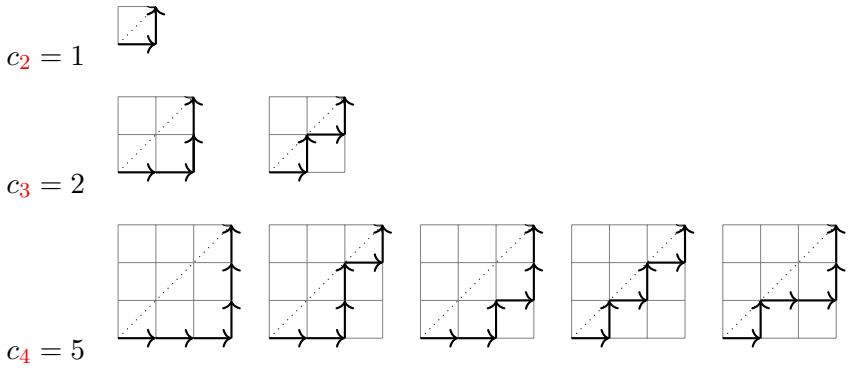


Figure 3.2 A non-monotone and monotone path on a 3×3 lattice grid.

The indexing used for the Catalan numbers will not match the size of the lattice grid,

though it does match the number of vertices along any side of the square. Here, the n-th Catalan number gives the number of $(n-1) \times (n-1)$ monotone lattice paths below the diagonal from the bottom left corner to the top right corner. We present paths for 1×1 up to 3×3 lattice grids.



3.1.3 Rooted binary trees

A *graph* is an ordered pair $G = (V, E)$, where V is a set of vertices and E is a set of edges connecting the vertices.

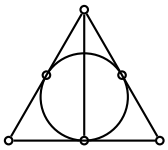


Figure 3.3 The Deathly Hallows.

While a general graph can take many forms, we are only concerned with rooted binary trees. A *rooted binary tree* has a designated root vertex. Every vertex has at most two edges coming out, away from the root vertex. Vertices with no edges coming out are called *leaves*. In the figure below, the root vertex is highlighted in red and the edges are labeled with arrowheads to indicate the direction they point toward. In general, we omit the directed edges.

A *full rooted binary tree* is a graph with a designated *root vertex*. Every other vertex has two or no edges coming away from the root vertex. The rooted binary tree given above is not a full rooted binary tree.

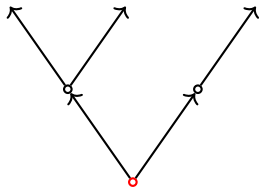


Figure 3.4 A rooted binary tree

The n-th Catalan number gives the number of full rooted binary trees with n leaves. Full rooted binary trees up to 4 leaves are given below.

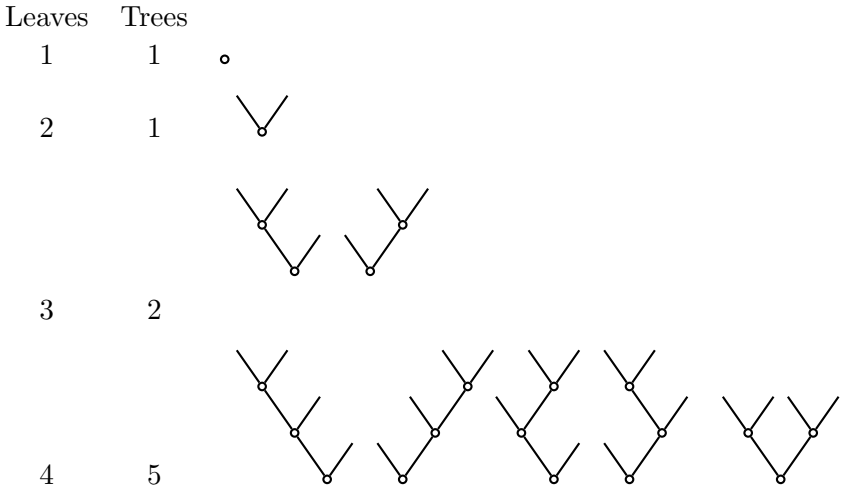


Figure 3.5 Full rooted binary trees, up to 4 leaves

Remark 3.1.1. Full rooted binary trees serve as a means to study quasigroup words. A full rooted binary tree must have at least one leaf, so the indexing used for the Catalan numbers starts at 1. The usual indexing starting at 0 gives the formula: $C_n = \frac{1}{n+1}\binom{2n}{n}$. For the remainder of this chapter, we only consider full rooted binary trees, so we will simply refer to them as trees.

3.1.4 Well-formed parentheses

Studying polygon triangulations was a hot topic through the years, and Catalan was no exception to this problem. French mathematician Gabriel Lamé (1795-1870) wrote to Liouville and provided an elegant solution to the polygon triangulations. Catalan was a former student

of Liouville at the École Polytechnique and became interested in this problem. After he proved the modern day standard formula, he went on to study the number of ways to write a non-associative product with n arguments. Essentially, this is equivalent to counting the number of ways to write well-formed sequences of parentheses. This is particularly fitting since the work in this dissertation is motivated by the study of nonassociative algebras. The n-th Catalan number gives the number of ways to properly write n pairs of parentheses.

0 pairs	$c_1 = 1$	
1 pair	$c_2 = 1$	()
2 pairs	$c_3 = 2$	(()), ()()
3 pairs	$c_4 = 5$	((())), (())(), ()(()), ()()(), (()())
4 pairs	$c_5 = 14$	(((()))),(((()))(), ...

Figure 3.6 Properly writings n pairs of parentheses

3.2 Magma Words and Rooted Binary Trees

The magma of interest is the free magma on the single generator $\{x\}$, denoted $F_M\{x\}$. We also refer to an element as a *magma word*. If a magma word has n arguments, we say it is a *length n word*. There are no relations imposed on this algebra. Elements look like:

$$x, x \cdot x, (x \cdot x) \cdot x, x \cdot (x \cdot x), (x \cdot x) \cdot (x \cdot x), (x \cdot (x \cdot x)) \cdot x, \ldots$$

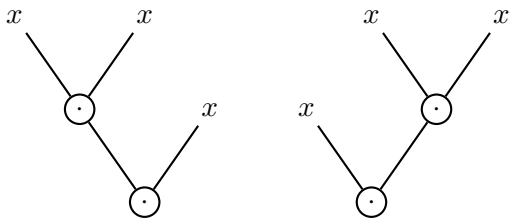
In Section 3.1.4, we saw for a natural number n, the n-th Catalan number gives the number of ways to properly write $n-1$ pairs of parentheses. Since we are concerned with nonassociative algebras, we can formulate the previous example as follows. For a natural number n, the n-th Catalan number gives the number of ways to bracket a nonassociative binary operation with n arguments.

In $(\mathbb{Z}, -)$, we write $2 - 3 := -1$. In the free magma, $(x \cdot x) \cdot x \neq x^3$. One can imagine how reading and writing long words in $F_M\{x\}$ becomes visually taxing due to the lack of relations on $F_M\{x\}$ and the nonasociative binary operation.

Fortunately, one can represent a magma word in a single generator $\{x\}$ with a full rooted binary tree. Each leaf is assigned x and remaining vertices are assigned a multiplication. The

root vertex represents the outermost pair of parentheses in a magma word. We refer to the assignments of pairs of parentheses as *bracketings*.

Example 3.2.1. The trees given below represent the words $(x \cdot x) \cdot x$ and $x \cdot (x \cdot x)$, respectively:



Since each argument in an element of the free magma is x, C_n gives us the number of magma words with n arguments. Each tree with n leaves represents a length n magma word in a single generator. So the number of rooted binary trees with n leaves is equal to the number of length n magma words. This relationship provides a launching point for quasigroup words and the peri-Catalan numbers.

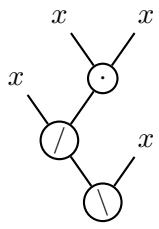
3.3 Quasigroup Words and Rooted Binary Trees

The quasigroup of interest is the free quasigroup on the single generator $\{x\}$, denoted $F_Q\{x\}$. Elements look like:

$$x, x \cdot x, x\backslash x, x/x, (x/x)/x, x/(x/x), x\backslash(x/x), \ldots$$

A *quasigroup word* is a concatenation of quasigroup elements by the three binary operations $\cdot, /$, and $\backslash$. Just as rooted binary trees represent magma words in a single generator, rooted binary trees also represent quasigroup words in a single generator. Each leaf is assigned x while remaining vertices are assigned one of the three operations $\cdot, /$, and $\backslash$.

Example 3.3.1. The quasigroup word $x/((x \cdot x)\backslash x)$ is represented by the tree



Note in the above example, the word $x/((x \cdot x)\backslash x)$ reduces to $x \cdot x$ via the (DL) identity. We say a quasigroup word is *reduced* if the word will not reduce via the quasigroup identities. A full rooted binary tree representing a quasigroup word in a single generator *reduces* if its corresponding quasigroup word reduces via quasigroup identities.

While the n-th Catalan number gives the number of rooted binary trees with n leaves, it also gives the number of ways to bracket a single nonassociative binary operation. To construct a length n quasigroup word in a single generator, there are three choices for $n-1$ many operations and C_n ways to bracket the word. This yields $3^{n-1}C_n$ many length n unreduced quasigroup words in a single generator.

In Example 3.3.1, the tree reduces down to a two-leaf tree. The number of length n reduced quasigroup words in a single argument is yet to be determined.

3.4 Peri-Catalan Numbers

Definition 3.4.1. The n-th *peri-Catalan number*, denoted P_n, gives the number of inequivalent length n quasigroup words in a single argument.

The prefix *peri−* comes from the Greek prefix $\pi\epsilon\rho\iota$, meaning "surrounding." The magmas $(Q, \cdot)$, $(Q, /)$, and $(Q, \backslash)$ live inside every quasigroup $(Q, \cdot, /, \backslash)$. One can think of a quasigroup structure surrounding a magma structure. For the case of a single generator x, there are C_n magma words of length n. This provides weak upper and lower bounds.

$$3C_n \leq P_n \leq 3^{n-1}C_n. \tag{3.1}$$

Since each quasigroup word in a single generator is represented by a rooted binary tree, computing the n-th peri-Catalan number can be done by computing the number of reduced rooted binary trees representing quasigroup words.

