College of the Holy Cross

A Study of Knots and Quandles

Mathematics Honors Thesis

Author: Zhaoqi Wu
Email: zwu25@g.holycross.edu

Supervisor: Prof. Neranga Fernando

May 2025

Acknowledgements

The author is heavily indebted to the WEISS Summer Research Program for research funding and housing during Summer 2023 and Summer 2024. He is also grateful to the J.D. Power Center for RA funding in fall 2024. He would also like to thank the Department of Mathematics and Computer Science and College of the Holy Cross for travel funding.

Abstract

We explore the mathematical theory of knots through the lens of algebraic structures known as kei and quandles. We begin by introducing classical knot invariants and then study the fundamental kei of a knot as a tool for distinguishing knot types. We generalize this approach using various kinds of quandles, including Alexander and dihedral quandles, and investigate their associated polynomial invariants. We also examine the connection between quandles and group theory, as well as their algebraic representations in quandle rings. Moreover, we analyze idempotent elements in quandle rings over finite fields, providing both general results and specific examples.

Contents

1. Introduction

Knot theory is a branch of topology concerned with the study of closed, non-self-intersecting curves embedded in three-dimensional space. Its mathematical development began in the 19th century, initially inspired by physical theories. In 1867, Lord Kelvin proposed the vortex atom theory, which viewed atoms as knotted tubes of ether. This hypothesis led Peter Guthrie Tait to produce some of the earliest knot tables, systematically classifying knots by crossing number. Although Kelvin's theory was later discredited, Tait's classification laid the foundation for modern knot theory.

Earlier contributions also came from Carl Friedrich Gauss, who defined the linking number to measure the entanglement between two curves. Johann Benedict Listing, a student of Gauss, worked on related topological concepts and introduced early terminology relevant to knots.

A major formal advancement occurred in the 1920s with Kurt Reidemeister, who introduced the three Reidemeister moves. These moves gave a rigorous framework for determining whether two knot diagrams represent the same knot. Subsequently, knot invariants were developed to distinguish knots algebraically. J. W. Alexander introduced the Alexander polynomial in 1928, and in 1984, Vaughan Jones discovered the Jones polynomial, which revealed unexpected connections between knot theory and statistical mechanics. This discovery spurred further development of polynomial invariants and established new links between topology and quantum field theory.

In addition to its mathematical significance, knot theory has practical applications. In biology, it models the knotting of DNA molecules; in chemistry, it aids in the synthesis of molecular knots; and in physics, it contributes to the understanding of topological quantum field theories and quantum computing.

Modern knot theory integrates algebraic methods such as quandles, knot groups, and braid groups, enhancing our ability to study knot equivalence and classification. These tools not only deepen the theoretical framework but also connect knot theory with

other areas of mathematics such as group theory, representation theory, and category theory.

A quandle is a non-empty set with a binary operation which satisfies three axioms. The three axioms of a quandle algebraically encode the three Reidemeister moves in knot theory. Quandles in general are non-associative algebraic structures introduced independently in the 1980s by Joyce [Joyce (1982)] and Matveev [Matveev (1982)] with the purpose of constructing knot invariants. In this thesis, we explore different types of quandles and their algebraic properties, and explain how to use quandles to distinguish different knots. Quandles have been investigated from an algebraic point of view by many because of their connection to Lie algebras, Hopf algebras, quasigroups and Moufang loops, Frobenius algebras and Yang-Baxter equation, ring theory, etc. We refer the reader to [Elhamdadi and Nelson(2015)], which is an excellent book written on the theory of quandles, and [Macquarrie(2011)] for more details about quandles.

In 2019, Bardakov, Passi, and Singh introduced quandle rings and rack rings analogous to group rings for groups [BPS(2019)]. Since then, several authors have studied zero divisors, idempotents and other ring theoretic properties in quandle rings. We refer the reader to [BPS(2019), Bardakov, Passi, and Singh(2022), Elhamdadi et al.(2019), Elhamdadi et al.(2022), Elhamdadi and Swain(2024)] for more details about quandle rings.

The following is the organization of the thesis.