3.5 Mirror Symmetry

We present an inductive process in Section 3.6 to construct n-leaf rooted binary trees that represent inequivalent length n reduced quasigroup words. Rather than counting individual

trees, we rely on symmetry of rooted binary trees and the six quasigroup identities to reduce the necessary work. We first discuss mirror symmetry in this section to motivate the inductive process described in the Section 3.6.

Two rooted binary trees are *mirror-symmetric* if they are reflections of one another across a vertical axis passing through the root vertex. We bring back four rooted binary trees from Section 3.1.3. The vertical axes are highlighted in red and blue for pairs of mirror symmetric trees.

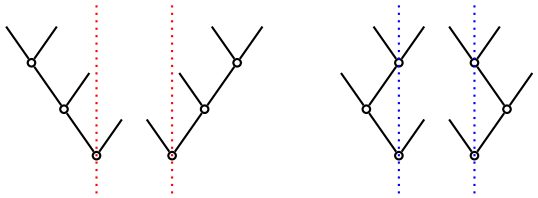
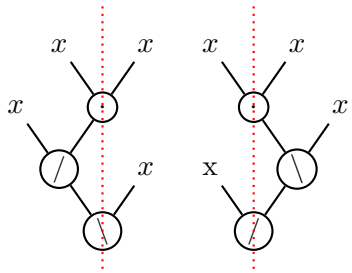


Figure 3.7 Mirror-symmetric rooted binary trees with four leaves

Quasigroup words also exhibit mirror symmetry. To develop intuition for mirror symmetry in quasigroup words, we exploit the mirror symmetry found in their rooted binary tree representations.

Definition 3.5.1. Two quasigroup words are *mirror-symmetric* if their corresponding rooted binary trees are mirror symmetric.

Example 3.5.2. The following trees represent the quasigroup words $(x/(x \cdot x))\backslash x$ and $x/((x \cdot x)\backslash x)$, respectively. Notice the reflection across the red vertical axis permutes the right and left divisions, while multiplication stays the same.



While the trees provide visual intuition for mirror symmetry, the concept is best described using the action of S_3 on the quasigroup operations [13§1.8]. We denote opposite operations

as follows:

$$x \circ y = x \cdot y,\ x//y = y/x,\ \text{and } x\backslash\backslash y = y\backslash x \tag{3.2}$$

Remark 3.5.3. The symbol $\circ$ used here is different than the usage in the previous chapter.

We denote a product such as $x \cdot y$ as $xy\mu$. A larger product such as $(x \cdot x) \cdot x$ is written as $xx\mu x\mu$. Given a quasigroup word written in this postfix notation, one unravels each multiplication μ by multiplying the two arguments or completed products immediately to its left. A longer word such as $xx\mu xx\mu x\mu\mu$ unravels as

$$\begin{aligned} xx\mu xx\mu x\mu\mu &= (xx\mu) \cdot (xx\mu x\mu) \\ &= (x \cdot x) \cdot ((xx\mu) \cdot x) \\ &= (x \cdot x) \cdot ((x \cdot x) \cdot x). \end{aligned}$$

Right division, left division, and opposite quasigroup operations can be represented by postfix notation. We consider the action of S_3 on the quasigroup operations. Let σ and τ represent (12) and (23), respectively [14]. We write

$x \cdot y = xy\mu$	$x\backslash y = xy\mu^{\tau}$	$x//y = xy\mu^{\tau\sigma}$
$x \circ y = xy\mu^{\sigma}$	$x\backslash\backslash y = xy\mu^{\sigma\tau}$	$x/y = xy\mu^{\sigma\tau\sigma}$

Figure 3.8 Triality symmetry of the quasigroup operations.

Let $g \in S_3$. Given an operation μ^g, its opposite operation is given by $\mu^{\sigma g}$ while its mirror symmetric operation is given by $\mu^{g\sigma}$.

Definition 3.5.4. Two quasigroup words u, v are *mirror symmetric* if their postfix notation can be written in terms of each other via multiplication by σ on the right.

The notation convention we will use is $u = v^{\sigma}$.

Example 3.5.5. Consider the words $(x\backslash y)/x$ and $x\backslash(y/x)$. When one writes out the trees for these two words, it is clear to see that they are mirror-symmetric quasigroup words. However, note that $(x\backslash y)/x = xy\mu^{\tau}x\mu^{\sigma\tau\sigma}$ while $x\backslash(y/x) = xy\mu^{\tau\sigma}x\mu^{\sigma\tau}$. The current postfix notation for $x\backslash(y/x)$ is inconsistent with Definition 3.5.4. There is not necessarily a unique way to express

a quasigroup word in postfix notation. The word $x\backslash(y/x)$ can be written in terms of opposite operations. Consider $x\backslash(y/x) = (y/x)x\mu^{\sigma\tau} = xy\mu^{\tau\sigma}x\mu^{\sigma\tau}$. Now we see that the postfix notation for $(x\backslash y)/x$ and $x\backslash(y/x)$ differ by multiplication by σ on the right for each of its operations.

Notice the six quasigroup identities exhibit a mirror symmetry:

$$\begin{array}{llll} \text{(SL)} & x \cdot (x\backslash y) = y\,, & \text{(SR)} & y = (y/x) \cdot x\,, \\ \text{(IL)} & x\backslash(x \cdot y) = y\,, & \text{(IR)} & y = (y \cdot x)/x\,, \\ \text{(DL)} & x/(y\backslash x) = y\,, & \text{(DR)} & y = (x/y)\backslash x\,, \end{array} \tag{3.3}$$

The postfix notation for the (SL) identity is $xxy\mu^{\tau}\mu = y$ while the postfix notation for the (SR) identity is $xxy\mu^{\tau\sigma}\mu^{\sigma}$. It is left as an exercise to the reader to write the remaining identities in postfix notation exhibiting mirror symmetry. We say (SR), (IR), and (DR) are the mirror-symmetric quasigroup identities for (SL), (IL), and (DL), respectively. This brings us to the following lemma.

Lemma 3.5.6 (Symmetry of Rooted Binary Trees)**.** *Let w be a quasigroup word in a single generator $\{x\}$. If w is reduced, then w^{σ} is reduced. If w is not reduced, then w^{σ} is not reduced.*

The result is evident from the mirror symmetry of the quasigroup identities.

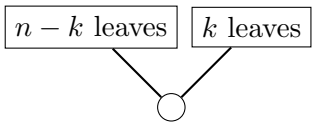
Corollary 3.5.7. *If w is an unreduced quasigroup word in a single generator, w^{σ} will reduce via the mirror-symmetric identities that reduce w.*

In Example 3.5.2, notice $(x/(x \cdot x))\backslash x$ reduces via the (DR) identity while $x/((x \cdot x)\backslash x)$ reduces via the (DL) identity. Consequently, this minimizes the number of trees we need to count.

3.6 The Inductive Process

We can consider trees with more leaves to the left of the root vertex. We refer to such trees as *left-heavy* trees. To construct trees with more leaves to the right of the root vertex, we reflect the left-heavy trees across the vertical axis passing through the root vertex. This allows us to capture mirror-symmetric words in a single generator via a reflection of trees.

For a natural number $n > 2$, let $1 \leq k \leq \lfloor \frac{n-1}{2} \rfloor$. To construct an n-leaf tree that represents a quasigroup word in a single generator, we adjoin a k-leaf reduced tree to an $(n-k)$-leaf reduced tree.



We have a choice of three operations to put in the root vertex. For each $1 \leq k \leq \lfloor \frac{n-1}{2} \rfloor$, we have $3P_{n-k}P_k$ many n-leaf trees. Since we adjoined reduced trees, we need only concern ourselves with cancellations that occur with the root vertex operation. Moreover, if n is even, we add the term $3P_{\frac{n}{2}}P_{\frac{n}{2}}$. We discuss this in more detail in Section 3.7.

The following provides an upper bound on the n-th peri-Catalan number.

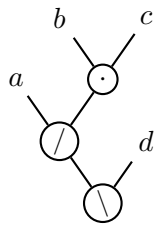
$$P_n \leq \delta_{\lceil \frac{n}{2} \rceil, \lfloor \frac{n}{2} \rfloor} + 6 \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} P_{n-k}P_k + 3P_{\frac{n}{2}}P_{\frac{n}{2}} \tag{3.4}$$

The next section will describe the type of word reductions incurred in the inductive process. From there, we will subtract the number of cancellations from the upper bound given above to replace the inequality with an equation.

3.7 Root Vertex Cancellations

We will use a lexicographical description to describe the branches and vertices of a rooted binary tree. Starting from the root vertex, we describe the left branch as L and the right branch as R. From the first vertex of the L branch, we use the same description.

Example 3.7.1. In the tree below, a is the LL leaf, b is the LRL leaf, c is the LRR leaf, and d is the R leaf. We will refer to $b \cdot c$ as the LR word and $a/(b \cdot c)$ as the L word.



We say a tree is *balanced* if the left and right branches have the same number of leaves. We say a tree is *unbalanced* if the number of leaves on the left and right branches differ.

3.7.1 Cancellations in unbalanced trees

Let $n > 2$ and $1 \leq k \leq \lfloor \frac{n-1}{2} \rfloor$. Let u, v, and w be reduced quasigroup words in a single generator such that sum of the lengths of u and v is $n-k$ and the length of w is k. Let the L word be a concatenation of u and v, and w be the R word. The following lemmas consider the possible concatenations of u and v.