In Section 2, we begin by introducing the mathematical definition of knots. The formal study of knots was motivated by 19th-century physics, particularly Lord Kelvin's vortex atom theory. One of the earliest mathematical approaches came from Carl Friedrich Gauss, who defined the linking number. We explore how knots are considered equivalent under ambient isotopy, and we present classical knot invariants, such as the crossing number and tricolorability, which are used to distinguish between different knots. These invariants were systematized by Peter Guthrie Tait, who compiled the first tables of knots.

In Section 3, we proceed by studying kei, or involutive quandles, which were introduced by Mituhisa Takasaki in 1942. Kei are algebraic structures defined by three axioms: idempotency, involutivity, and right self-distributivity. We construct the fundamental kei of a knot and use it as a knot invariant. We also define kei homomorphisms and the kei counting invariant, which counts the number of homomorphisms from a knot's fundamental kei into a fixed finite kei.

In Section 4, we examine several types of quandles: Latin quandles, dihedral quandles, and Alexander quandles. We discuss their construction, algebraic properties, and how they are used to define colorings of knot diagrams. We also study two major polynomial invariants: the Alexander polynomial and the quandle polynomial.

In Section 5, we explore the algebraic connections between quandles and groups. We study how quandles can generate groups via their column structures and examine the fundamental group of the knot complement, a concept first formulated by Max Dehn and further developed by Emil Artin. We also review braid groups, introduced by Artin in the 1920s, which represent knots as closures of braids. Additionally, we define quasigroups, generalizing group-like operations, and describe their intersection with quandle theory.

In Section 6, we talk about racks as algebraic structures that satisfy right self-distributivity without requiring idempotency. The concept of racks was first formally introduced by John Conway and Gavin Wraith in the 1950s, and later independently studied by David Joyce in the 1980s as a generalization of group conjugation operations. In this section, we explore the algebraic structure of racks and introduce the rack polynomial, which was developed to distinguish finite racks through combinatorial data.

In Section 7, we then study shelves, which are sets equipped with a binary operation that satisfies only the self-distributive property. This minimal structure first appeared implicitly in the work of Richard Laver during his study of set theory and large cardinals in the 1990s. We provide examples of shelves and define the shelf polynomial, a recent

invariant designed to capture structural features specific to these non-idempotent self-distributive systems.

In Section 8, we investigate quandle rings and rack rings. Quanlde rings were first studied mainly for their algebraic properties, but they have garnered a lot of attention recently due to their applications in knot theory. In [Elhamdadi and Swain(2024)], the authors showed that the idempotents in quandle rings can be used to construct stronger knot invariants.

In Section 9, we investigate idempotent elements in quandle rings over Z_p. We begin Section 9 with the case where $|Q| = 3$. We generate systems of equations for the coefficients of idempotents and solve them using Gröbner basis.

In Section 10, we find formulas for the number of idempotents in quandle rings $\mathbb{Z}_p[Q]$, where the order of quandle is 3 or 5 and p is a prime number.

In Section 11, we present a generalization of our technique used in Section 9 to quandle rings where the quandle is a connected quandle of order 5. However, due to computational complexity, we can only generalize the patterns of connected quandles of order up to 5.

To the best of our knowledge, the results in Sections 9, 10 and 11 have not appeared in the literature.

The appendix contains essential background material on groups and rings. These summaries are intended to support the algebraic concepts discussed throughout the thesis and provide the reader with a clear reference for key definitions and theorems.

Throughout the thesis, we denote a quandle by X or Q.

2. Knots

2.1. What is a Knot?

Definition 2.1. A *knot* is a simple closed curve. Simple means it doesn't intersect itself. Closed means it has no loose ends.

Definition 2.2. A *knot diagram* is a two-dimensional projection of a three-dimensional knot. Over and under crossings are indicated by small gaps in the strands to show which strand is on top.

Definition 2.3. A knot is called *tame* if it has a knot diagram with finite number of crossings. A knot is called *wild* if every projection of it has infinitely many crossings. In this thesis, we only consider tame knots.

Example 2.4. *Trefoil Knot is the simplest nontrivial knot. It has a crossing number of three, meaning the minimum number of crossings in any projection of the knot is three.*

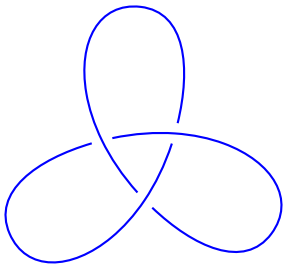


Figure 1. The knot diagram of trefoil Knot.