Proposition 3.7.2. *Let $u \cdot v$ be a length $n-k$ reduced quasigroup word in a single generator. Then*

1. *$(u \cdot v) \cdot w$ will not reduce,*
2. *$(u \cdot v)/w$ reduces if and only if $v = w$, and*
3. *$(u \cdot v)\backslash w$ will not reduce.*

Proof. For 1), we start off with $u \cdot v$ as a reduced word, so we need only consider cancellations that may occur from multiplying $u \cdot v$ on the right by w. Since the outermost binary operation for the words u, v, w is multiplication, we consider the (SR) identity. If v could be written as $v = v'/w$ for some non-empty reduced quasigroup word v', the bracketing of $(u \cdot v) \cdot w) = (u \cdot (v'/w)) \cdot w$ will not satisfy the format of the (SR) identity. Since w is a reduced word whose length is less than the length of $u \cdot v$, we cannot express w as a reduced word that contains $u \cdot v$ as a factor (i.e. $w \neq (u \cdot v)\backslash w'$ for some non-empty word w' such that the length of $(u \cdot v)\backslash w'$ is less than the length of $u \cdot v$.) Thus, the (SL), (IL), (DL) identities will not apply either. Indeed, $(u \cdot v) \cdot w$ is a reduced word.

For 2), the (IR) identity is an immediate candidate for the collapsing of $(u \cdot v)/w$. It is clear that $(u \cdot v)/w$ reduces if $v = w$. If v could be expressed a reduced word in terms of $v' \cdot w$ for some non-empty word v', the bracketing on $(u \cdot (v' \cdot w))/w$ would not follow the format of the (IR) identity. In a similar vein, we see we cannot write u in a nontrivial way so as to get another (IR) reduction.

The outermost binary operation for $(u \cdot v)/w$ is right division, so the (SL), (SR), and (IL) identities are excluded cancellation candidates. The (DL) identity applies if w can be expressed as a reduced word $w'\backslash(u \cdot v)$, where w' is a non-empty reduced quasigroup word. However, the

length of w is less than the length of $u \cdot v$. We cannot write $u \cdot v$ in a way that satisfies the bracketing of the (DL) identity.

For 3), the outermost binary operation of $(u \cdot v)\backslash w$ is left division, so the word will not satisfy the (SR), (IR), and (DL) identities. Since the length of w is less than the length of $u \cdot v$, we cannot rewrite w as a reduced word in terms of $u \cdot v$. The (SL) and (IL) identities are eliminated as cancellation candidates in addition to the (SR) and (IR) identities. If u could be rewritten as reduced word in terms of w, i.e. $u = w/u'$, for some non-empty word u', the bracketing on $((w/u') \cdot v)\backslash w$ fails to satisfy the (DR) identity. Thus, $(u \cdot v)\backslash w$ is a reduced word. □

Proposition 3.7.3. *Let u/v be a length $n-k$ reduced quasigroup word in a single generator. Then*

1. *$(u/v) \cdot w$ reduces if and only if $v = w$,*
2. *$(u/v)/w$ will not reduce, and*
3. *$(u/v)\backslash w$ will reduce if and only if $u = w$.*

Proof. For 1), the word $(u/v) \cdot w$ satisfies the (SR) identity. It is clear that the word will reduce if $v = w$. If $v \neq w$, then it is clear the word will not reduce. The outermost binary operation is multiplication, so the word does not satisfy the (IR) and (DR) equation formats. Since the length of w is less than the length of u/v, the (SL) identity is eliminated as a cancellation candidate. The bracketing and operations of the (IL) and (DL) equations are also not satisfied by $(u/v) \cdot w$).

For 2), the outermost binary operation on the word $(u/v)/w$ is right division, so the (SL) and (IL) equations are immediately eliminated since they do not use right division. Since the length of w is less than the length of u/v, we cannot write $w = w'\backslash(u/v)$ for some non-empty word w'. This eliminates the (DR) identity.

If we could write $v = v' \cdot w$ for non-empty word v', the bracketing on $(u/(v' \cdot w))/w$ does not follow the (IR) equation. Since the length of w is less than the length of u/v, we cannot rewrite

w as a reduced word in terms of u/v, so the (DL) equation is eliminated as a cancellation candidate. Lastly, we cannot rewrite u/v in terms of w so that the (SR) equation applies.

For 3), it is clear that $(u/v)\backslash w$ reduces if $u = w$. If $u \neq w$, then $(u/v)\backslash w$ will not reduce. The bracketing on $(u/v)\backslash w$ does not match the bracketing in the (DL) identity. The (SR) and (IR) equations do not have left division, so those are eliminated as cancellation candidates as well. While the (SL) and (IL) identities have left divisions, we cannot derive the same necessary bracketings in those identities in the word $(u/v)\backslash w$. □

Proposition 3.7.4. *Let $u\backslash v$ be a length $n-k$ reduced quasigroup word. Then any concatenation of $u\backslash v$ with w will be a reduced word.*

Proof. First consider $(u\backslash v)\cdot w$. The outermost binary operation of multiplication and bracketing in $(u\backslash v)\cdot w$ prevent the word from being written in a format that satisfies the (IL), (DL), (IR), and (DR) equations. Since the length of w is less than the length of $u\backslash v$, we cannot rewrite w as a reduced word in terms of $u\backslash v$, i.e. $w \neq (u\backslash v)\backslash w'$ for some reduced word w'. This eliminates the (SL) equation. If v could be written as reduced word in terms of w, i.e. $v = v'/w$, the bracketing in $(u\backslash(v'/w))\cdot w$ doesn't follow the bracketing in the (SR) equation. Thus, $(u\backslash v)\cdot w$ is a reduced word.

Next consider $(u\backslash v)/w$. The (SL) and (IL) equations do not contain a right division, so they are eliminated as cancellation candidates. The length of w is less than the length of $u\backslash v$, so we cannot express w as a reduced word in terms of $w = w'\backslash(u\backslash v)$ for some non-empty word w'. This eliminates the (DL) and (DR) equations. The length of w is less than the length of $u\backslash v$, so we cannot express w as a reduced word in terms of $w = (u\backslash v)\cdot w'$ for some non-empty word w'. If v could be written as reduced word in terms of w, i.e. $v = v'\cdot w$, the bracketing in $(u\backslash(v'\cdot w))/w$ doesn't follow the bracketing in the (SR) equation.

Lastly, consider the word $(u\backslash v)\backslash w$. Since this word lacks multiplication, cancellation via the (SL) and (SR) identities are eliminated. The (IR) equation does not contain a left division so it is eliminated as a cancelation candidate. Since the length of w is less than the length of $u\backslash v$, we cannot write $w = (u\backslash v)\cdot w'$ for some non-empty word w'. This eliminates the (IL) equation. The (DL) equation is eliminated similarly: we cannot write w as a reduced word in

terms of $u\backslash v$, i.e. $w'\backslash(u\backslash v)$. If we could write u as a reduced word in terms of w, i.e. $u = w/u'$ for some non-empty word u', the bracketing on $((w/u')\backslash v)\backslash w$ prohibits cancellation via the (DR) equation.

□

3.7.2 Cancellations in balanced Trees

For the following case, let n be an even number. We consider a length n reduced quasigroup word written in terms of three reduced quasigroup words u, v, and w. We consider three cases for balanced trees. As each case is argued similarly, we present a proof for one of the three cases.

Lemma 3.7.5. *Let n be a positive even number. Let $u \cdot v$ and w be reduced quasigroup words in a single generator such that the lengths of $u \cdot v$ and w are $\frac{n}{2}$. Any concatenation of $u \cdot v$ and w will be a reduced word.*

Proof. Consider $(u \cdot v) \cdot w$. Since $u \cdot v$ is a reduced word, potential cancellations must involve w. However, note that the length of w is greater than the length of u and v. It is not possible for $u = w$ or $v = w$. Since the length of w is equal to the length of $u \cdot v$, we cannot write w as a reduced word in terms of $u \cdot v$, i.e. $w = (u \cdot v)\backslash w'$ for some non-empty word w'. Thus none of the six quasigroup equations are applicable. □

Lemma 3.7.6. *Let n be a positive even number. Let u/v and w be reduced quasigroup words in a single generator such that the lengths of u/v and w are $\frac{n}{2}$. Any concatenation of u/v and w will be a reduced word.*

Lemma 3.7.7. *Let n be a positive even number. Let $u\backslash v$ and w be reduced quasigroup words in a single generator such that the lengths of $u\backslash v$ and w are $\frac{n}{2}$. Any concatenation of $u\backslash v$ and w will be a reduced word.*

3.8 Refining the Recursive Formula

Based on Propositions 3.7.2, 3.7.3, and 3.7.4, we encounter three types of cancellation in the inductive process described in Section 3.6. We continue to use the convention that u, v, and

w are reduced quasigroup words. Lemmas 3.7.5, 3.7.6, and 3.7.7 demonstrate that balanced trees generated by the inductive process are reduced trees. We may assume the sum of the lengths of u and v is $n-k$ while the length of w is k. We introduce the following notation that describes the types of cancellations that occur in the inductive process.

3.8.1 Counting the cancellations

Given reduced words u, v such that $u \cdot v$ is a reduced length $n-k$ word, Proposition 3.7.2 says a concatenation with a length k reduced word w will only reduce via the (IR) quasigroup identity. This type of cancellation requires the length of v to be equal to the length of w and multiplication in the root vertex of the L word. As a consequence, we only want to count the number of rooted binary trees representing $n-k$ quasigroup words that have $n-2k$ leaves on the L branch and k leaves on the R branch.

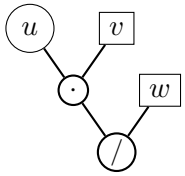


Figure 3.9 A tree exhibiting the necessary format for the (IR) cancellation.

Definition 3.8.1. Let a and b be positive integers. The function $m(a,b)$ counts the number of $(a+b)$-leaf trees representing reduced quasigroup words with a leaves on the left branch, b leaves on the right branch, and a multiplication in the root vertex.

Definition 3.8.2. Let a and b be positive integers. The function $r(a,b)$ counts the number of $(a+b)$-leaf trees representing reduced quasigroup words with a leaves on the left branch, b leaves on the right branch, and a right division in the root vertex.

Definition 3.8.3. Let a and b be positive integers. The function $l(a,b)$ counts the number of $(a+b)$-leaf trees representing reduced quasigroup words with a leaves on the left branch, b leaves on the right branch, and a left division in the root vertex.

We refer to the m, r, and l functions as *auxiliary bivariates*. Since auxiliary functions output the numbers of trees exhibiting a certain property, we note that the auxiliary functions

are nonnegative functions. If one of the arguments is nonpositive, the output of the auxiliary bivariate is zero.

Proposition 3.8.4. *Let $n \geq 3$ and $1 \leq k \leq \lfloor \frac{n-1}{2} \rfloor$. The number of (IR) tree reductions incurred at the root vertex during the inductive process is given by $m(n-2k, k)$.*

Proof. If a concatenation of reduced words u, v, and w reduces via the (IR) identity, Proposition 3.7.2 says the operations must be $(u \cdot v)/w$ with $v = w$. Given an $(n-k)$ leaf tree representing $u \cdot v$, we append all possible k-leaf trees to the right of the new root vertex via right division. Each k-leaf tree, w, appears at most once in the tree representing $u \cdot v$ as the LR word. Since we need $v = w$ in order to incur a cancellation, we need only count how many $(n-k)$-leaf trees have k leaves on the right branch and multiplication in the root vertex. This number is given by $m(n-2k, k)$. □

Given reduced words u and v such that $u\backslash v$ is a reduced word of length $n-k$, Proposition 3.7.4 says any concatenation with a length k word w on the right will not reduce. If u/v is a reduced word of length $n-k$, Proposition 3.7.3 says two types of cancellations may occur. Namely, (SR) and (DR) cancellations. The figure given below highlights the formats necessary for both (SR) and (DR) cancellation. The boxed words indicate which branches need to have the same word.

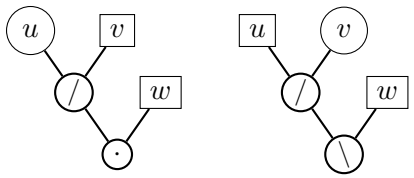


Figure 3.10 Trees exhibiting the necessary format for the (SR) and (DR) cancellations.

Proposition 3.8.5. *Let $n \geq 3$ and $1 \leq k \leq \lfloor \frac{n-1}{2} \rfloor$. The number of (SR) tree reductions incurred at the root vertex during the inductive process is given by $r(n-2k, k)$.*

Proof. If a concatenation of reduced words u, v, and w reduces via the (SR) identity, Proposition 3.7.3 says the operations must be $(u/v) \cdot w$ with $v = w$. Given an $(n-k)$-leaf tree, we append all possible k-leaf trees to the right of the new root vertex. Each k-leaf tree, w, we append

appears at most once in the tree representing u/v as the LR word. Since we need $v = w$ to incur a cancellation, we need only count how many $(n-k)$-leaf trees have k leaves on the right branch and a right division in the root vertex. This number is given by $r(n-2k, k)$. □

Proposition 3.8.6. *Let $n \geq 3$ and $1 \leq k \leq \lfloor \frac{n-1}{2} \rfloor$. The number of (DR) tree reductions incurred at the root vertex during the inductive process is given by $r(k, n-2k)$.*

Proof. If a concatenation of reduced words u, v, and w reduces via the (DR) identity, Proposition 3.7.3 says the operations must be $(u/v)\backslash w$ with $u = w$. Given an $(n-k)$-leaf tree, we append all possible k-leaf trees to the right of the new root vertex. Each k-leaf tree, w, we append appears at most once in the tree representing u/v as the LL word. Since we need $u = w$ to incur a cancellation, we need only count how many $(n-k)$-leaf trees have k leaves on the left branch and a right division in the root vertex. This number is given by $r(k, n-2k)$. □

Corollary 3.8.7. *Let $n \geq 3$ and $1 \leq k \leq \lfloor \frac{n-1}{2} \rfloor$. If the inequality $n > 3k$ holds, then $m(n-2k, k)$ is specified by:*

$$m(n-2k, k) = P_{n-2k}P_k - r(n-3k, k) \tag{3.5}$$

Proof. Equation 3.5 hearkens to Proposition 3.8.4. We once again consider a reduced word $u \cdot v$ of length $n-k$, where u and v are both reduced words. Now append a word w of length k to the right $u \cdot v$ using right division. We know from Proposition 3.8.4, a reduction via the (IR) identity at the root vertex will occur if and only if $v = w$. This is implies we need only count words $u \cdot v$ of length $n-k$ that can be written as $u \cdot w$, for a reduced word w of length k. Note that in this case, the length of w is k and the length of u is $n-2k$. Since we supposed $n > 3k$, we still have that $u \cdot w$ is a left-heavy tree. This is very important to note, since we need left-heavy trees in order to use Propositions 3.7.2 and 3.7.3.

With a multiplication in the root vertex, the word $u \cdot w$ may reduce via the (SR) identity. We know that u and w are both reduced words, so that an (SR) reduction at the root vertex is the only possibility for a reduction. So we need to consider how many words $u \cdot w$ can be rewritten as $(u'/w) \cdot w$, where $u = u'/w$ for a non-empty reduced word u'. Now we apply

Proposition 3.8.5 to count how many $(n-2k)$-leaf trees have right division in the root vertex and k leaves on the right branch. This number is given by $r(n-3k,k)$.

The total number of possible trees of length $n-k$ with multiplication in the root vertex is given by $P_{n-2k}P_k$. Only $r(n-3k,k)$ of these trees reduce, we have

$$m(n-2k,k) = P_{n-2k}P_k - r(n-3k,k),$$

as desired.

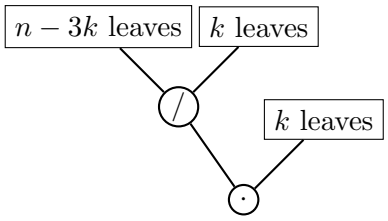


Figure 3.11 A tree exhibiting the necessary format for the (SR) cancellation on the left branch.

□

Corollary 3.8.8. *Let $n \geq 3$ and $1 \leq k \leq \lfloor \frac{n-1}{2} \rfloor$. If the inequality $n > 3k$ holds, then $r(n-2k,k)$ is specified by:*

$$r(n-2k,k) = P_{n-2k}P_k - m(n-3k,k) \tag{3.6}$$

Proof. Equation 3.6 uses the word format from Proposition 3.8.5. We consider a reduced word u/v of length $n-k$, where u and v are both reduced words. If we append a word w of length k to the right of u/v via multiplication, Proposition 3.8.5 says an (SR) reduction at the root vertex will occur if and only if $v = w$. This implies we need only count words u/v of length $n-k$ that can be written as u/w, for a reduced word w of length k. Since we supposed $n > 3k$, we know u/w is a left-heavy tree.

With a right division in the root vertex, the word u/w may reduce via the (IR) identity. We know that u and w are both reduced words, so an (IR) reduction at the root vertex is the only possibility for a reduction. We need to consider how many words u/w can be written as $(u' \cdot w)/w$, where $u = u'/w$ for a non-empty reduced word u'. Now we apply Proposition 3.8.4

to count how many $(n-2k)$-leaf trees have multiplication in the root vertex and k leaves on the right branch. This number is given by $r(n-3k,k)$.

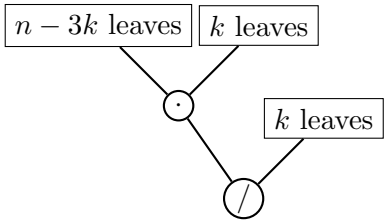


Figure 3.12 A tree exhibiting the necessary format for the (IR) cancellation on the left branch.

The right quotient of an $(n-2k)$-leaf tree and k-leaf tree will yield $P_{n-2k}P_k$ many trees. Of these, $m(n-3k,k)$ many trees will reduce via the (IR) identity. Thus,

$$r(n-2k,k) = P_{n-2k}P_k - m(n-3k,k),$$

as desired. □

Corollary 3.8.9. *Let $n \geq 3$ and $1 \leq k \leq \lfloor \frac{n-1}{2} \rfloor$. If the inequality $n > 3k$ holds, then $r(k, n-2k)$ is specified by:*

$$r(k,n-2k) = P_{n-2k}P_k - l(n-3k,k) \tag{3.7}$$

Proof. To prove Equation 3.7, we consider the word format given in Proposition 3.8.6. We consider a reduced word u/v of length $n-k$, where u and v are both reduced words. If we append a word w of length k to the right of u/v via left division, Proposition 3.7.3 says a (DR) reduction will only occur at the root vertex if and only if $u = w$. This implies we need only only count words u/v of length $n-k$ that can be written as w/v. Since we supposed $n > 3k$, we know w/v is a right-heavy tree.

With a right division in the root vertex, the word w/v may reduce via the (DL) identity. We know that w and v are both reduced words, so an (DL) reduction at the root vertex is the only possibility for a reduction. We need to consider how many words w/v can be written as $w/(v'\backslash w)$, where $v = v'\backslash w$ for a non-empty reduced word v'. Note that the number of $(n-2k)$-leaf trees with k leaves on the right branch and a left division in the root vertex is given by $l(n-3k,k)$.

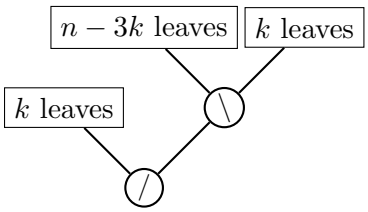


Figure 3.13 A tree exhibiting the necessary format for the (DR) cancellation on the left branch.

The left quotient of an $(n-2k)$-leaf tree and k-leaf tree will yield $P_{n-2k}P_k$ trees. Of these, $l(n-3k,k)$ many trees will follow the specified format above. Thus, $l(n-3k,k)$ many $(n-2k)$-leaf trees will reduce via the (DR) identity and

$$r(k,n-2k) = P_{n-2k}P_k - l(n-3k,k),$$

as desired. □

Given a natural number n, Corollaries 3.8.7, 3.8.8, and 3.8.9 allow for computations of $m(n-2k,k)$, $r(n-2k,k)$, and $r(k,n-2k)$ at previous steps in the inductive process.

The propositions in Section 3.7 consider left-heavy trees, and consequently only discuss cancellations that occur from the (IR), (SR), and (DR) identities. The $l(n-3k,k)$ auxiliary bivariate function makes its first appearance in Equation 3.7. In order to write $l(n-3k,k)$ in terms of smaller peri-Catalan numbers and auxiliary bivariates with smaller inputs, we exploit the mirror symmetry in the trees representing reduced quasigroup words and the mirror symmetry in the quasigroup identities.