Example 2.5. *Figure-Eight Knot has a crossing number of four and is the simplest knot with an even number of crossings.*

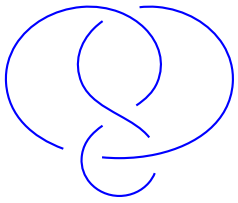
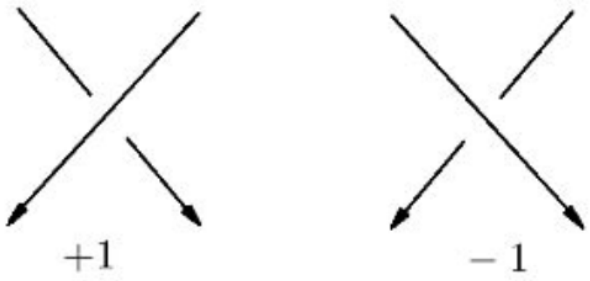


FIGURE 2. The knot diagram of figure-eight Knot.

Definition 2.6. In an oriented knot diagram, each crossing can be classified as either a *positive crossing* or a *negative crossing*, depending on the orientation of the strands.

- A crossing is called **positive** if the *under strand rotates clockwise to reach the over strand.*
- A crossing is called **negative** if the *under strand rotates counterclockwise to reach the over strand.*



2.2. **Knot Invariants.**

Definition 2.7. A *knot invariant* is a function $f : \mathcal{K} \to X$ from the set of all knot diagrams to a set X such that for each Reidemeister move, we have

$$f(K_1) = f(K_2)$$

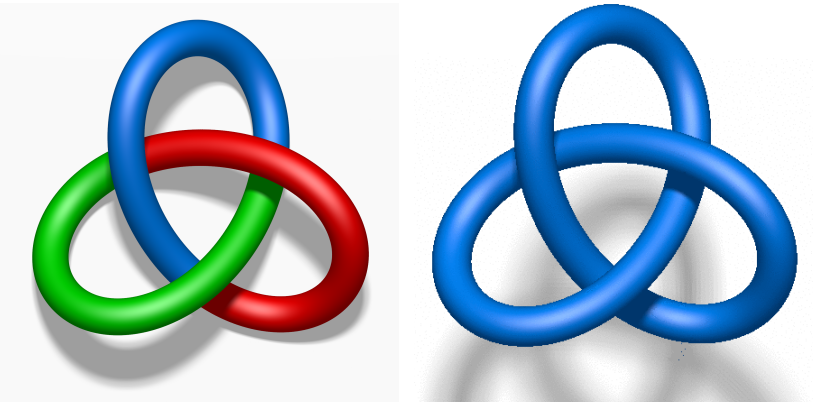
where K_1 is the knot diagram before the move and K_2 is the same diagram after the move. If f is a knot invariant, then any two diagrams related by Reidemeister moves must give the same value when we evaluate f.

2.2.1. *Fox Tricoloring. Fox Tricoloring* is a knot invariant which was introduced by Ralph Fox in the 1950s.

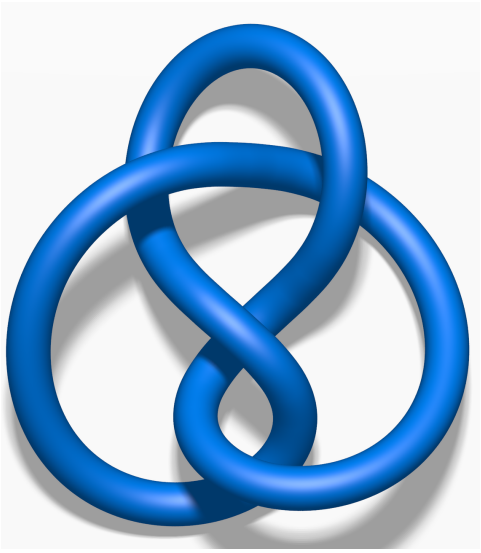
A *tricoloring* of a knot diagram is a choice of color for each arc in the diagram from a set of three colors. A tricoloring is *valid* if at every crossing we either have all three colors the same or all three colors different.

A valid tricoloring is *nontrivial* if it uses all three colors.