We can use the mirror symmetry in the quasigroup identities to obtain the mirror symmetric versions of Propositions 3.7.2, 3.7.3, and 3.7.4. From there, we obtain the mirror symmetric versions of of Propositions 3.8.4, 3.8.5, and 3.8.6 and Corollaries 3.8.7, 3.8.8, and 3.8.9 to obtain:

$$l(n-3k,k) = P_{n-3k}P_k - r(k,n-4k) \tag{3.8}$$

Additionally, having mirror symmetry in the trees yields $l(n-3k,k) = r(k,n-3k)$.

The n-th peri-Catalan number is specified by a quadruple of data consisting of P_k for $k < n$ and the outputs of all three auxiliary bivariates. These propositions culminate in the following theorem which gives the n-th peri-Catalan number.

Proposition 3.8.10. *For $n \geq 2$, the n-th peri-Catalan number is given by*

$$P_n = \delta_{\lfloor \frac{n}{2} \rfloor, \lceil \frac{n}{2} \rceil} 3P_{\frac{n}{2}}P_{\frac{n}{2}} + 2\sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} (3P_{n-k}P_k - m(n-2k,k) - r(n-2k,k) - r(k,n-2k)). \quad (3.9)$$

Proposition 3.8.11. *For positive integers n and k, $m(n,k) = r(n,k) = l(n,k)$.*

Proof. We begin induction in the argument n. Let $k = 1$. We have $m(1,1) = r(1,1) = l(1,1)$. For the inductive step, suppose for a natural number $n > 1$, $m(n,1) = r(n,1) = l(n,1)$. Notice that $m(n+1,1) = P_{n+1}P_1 - r(n,1)$, $r(n+1,1) = P_{n+1}P_1 - m(n,1)$, and $l(n+1,1) = r(1,n+1) = P_{n+1}P_1 - l(n,1)$. From our inductive step, we have that $m(n+1,1) = r(n+1,1) = l(n+1) = P_{n+1}P_1 - m(n,1)$. Thus we have for any natural number n,

$$m(n,1) = r(n,1) = l(n,1). \quad (3.10)$$

To induct in the argument k, Equation 3.10 gives us our base case. We fix a natural number n. We will now take $k > 1$. Suppose that $m(n,k) = r(n,k) = l(n,k)$. If $n = k+1$, then we have that $m(n,k+1) = r(n,k+1) = l(n,k+1) = P_nP_n$ as a consequence of Propositions 3.7.5, 3.7.6, and 3.7.7. Any concatenation of equal length reduced words will be a reduced word. So we have our inductive step.

If $n \neq k+1$, we will consider the case when $n > k+1$. The case when $n < k+1$ will be argued similarly since the mirror symmetry of reduced words and their trees imply $m(n,k+1) = m(k+1,n)$, $r(n,k+1) = l(k+1,n)$ and $l(n,k+1) = r(k+1,n)$.

For $n > k+1$, we have the following from Equations 3.5, 3.6, and 3.7

$$m(n,k+1) = P_nP_{k+1} - r(n-(k+1),k+1), \quad (3.11)$$

$$r(n,k+1) = P_nP_{k+1} - m(n-(k+1),k+1), \text{ and} \quad (3.12)$$

$$l(n,k+1) = r(k+1,n) = P_nP_{k+1} - l(n-(k+1),k+1). \quad (3.13)$$

Case 1: If $k+1 > n-(k+1)$, then $n-(k+1) < k$. The induction hypothesis, along with mirror symmetry of the arguments in the auxiliary bivariates, implies $l(k+1,n-(k+1)) =$

$m(k+1, n-(k+1)) = r(k+1, n-(k+1))$. This shows that Equations 3.11, 3.12, and 3.13 coincide.

Case 2: If $k+1 = n-(k+1)$, then Propositions 3.7.5, 3.7.6, and 3.7.7 imply

$$m(n-(k+1), k+1) = r(n-(k+1), k+1) = l(n-(k+1), k+1) = P_{k+1}P_{k+1}.$$

Once again, we have that Equations 3.11, 3.12, and 3.13 coincide.

Case 3: If $k+1 < n-(k+1)$, then we reduce the first argument again via Propositions 3.5, 3.6, and 3.7 once more. We will have

$$m(n, k+1) = P_nP_{k+1} - P_{n-(k+1)}P_{k+1} + m(n-2(k+1), k+1) \tag{3.14}$$

$$r(n, k+1) = P_nP_{k+1} - P_{n-(k+1)}P_{k+1} + r(n-2(k+1), k+1) \tag{3.15}$$

$$l(n, k+1) = P_nP_{k+1} - P_{n-(k+1)}P_{k+1} + l(n-2(k+1), k+1) \tag{3.16}$$

We now focus on the arguments $n-2(k+1)$ and $k+1$. If Case 1 or Case 2 apply to these arguments, then the induction step is done. If not, we reduce the first argument in $m(n-2(k+1), k+1), r(n-2(k+1), k+1)$, and $l(n-2(k+1), k+1)$ again. This process will terminate in finitely many steps. Though if n is large and k is small, we will need to repeat this process more. Now we have for natural numbers n and k, $m(n,k) = r(n,k) = l(n,k)$, as desired. □

Remark 3.8.12. Proposition 3.8.11 can be proven using the language and tools of *hyperquasigroups*, à la parastrophes and quasigroup conjugates. We include the longer inductive proof as it requires less technical expertise from the reader.

Corollary 3.8.13. *For positive integers n and k, we have*

$$m(n,k) = m(k,n) \tag{3.17}$$

$$r(n,k) = r(k,n) \tag{3.18}$$

$$l(n,k) = l(k,n) \tag{3.19}$$

Proof. Notice, Equation 3.17 follows directly from mirror symmetry of a tree with multiplication in the root vertex. From mirror symmetry, we know $r(n,k) = l(k,n)$. Proposition 3.8.11 says $l(k,n) = r(k,n)$ which gives Equation 3.18. Equation 3.19 is similarly justified. □

The amalgamation of Corollaries 3.8.7, 3.8.8, 3.8.7, Theorem 3.8.10, and Proposition 3.8.11 is the following Main Theorem.

Theorem 3.8.14. *For $n \geq 2$, the n-th peri-Catalan number is given by*

$$P_n = \delta_{\lfloor \frac{n}{2} \rfloor, \lceil \frac{n}{2} \rceil} 3P_{\frac{n}{2}} P_{\frac{n}{2}} + 6 \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} (P_{n-k}P_k - m(n-2k,k)), \tag{3.20}$$

with $m(n-2k,k) = P_{n-2k}P_k + m(n-3k,k)$.

Corollary 3.8.15. *Each peri-Catalan number P_n is divisible by 3.*

The n-th peri-Catalan number P_n is specified by P_k for $k < n$ and the outputs of the auxiliary bivariates. While Corollary 3.8.7 and Proposition 3.8.11 allow us to compute $m(n-2k,k)$ in terms of smaller peri-Catalan numbers and auxiliary bivariates with smaller inputs, we refrain from writing Equation 3.20 solely in terms of P_k. Rewriting each $m(n-2k,k)$ in terms of peri-Catalan numbers is dependent on the arguments. As such, procuring a general form will reap little benefit. In practice, knowing the precise arguments of the auxiliary bivariates allows for quick and straightforward computations.

Table 3.1 The first ten peri-Catalan numbers

n	P_n
1	1
2	3
3	12
4	87
5	666
6	5,478
7	47,322
8	422,145
9	3,859,026
10	35,967,054

CHAPTER 4. DERIVATION AND THE FREE QUASIGROUP

4.1 Introduction

Let x be an element in an arbitrary semigroup $(S, \cdot)$. The free semigroup on one generator is the semigroup of positive integers under addition. Elements in $\mathbb{Z}^+$ index arbitrary powers of x, i.e.

$$x,\ x^2,\ x^3,\ x^4, \ldots$$

The nonassociative analogue of a semigroup is a magma. As is turns out, there is a nonassociative analogue of the free semigroup on one generator that indexes arbitrary nonassociative powers.

In 1957, Minc proved that rooted binary trees are represented faithfully by *index π-polynomials*. In [8], he referred to rooted binary trees as *bifurcating root trees*. The index π-polynomials he used are written in two noncommuting variables λ and μ rather than R and L as we will use in later sections. However, in this chapter, discussions of representing the free quasigroup on a single generator follow in the spirit of quasigroup derivatives from [13].

The free group on one generator is the group of integers under addition. Elements of $\mathbb{Z}$ index arbitrary powers of an element x in a group. However, the nonassociative analogue of the integers does not faithfully index arbitrary quasigroup words in a single generator. We begin with preliminary components from universal algebra and then proceed to the nonassociative analogues of $\mathbb{Z}^+$ and $\mathbb{Z}$. Section 4.3 will introduce nonassociative integers and describe the indexing of nonassociative powers of a single element x.

4.2 Centrality

We turn our discussion to the nonassociative analogues of familiar group theory objects: subgroups, normal subgroups, and abelian groups.

Definition 4.2.1. Let Q be a quasigroup. A *subquasigroup* P of Q is a subset that forms a quasigroup under the multiplication, right division, and left division of Q.

A notable subquasigroup for upcoming sections is the *diagonal* of a quasigroup, defined as $\hat{Q} = \{(x, x) | x \in Q\}$. The definition of a subquasigroup is an intuitive generalization of a subgroup. The definition of a normal subquasigroup follows a less obvious intuition. While there are multiple characterizations of normal subgroups of a group G, we consider the following proposition:

Proposition 4.2.2. *A subgroup N of the group G is normal if and only if it is the kernel of some homomorphism.*

The kernel of a group homomorphism $\varphi : G \to H$ is defined as the set of elements of G that map to the identity element of H. Since quasigroups are not required to possess an identity element (or even be non-empty), the business of defining a normal subquasigroup becomes a more subtle endeavor. In order to continue the discussion, we will need the notion of congruences. While we can define congruences for a general algebra, we abstain from the spirit of universal algebra and specify congruences for quasigroups.