Example 2.8. *The trefoil knot is tricolorable.*



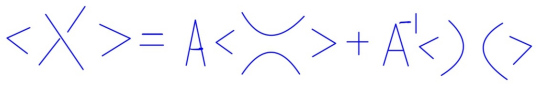
Example 2.9. *The figure-8 knot is not tricolorable. This shows that the figure-8 knot is a different knot.*



2.2.2. *Jones Polynomial.*

Definition 2.10. The bracket polynomial, $\langle L\rangle$ of a link L is defined recursively using the following rules:

(i) $< O >= 1$, we denote the bracket polynomial of trivial knot is 1.



(ii)

(iii) For a disjoint union of a loop and a link L:$\langle L \cup \bigcirc\rangle = \delta \langle L\rangle$, where $\delta = -A^2 - A^{-2}$.

The Jones polynomial is a polynomial invariant of a knot or link, discovered by Vaughan Jones in 1984. It can be defined using the bracket polynomial, also known as the Kauffman bracket polynomial, with an additional normalization factor.

Definition 2.11. The Jones polynomial of a link L s given by:

$$V_L(t) = (-A^3)^{-w(L)}\langle L\rangle\big|_{A=t^{-1/4}}.$$

Here L represents a specific knot or link. It is the object for which we are calculating the Jones polynomial.

$\langle L\rangle$ denotes the bracket polynomial (also called the Kauffman bracket) of the knot or link L. This is a key polynomial invariant that encodes information about the knot or link, and it is computed through a recursive process based on the crossing structure of the knot or link.

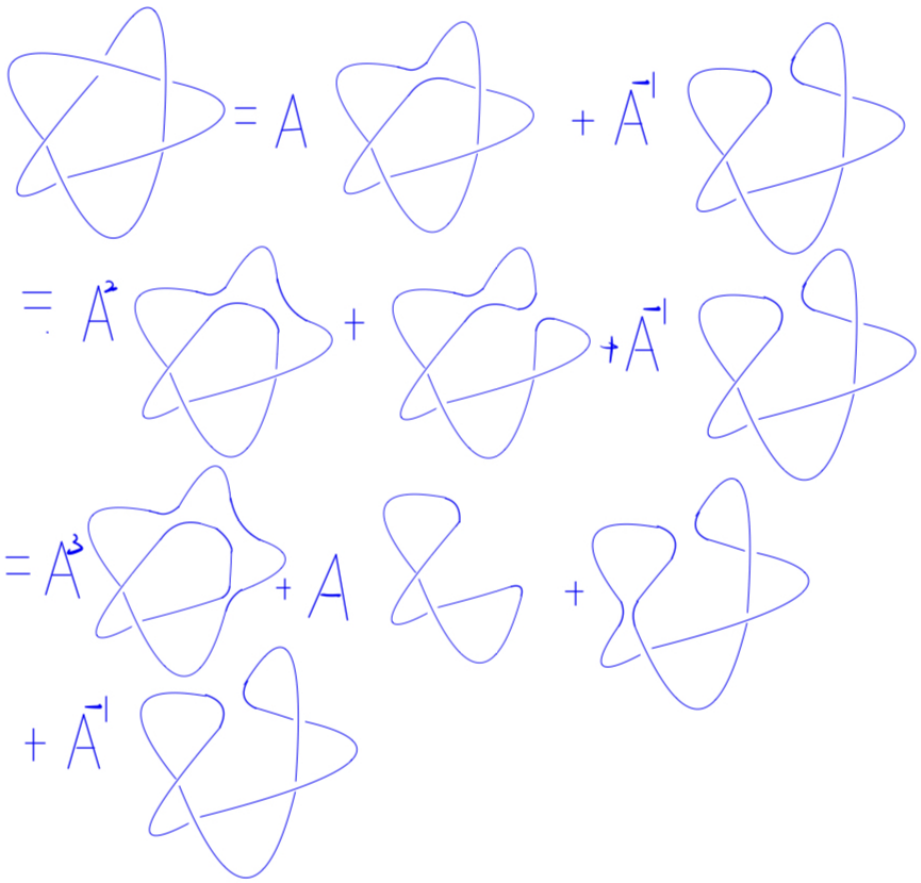
After we get the bracket polynomial. We can get the X polynomial of

$$X_L(A) = (-A^3)^{-w(L)}\langle L\rangle$$

Finally, we replace A by $t^{-1/4}$ translates the X polynomial into the Jones polynomial.