For a natural number n, we denote a product of n copies of Q as Q^n. The operations on Q^n are defined componentwise. A *congruence* θ on a quasigroup $(Q, \cdot, /, \backslash)$ is an equivalence relation on Q and a subquasigroup of Q^2. Let $f : Q \to P$ be a quasigroup homomorphism. The *kernel of* f is defined as $\ker f = \{(x, y) \in Q^2 | x^f = y^f\}$. It is clear to see $\ker f$ defines an equivalence relation on Q. Moreover, $\ker f$ is a congruence on Q.

Definition 4.2.3. A subquasigroup P of a quasigroup Q is *normal* if there is a congruence θ on Q for which P is a congruence class. We denote this with $P \lhd Q$.

The discussion in subsequent sections will not focus on normal subquasigroups. Rather, we only need the notion of a normal subquasigroup for the following definitions.

A group G is abelian if and only if the diagonal of the group is a normal subgroup of G^2. If G is abelian, then we have G^2 is abelian and that every subgroup of G^2 is normal. Conversely, suppose $\widehat{G}$ is a normal subgroup of G^2. Observe for all $x, y \in G$,

$$(x, y)^{-1}(x, x)(x, y) = (x, y^{-1}xy) \in \widehat{Q}.$$

This shows that $y^{-1}xy = x$ and $xy = yx$ for all $x, y \in G$. This way of thinking about an abelian group lays the groundwork for the nonassociative analogue of an abelian group.

Definition 4.2.4. A quasigroup Q is *central* if the diagonal is a normal subquasigroup of Q^2.

If N is normal subquasigroup of a quasigroup Q, there is a congruence θ that has N as an equivalence class. Rather than taking the quotient of Q by N, we take the quotient of Q by the congruence θ. Let $a, b \in Q$. If a is equivalent to b under θ, we write $(a, b) \in \theta$ or $a\theta b$. We denote equivalence class of a by $a^\theta = \{b \in A \mid a\theta b\}$.

Definition 4.2.5. A congruence θ on a quasigroup Q is *central* if $\widehat{Q} \lhd \theta$.

Corollary 4.2.6. *[13§3.3] Homomorphic images and subquasigroups of central quasigroups are central.*

Corollary 4.2.7. *[13§3.3] Products of central quasigroups are central.*

There are many ways to check whether or not a quasigroup is central. Let Mlt$Q$ be the multiplication group of a quasigroup Q. We define a map

$$\rho : Q \times Q \to \mathrm{Mlt}Q; (x, y) \mapsto R(x\backslash x)^{-1}R(x\backslash y) \tag{4.1}$$

Proposition 4.2.8. *[13§2.5]. Let Q be a quasigroup. The derived quasigroup operation*

$$P : Q^3 \to Q; (x, y, z) \mapsto x\rho(y, z) \tag{4.2}$$

satisfies the identities

$$(x, x, z)P = z \text{ and } (x, y, y)P = x. \tag{4.3}$$

Corollary 4.2.9. *[13§3.2] For an element (x, y) of a central congruence V on a quasigroup Q, and for each z in Q,*

$$z = ((z, x, y)P, y, x)P \tag{4.4}$$

Unpacking the derived operation P in Equation 4.4 yields:

$$z = ((z, x, y)P, y, x)P = (z, x, y)P\rho(y, x) = z\rho(x, y)\rho(y, x).$$

Since the codomain of ρ is the combinatorial multiplication group of a quasigroup Q, we interpret $\rho(x, y)\rho(y, x)$ as a permutation of the underlying set Q. In essence, for a central congruence V on Q and $(x, y) \in V$, one has

$$\rho(x, y)\rho(y, x) = 1 \tag{4.5}$$

For a group G, Equation 4.5 is always true. For elements x, y in a group G,

$$\rho(x, y) = R(x\backslash x)^{-1}R(x\backslash y) = R(1_G)^{-1}R(x^{-1}y = R(x^{-1}y),$$

while

$$\rho(y, x) = R(y\backslash x)^{-1}R(y\backslash x) = R(y^{-1}x).$$

We have $R(x^{-1}y) = R(y^{-1}x)^{-1}$ and that $\rho(x, y)\rho(y, x) = 1$.

While there are various ways to characterize and test for centrality, we will adapt Equation 4.4 into a simple computational test for centrality. Note that for a quasigroup Q, the product Q^2 is congruence on Q. If Q is a central quasigroup, then Q^2 is a central congruence on Q. This follows directly from Definition 4.2.5. If $\rho(x, y)\rho(y, x) \neq 1$ for some x, y in a quasigroup Q, then Q is not a central quasigroup.

Consider the following finite quasigroup.

Table 4.1 A finite quasigroup generated by a single element

Q	1	2	3	4	5	6
1	1	3	2	5	6	4
2	3	2	1	6	4	5
3	2	1	3	4	5	6
4	4	5	6	1	2	3
5	5	6	4	2	3	1
6	6	4	5	3	1	2

First note that this quasigroup is generated by the element 4. We can generate every element via multiplication, right division, or left division. We only display the computations for multiplication:

$$4 \cdot 4 = 1,\ 1 \cdot 4 = 5,\ 5 \cdot 4 = 2,\ 2 \cdot 4 = 6,\ \text{and } 6 \cdot 4 = 3.$$

We refer to this quasigroup $Q = \langle 4 \rangle$ as *monogenic*, meaning singly generated. Notice

$$\rho(3,4) = R(3\backslash 3)^{-1} R(3\backslash 4) = R(3)^{-1} R(4) = (12)(456)(152634) = (16)(2534)$$

while,

$$\rho(4,3) = R(4\backslash 4)^{-1} R(4\backslash 3) = R(1)^{-1} R(6) = (23)(143625) = (26)(3514)$$

Thus, $\rho(3,4)\rho(4,3) = (12)(46)$. This shows that $Q = \langle 4 \rangle$ is not central.

Now consider the free quasigroup on a single generator $F_Q\{x\}$ and the monogenic order 6 quasigroup given above. We define a quasigroup homomorphism $f : F_Q\{x\} \to Q; x \mapsto 4$. Notice this is a surjective quasigroup homomorphism, so $\mathrm{im}(f)$ is the whole quasigroup $Q = \langle 4 \rangle$.

4.3 Nonassociative Integers

Since the free group on one generator is abelian, its nonassociative analogue must be central. The free quasigroup on one generator does not fill the role, so we consider the following character.

Let $\langle R, L \rangle$ be the free group on the set $\{R, L\}$. The integral group algebra is $\mathbb{Z}\langle R, L \rangle$. The integral group algebra becomes a quasigroup under the multiplication $x \cdot y = x^R + y^L$. The multiplication should look familiar. As we saw in Section 2.2.2, $\mathbb{Z}\langle R, L \rangle$ is a $\mathbb{Z}$-linear quasigroup, with 0 as the pointed idempotent element. The right and left divisions are given by

$$x/y = (x - y^L)^{R^{-1}} \text{ and } x\backslash y = (y - x^R)^{L^{-1}}.$$

In fact, $\mathbb{Z}\langle R, L \rangle$ under the multiplication $x \cdot y = x^R + y^L$ is the free central quasigroup on a single generator 1 [13§11.1].

For a quasigroup Q, we can define a differential operator for quasigroup words and identities. We are primarily concerned with quasigroup words in a single generator, so we formulate the definitions accordingly [13§11.1].

Let u and v be quasigroup words in a single generator x. The following product, right quotient, and left quotient rules are defined as follows:

$$(u \cdot v)' = u'R + v'L \tag{4.6}$$

$$(u/v)' = u'R^{-1} - v'LR^{-1}, \tag{4.7}$$

$$(u\backslash v)' = -u'RL^{-1} + v'L^{-1}. \tag{4.8}$$

We have $x' = 1$. We write u' and v' for the derivatives of u and v, respectively.

Remark 4.3.1. Equations 4.6, 4.7, and 4.8 are analogous to the Fox derivative for groups.

The following theorem shows the magma $\mathbb{Z}\langle R, L\rangle^+$ generated by 1 in $\mathbb{Z}\langle R, L\rangle$ under the multiplication $x \cdot y = xR + yL$ is the free magma on a single generator x.

Theorem 4.3.2. *[13§11.1] Derivation gives an isomorphism from the free magma on a singleton $\{x\}$ to the submagma $\mathbb{Z}\langle R, L\rangle^+$ generated by 1 in the multiplicative reduct of the free central pique $\mathbb{Z}\langle R, L\rangle$ generated by 1.*

The proof of this theorem uses an inductive process. We use the same procedure in the following exercise.

Example 4.3.3. We use the proof of Theorem 4.3.2 to solve the differential equations $w' = R^2 + LR + L$ and $w' = (R + L)^3$.

1. First note that $w' = R^2+LR+L = (R+L)R+L$. Since $x' = 1$, we see that $(x\cdot x)' = R+L$. It follows that $w = (x \cdot x) \cdot x$.

2. In order to use the inductive process, we need to expand $w' = (R + L)^3$. We have

$$\begin{aligned} w' &= (R + L)^3 \\ &= (R^2 + RL + LR + L^2)(R + L) \\ &= (R^2 + RL + LR + L^2)R + (R^2 + RL + LR + L^2)L \\ &= ((R + L)R + (R + L)L)R + ((R + L)R + (R + L)L)L \end{aligned}$$

This shows $u' = v' = (R+L)R+(R+L)L$. We saw in the first example that $(x\cdot x)' = R+L$, so $(x^2\cdot x^2)' = u' = v'$. From Equation 4.6, we have $w = u\cdot v$, we have $w = (x^2\cdot x^2)(x^2\cdot x^2)$.

Theorem 4.3.2 exhibits an isomorphism between the free magma on one generator and $\mathbb{Z}\langle R, L\rangle^+$. This shows that the nonassociative analogue of the positive integers $\mathbb{Z}^+$ faithfully represents magma words in a single generator. However, the same does not hold for quasigroup words in a single generator.

Proposition 4.3.4. *Derivation is not a faithful representation from the free quasigroup on a single $\{x\}$ to the central pique $\mathbb{Z}\langle R, L\rangle$ generated by 1.*

Proof. Recall the order six monogenic quasigroup generated by 4. Consider the homomorphism $h : Q = \langle 4\rangle \to \mathbb{Z}/_2; 4 \mapsto 1$. Notice that this is a surjective homomorphism. Let $\theta = \ker h$. The universal algebra analogue of the First Isomorphism Theorem for groups says the following diagram commutes.

$$\begin{array}{ccc} Q & \xrightarrow{h} & \mathbb{Z}/_2 \\ {\scriptstyle\pi}\downarrow & \nearrow_{\bar{h}} & \\ Q^\theta & & \end{array} \tag{4.9}$$

Here, $\pi : Q \to Q/\theta; q \mapsto q^\theta$ is the natural projection homomorphism. Since h is surjective, $\bar{h}$ is an isomorphism. Since $\mathbb{Z}/_2$ is an abelian group, it is certainly a central quasigroup. So we have that Q/θ is a central quasigroup. If there were a larger central quotient of Q, say Q/ψ, it would have to be of order 3 and disjoint from Q/θ. This implies $Q \cong Q/\theta \times Q/\psi$. The product of two central quasigroups is central (Corollary 4.2.7), which implies Q is central. We know this to be false, so Q/θ is the largest central quotient. Note $Q/\theta = \{4^\theta, 1^\theta\}$.

Recall the quasigroup homomorphism $f : F_Q\{x\} \to Q; x \mapsto 4$ and the homomorphism $\pi : Q \to Q/\theta; q \mapsto q^\theta$ from above. The differential operator $\frac{\partial}{\partial x} : F_Q\{x\} \to \mathbb{Z}\langle R, L\rangle$ is defined by $x \mapsto 1$. The map $g : \mathbb{Z}\langle R, L\rangle \to Q/\theta$ is defined by $1 \mapsto 4^\theta$. Now consider the following diagram.

$$\begin{array}{ccc} F_Q\{x\} & \xrightarrow{\frac{\partial}{\partial x}} & \mathbb{Z}\langle R, L\rangle \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} \\ Q = \langle 4\rangle & \xrightarrow[\pi]{} & Q/\theta \end{array} \tag{4.10}$$

A quick diagram chase shows $x\frac{\partial}{\partial x}g = 1^g = 4^\theta = 4\pi = x^f\pi$. So we have that (4.10) commutes. Since this diagram commutes, we see that $\frac{\partial}{\partial x}$ has a nontrivial kernel. Thus, the nonassociative analogue of the integers does not faithfully index quasigroup words in a single generator. $\square$

CHAPTER 5. FUTURE WORK

This dissertation exhibits initial work in the study of the free quasigroup on a single generator and quasigroup representations. We will outline some future directions for each project.

5.1 Permutational Intertwinings

In Chapter 2, we saw that ordinary characters are sufficient for classifying permutation representations of linear piques defined on cyclic groups whose order is not divisible by 8. The main theorem holds for any cyclic group, provided the automorphisms of the 2-component form a cyclic group. The next step is to investigate the extent to which ordinary characters classify $\mathbb{Z}$-linear piques defined on elementary abelian groups.

5.1.1 Linear piques on elementary abelian groups

Let p be a prime. We will consider linear piques built on elementary abelian groups. The automorphism group of an elementary abelian group is $\mathsf{GL}_n(\mathbb{F}_p)$. When we built piques on an elementary abelian group $A \cong (\mathbb{Z}/p)^n$ for some $n \in \mathbb{N}$, we take ρ, λ to be matrices from $\mathsf{GL}_n(\mathbb{F}_p)$.

Let $U \in \mathsf{GL}_n(\mathbb{F}_p)$ and $v \in (\mathbb{F}_p)^n$. Computing the number of fixed points of U is equivalent to finding the number of elements in kernel of $U - I_n$. Suppose the dimension of $ker(U - I_n)$ is k. It follows that there are p^k many vectors in $(\mathbb{Z}/p)^n$ that satisfy $vU = v$. Hence, $U\phi = p^k$.

Example 5.1.1. Consider the two-dimensional vector space over $\mathbb{F}_3$. Let $C = \begin{bmatrix} 2 & 0 \\ 1 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}$. The matrices have the same characteristic polynomial $p_B(t) = p_C(t) = (t-2)(t-1)$. It

follows that B and C have the same Jordan canonical form $J = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ and the same number of fixed points. Since $B \neq C$ and

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix},$$

B and C are not permutation-similar. However, B and C are similar by $S = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$.

Consider the piques $(\mathbb{F}_3^2, x \circ_1 y = xB + y)$ and $(\mathbb{F}_3^2, x \circ_2 y = xC + y)$. These piques yield isomorphic representations in characteristic p. The matrix S serves as the linear intertwining. This shows the result of Theorem 2.3.10 does not apply to linear piques defined on elementary abelian groups.

Consider the matrix $T_1 = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$ and $T_2 = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}$ in $\mathsf{GL}_2(\mathbb{F}_3)$. Notice $p_{T_1}(t) = p_{T_2}(t) = t^2 + 1$. This polynomial does not split over $\mathbb{F}_3^2$, but notice

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}.$$

The matrices T_1, T_2 are permutation-similar even though their characteristic polynomials do not split.

5.2 Peri-Catalan Numbers

The Catalan numbers arise in many combinatorics questions. It is curious to see that a nonassociative relative of the Catalan numbers is a new sequence. Even the sequence of thirds, given by $\frac{P_n}{3}$ for $n > 1$, is a new sequence in that it is not on the Online Encyclopedia of Integer Sequences. It will be fruitful to investigate what other structures are related to the peri-Catalan numbers.

Additionally, the fact that each peri-Catalan number is a multiple of 3 is rather surprising. Before the recursive formula was fully developed, initial computations of small peri-Catalan numbers showed that (IR), (SR), and (DR) cancellations were not evenly distributed at each

step in the inductive process. However, on the whole, the number of cancellations for the six quasigroup identities were equal.

In [6], rooted binary trees are constructed with ϵ on the leaves and functions from a set E in the remaining vertices. In Grust's work, ϵ denotes the empty tree. If we take E to be the set of three quasigroup binary operations, Grust's construction of trees is similar to the construction of trees representing unreduced quasigroup words in a single generator.

5.2.1 A generating function

While the recursive formula given in Theorem 3.8.14 is easy to compute for the first ten peri-Catalan numbers, the next step in the work is to find a generating function for the n-th peri-Catalan number. A goal is to study asymptotics of the peri-Catalan numbers. Already, with the first ten terms, we see some interesting behavior. Below, we define $R_n = \frac{P_n}{3^{n-1}C_n}$.

Table 5.1 The first ten peri-Catalan numbers and their ratios.

n	C_n	$3^{n-1}C_n$	P_n	R_n	$R_n - R_{n-1}$	$\frac{P_n}{3}$	R_n/R_{n-1}
1	1	1	1	1	-	-	-
2	1	3	3	1	0	1	1
3	2	18	12	0.6667	0.3333	4	0.6667
4	5	135	87	0.6444	0.0222	29	0.9667
5	14	1134	666	0.5873	0.0571	222	0.9113
6	42	10,206	5,478	0.5367	0.0506	1826	0.9139
7	132	96,228	47,322	0.4918	0.0450	15774	0.9162
8	429	938,223	422,145	0.4499	0.0418	140715	0.9149
9	1,430	9,382,230	3,859,026	0.4113	0.0386	1286342	0.9141
10	4,862	95,698,746	35,967,054	0.3758	0.0355	11989018	0.9137

5.2.2 Words in n generators

The Catalan and peri-Catalan numbers give the number of length n magma and quasigroup words in a single generator, respectively. A length n magma word in r generators has r^n many possibilities for each argument, with C_n many ways to bracket the nonassociative multiplication. This yields a total of r^nC_n length n magma words in r generators.

The cancellations we saw for length n quasigroup words in a single generator may not hold for quasigroup words in r generators. A natural extension to find a recursive formula to compute the number of inequivalent reduced length n quasigroup words in r generators. The number of reduced trees with multiplication, right division, and left division in the root vertex are equal. Triality and parastrophes were given minimal consideration over the course of this project. Future work will revisit the inductive process through the eyes of parastrophes and triality.

5.3 A Faithful Representation of the Free Quasigroup

In Chapter 4, we saw that derivation is a faithful representation from the free magma on the single generator $\{x\}$ to the central pique $\mathbb{Z}\langle R, L\rangle$ generated by 1 under the multiplication $x \cdot y = x^R + y^L$. Since derivation is not a faithful representation of reduced quasigroup words in a single generator, further work will investigate what the elements kernel of the representation. Another goal is finding a faithful representation of the free quasigroup on a single generator.

The *restricted peri-Catalan* numbers give the number of length n reduced quasigroup words in a single generator whose derivatives are distinct. The Nielsen-Schreier Theorem states that every subgroup of a free group is free. Once I get a characterization of the kernel of $\frac{\partial}{\partial x} : F_Q\{x\} \to \mathbb{Z}\langle R, L\rangle$, I can study the asymptotics of the restricted peri-Catalan numbers.