Here we give a few examples on how to compute the Jones polynomial of a given knot.

Example 2.12. *We compute the Jones polynomial of the knot* 5_1.



First we compute the bracket polynomial of the knot 5_1.

$$\begin{aligned}\langle L\rangle = {} & A^3\left(-A^4-A^{-4}\right)+A\left(-A^{-3}\right)^2+\left(-A^{-3}\right)^3+A^{-1}\left(-A^{-3}\right)^4\\ & -A^7-A^{-1}+A^{-5}+\left(-A^{-9}\right)+A^{-13}\end{aligned}$$

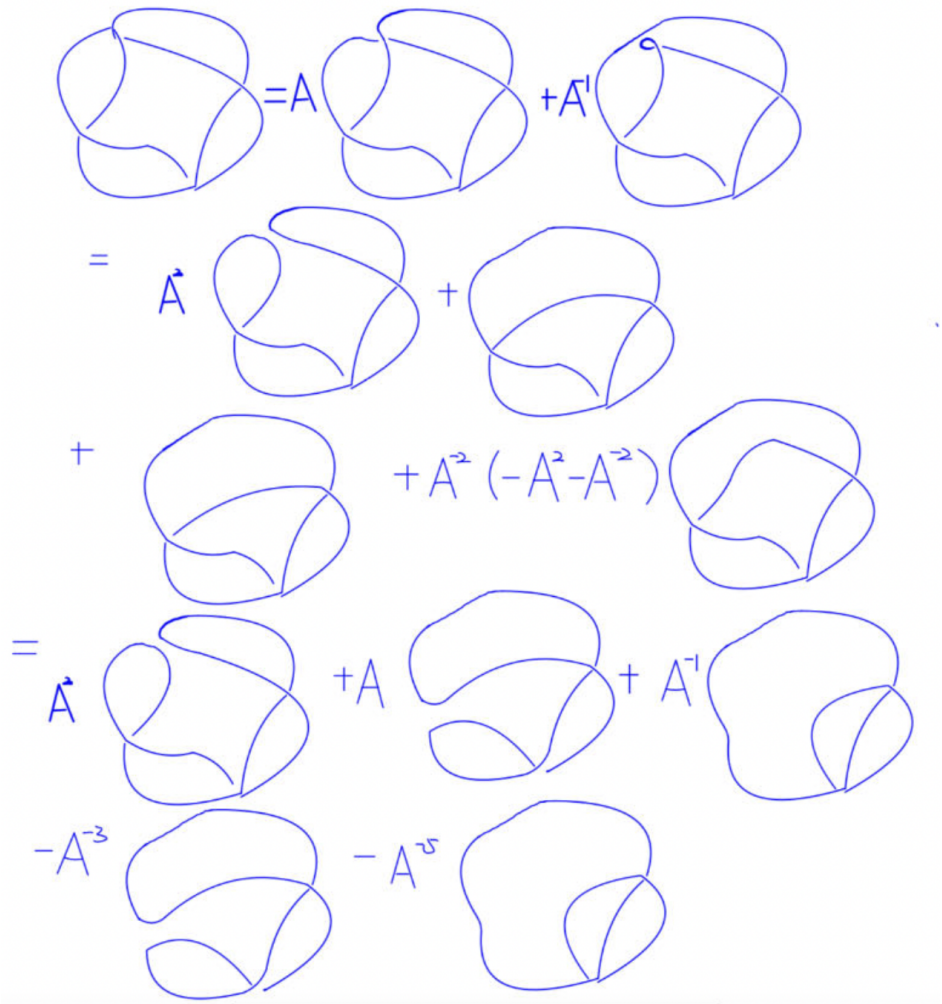
Next we compute the X polynomial of the knot 5_1.

$$\begin{aligned}\left(-A^{-3}\right)^{\mathrm{w(L)}}\quad \langle L\rangle &= \left(-A^{-3}\right)^5\cdot\left(-A^7-A^{-1}+A^{-5}+\left(-A^{-9}\right)+A^{-13}\right)\\ &= A^{-8}+A^{-16}-A^{-20}+A^{-24}-A^{-28}\end{aligned}$$

We replace A by $t^{-\frac{1}{4}}$ to obtain the Jones Polynomial of the knot 5_1 given below.

$$V_{5_1}(t)=t^2+t^4-t^5+t^6-t^7$$

Example 2.13. *We compute the Jones polynomial of the knot* 5_2.