APPENDIX A. FIXED POINTS FOR LINEAR PIQUES ON $\mathbb{Z}/_{2^n}$

The following is a computer program written in Sage. I used it to compute the number of fixed points and permutations for automorphisms of linear piques defined on $\mathbb{Z}/_{2^n}$.

```
#include<stdio.h>


main()
{
n=5
allperms=[]
U=[ 2*i+1 for i in range(1,2^(n-1))]
for aut in U:
    i=1
    next_sm_st_elt=Set(range(1, 2^n))
    perms=[]
    aut_fixedpoint=1
    aut_cycle_type=[]
    while i:
        startelement=min(list(next_sm_st_elt))
        v=(startelement,)
        next_elt=startelement
        while i:
            #print(v)
            if next_elt==mod(aut*next_elt,2^n):
```

```
                aut_fixedpoint=aut_fixedpoint+1
            next_elt=mod(aut*next_elt,2^n)
            #print(next_elt)
            if next_elt==startelement:
                #print(len(list(v)))
                #if len(list(v))==1:
                    #aut_fixedpoint=aut_fixedpoint+1
                break
            v=v+(next_elt,)
        aut_cycle_type.append(len(list(v)))
        perms.append(v)
        next_sm_st_elt=next_sm_st_elt.difference(Set(v))
        if next_sm_st_elt.is_empty()==True:
            break
    allperms.append(perms)
    #print(aut_fixedpoint)
    #print(sorted(aut_cycle_type,reverse=1))
    print(perms)
}
```

APPENDIX B. CHARACTER TABLES

Table B.1 Full character table for linear piques defined on $\mathbb{Z}/_3$

ρ	λ	$\chi(R)$	$\chi(L)$
1	1	3	3
1	2	3	1
2	1	1	3
2	2	1	1

Table B.2 Full character table for linear piques defined on $\mathbb{Z}/_4$

ρ	λ	$\chi(R)$	$\chi(L)$
1	1	4	4
1	3	4	1
3	1	1	4
3	3	1	1

Table B.3 Full character table for linear piques defined on $\mathbb{Z}/_5$

ρ	λ	$\chi(R^3L)$	$\chi(RL^2)$	$\chi(R)$	$\chi(L^2)$
1	2	1	1	5	1
1	3	1	1	5	1
4	2	1	5	1	1
4	3	1	5	1	1
1	4	1	5	5	5
2	2	5	1	1	1
3	3	5	1	1	1
3	2	1	1	1	1
4	4	5	1	1	5
1	1	5	5	5	5

Table B.4 Partial character table for linear piques defined on $\mathbb{Z}/_{32}$.

ρ	λ	R	R^2	R^4	RL	R^2L	R^4L	RL^2	R^2L^2	R^4L^2	RL^4	R^2L^4	R^4L^4	L	L^2	L^4
3	15	2	8	16	2	2	2	2	8	16	2	8	16	2	32	32
3	31	2	8	16	2	2	2	2	8	16	2	8	16	2	32	32
11	15	2	8	16	2	2	2	2	8	16	2	8	16	2	32	32
11	31	2	8	16	2	2	2	2	8	16	2	8	16	2	32	32
19	15	2	8	16	2	2	2	2	8	16	2	8	16	2	32	32
19	31	2	8	16	2	2	2	2	8	16	2	8	16	2	32	32
27	15	2	8	16	2	2	2	2	8	16	2	8	16	2	32	32
27	31	2	8	16	2	2	2	2	8	16	2	8	16	2	32	32
3	23	2	8	16	2	2	2	2	8	32	2	8	16	2	16	32
11	7	2	8	16	2	2	2	2	8	32	2	8	16	2	16	32
11	23	2	8	16	2	2	2	2	8	32	2	8	16	2	16	32
19	7	2	8	16	2	2	2	2	8	32	2	8	16	2	16	32
19	23	2	8	16	2	2	2	2	8	32	2	8	16	2	16	32
27	7	2	8	16	2	2	2	2	8	32	2	8	16	2	16	32
27	23	2	8	16	2	2	2	2	8	32	2	8	16	2	16	32
11	11	2	8	16	2	2	2	2	16	8	2	8	32	2	8	16
19	19	2	8	16	2	2	2	2	16	8	2	8	32	2	8	16
27	27	2	8	16	2	2	2	2	16	8	2	8	32	2	8	16
3	19	2	8	16	2	2	2	2	16	8	2	8	32	2	8	16
11	27	2	8	16	2	2	2	2	16	8	2	8	32	2	8	16
19	3	2	8	16	2	2	2	2	16	8	2	8	32	2	8	16
27	11	2	8	16	2	2	2	2	16	8	2	8	32	2	8	16
3	27	2	8	16	2	2	2	2	32	8	2	8	32	2	8	16
11	19	2	8	16	2	2	2	2	32	8	2	8	32	2	8	16
19	11	2	8	16	2	2	2	2	32	8	2	8	32	2	8	16
27	3	2	8	16	2	2	2	2	32	8	2	8	32	2	8	16
3	11	2	8	16	2	2	2	2	32	8	2	8	32	2	8	16
11	3	2	8	16	2	2	2	2	32	8	2	8	32	2	8	16
19	27	2	8	16	2	2	2	2	32	8	2	8	32	2	8	16
27	19	2	8	16	2	2	2	2	32	8	2	8	32	2	8	16

APPENDIX C. CALCULATIONS FOR SMALL PERI-CATALAN NUMBERS

For $n = 1$, there is a single quasigroup word of length 1. We have $P_1 = 1$.

For $n = 2$, we have $P_2 = 3P_1P_1 = 3$.

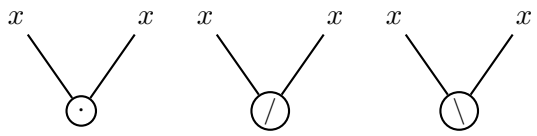


Figure C.1 The trees for P_2.

For $n = 3$,

$$\begin{aligned} P_3 =& 2(3P_2P_1 - m(1,1) - r(1,1) - r(1,1)) \\ =& 2(3 \cdot 3 \cdot 1 - 1 - 1 - 1) \\ =& 2(9 - 3) = 12 \end{aligned}$$

Using the data below, we have:

$$\begin{aligned} P_4 =& 2(3P_3P_1 - m(2,1) - r(2,1) - r(1,2)) + 3P_2P_2 \\ =& 2(3 \cdot 12 - 2 - 2 - 2) + 3 \cdot 3 \cdot 3 \\ =& 2(36 - 6) + 27 = 60 + 27 = 87 \end{aligned}$$

For $n = 5$, we have:

$$\begin{aligned}
P_5 =& 2\sum_{k=1}^{2} 3P_{n-k}P_k - m(n-2k,k) - r(n-2k,k) - r(k,n-2k) \\
=& 2[(3P_4P_1 - 10 - 10 - 10) + (3P_3P_2 - 2 - 2 - 2)] \\
=& 2[(3 \cdot 87 - 30) + (3 \cdot 12 \cdot 3 - 6)] \\
=& 2(231 + 102) = 666
\end{aligned}$$

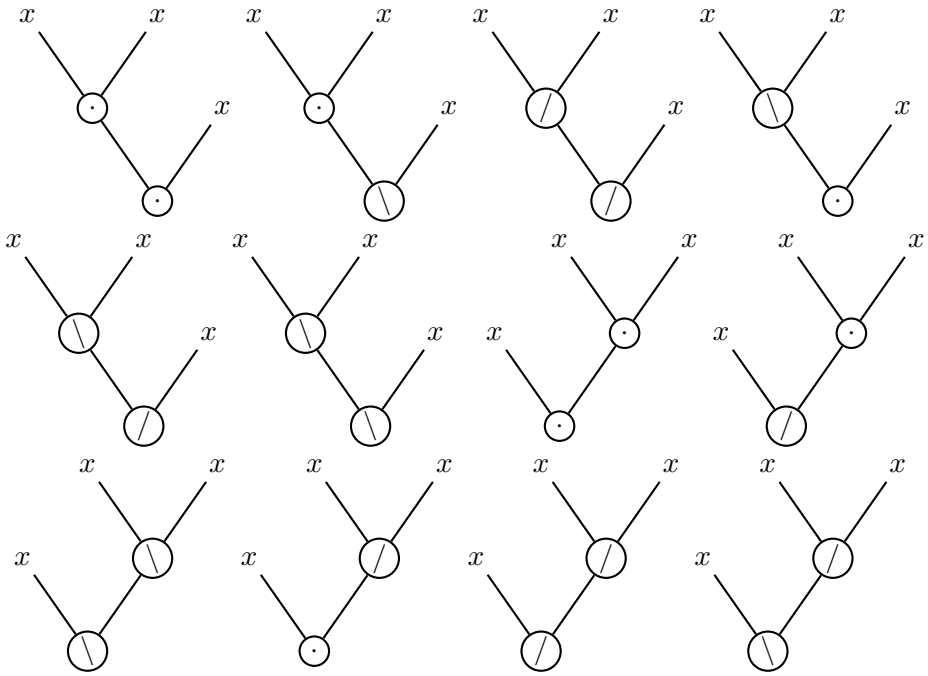


Figure C.2 All possible trees with 3 arguments

BIBLIOGRAPHY

[1] A. Abraham, J. Dvorský, E. Ochodková, and V. Snášel, "Large quasigroups in cryptography and their properties testing", NaBIC 2009, IEEE, 2010, 965–971. DOI:10.1109/NABIC.2009.5393884

[2] G.B. Belyavskaya, "Abelian quasigroups are T-quasigroups", *Quasigroups Related Systems* **1** (1994), 8–21.

[3] C. Bergman, *Universal Algebra, Fundamentals and Selected Topics*, CRC Press, Boca Raton, FL, 2012.

[4] P. Cameron, *Permutation Groups*, Cambridge University Press, Cambridge, 1999.

[5] A. Drápal, "Group isotopes and a holomorphic action", *Results Math.* **54** (2009), 253–272.

[6] T. Grust, "Comprehending Queries", *Universität Konstanz Ph.D. thesis* 1999.

[7] L. Long and J. Smith, "Catalan Loops", *Math. Proc. Cambridge Philos. Soc.*, **149** (2010), no. 3, 445-453.

[8] H. Minc, "Index polynomials and bifurcating root-trees", *Proc. Roy. Soc. Edin.*, A, 65, 319-341, 1957.

[9] P. Němec and T. Kepka, "T-quasigroups", I, II, *Acta Univ. Carolinae–Math. et Phys.* **12** (1971), no. 1, 39–49; no. 2, 31–49.

[10] I. Pak, "History of Catalan Numbers", Appendix B in: R. Stanley, *Catalan Numbers*, Cambridge University Press, 2015.

[11] J.-P. Serre, *Linear Representations of Finite Groups*, Springer-Verlag, New York, NY, 1977.

[12] W.R. Scott, *Group Theory*, Prentice-Hall, Englewood Cliffs, NJ, 1964.

[13] J.D.H. Smith, *An Introduction to Quasigroups and Their Representations*, Chapman and Hall/CRC, Boca Raton, FL, 2007.

[14] J.D.H. Smith, "Groups, triality, and hyperquasigroups", *J. Pure Appl. Algebra* **216** (2012), 811–825.