First, we compute the bracket polynomial of 5_2 knot.

$$\begin{aligned}\langle L\rangle &= A^2\left(-A^3\right)^3 + A\left(-A^3\right)^2 + A^{-1}\left(A^4 - A^{-4}\right)\\ &\quad - A^{-3}\left(A^3\right)^2 - A^{-5}\left(A^{-4} - A^4\right)\\ &= -A^{-11} + A^7 - 2A^3 - A^{-5} + A^{-1} + A^{-9}\end{aligned}$$

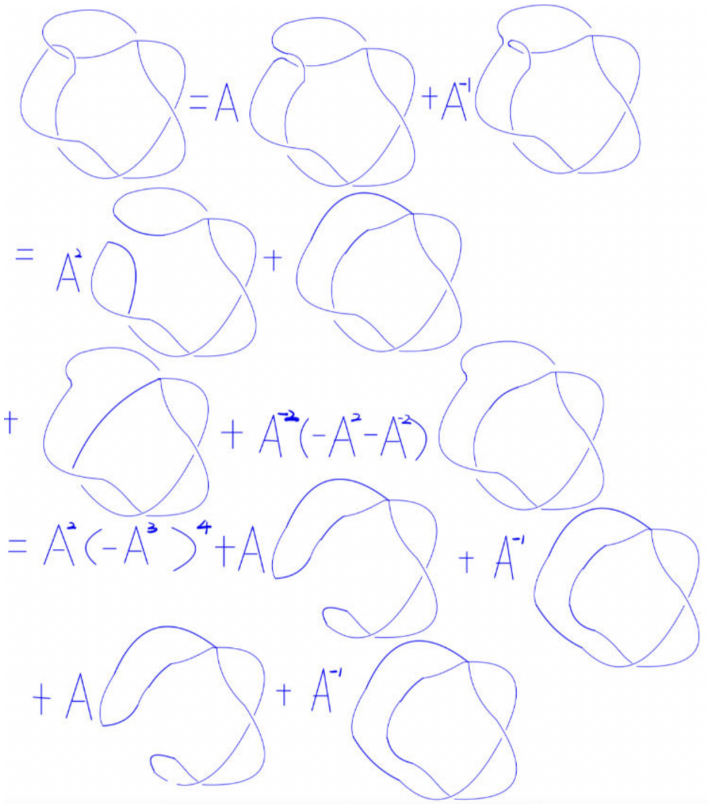
Now we compute the X polynomial of the knot 5_2.

$$\begin{aligned}\left(-A^{-3}\right)^{\mathrm{w(L)}} \quad \langle L\rangle &= \left(-A^{-3}\right)^5 \cdot \quad \left(-A^{11} + A^7 - 2A^3 - A^{-5} + A^{-1} + A^{-9}\right)\\ &= A^{-4} - A^{-8} + 2A^{-12} + A^{-20} - A^{-16} - A^{-24}\end{aligned}$$

We replace A by $t^{-\frac{1}{4}}$ to obtain the Jones Polynomial of the knot 5_2 given below.

$$V_{5_2}(t) = t^1 - t^2 + 2t^3 - t^4 + t^5 - t^6$$

Example 2.14. *We compute the Jones polynomial of the knot* 6_1*:*



First, we compute the bracket polynomial of the knot 6_1.

$$\begin{aligned}\langle L\rangle &= A^2\left(-A^3\right)^4 + tA\left(-A\right)^3 + 2\left(-A^3\right)^2 + A^2\left(-A^4 - A^{-4}\right) - A^8\left(-A^2 - A^{-2}\right)\\ &\quad + A^2\left(-A^2 - A^{-2}\right)\left(A^3\right)^2 + A^{-4}\left(-A^2 - A^{-2}\right)\left(A^{-4} + A^4\right)\\ &= A^{14} - A^{10} + 2A^6 - 2A^2 - A^{-6} + A^{-2} + A - 10\end{aligned}$$

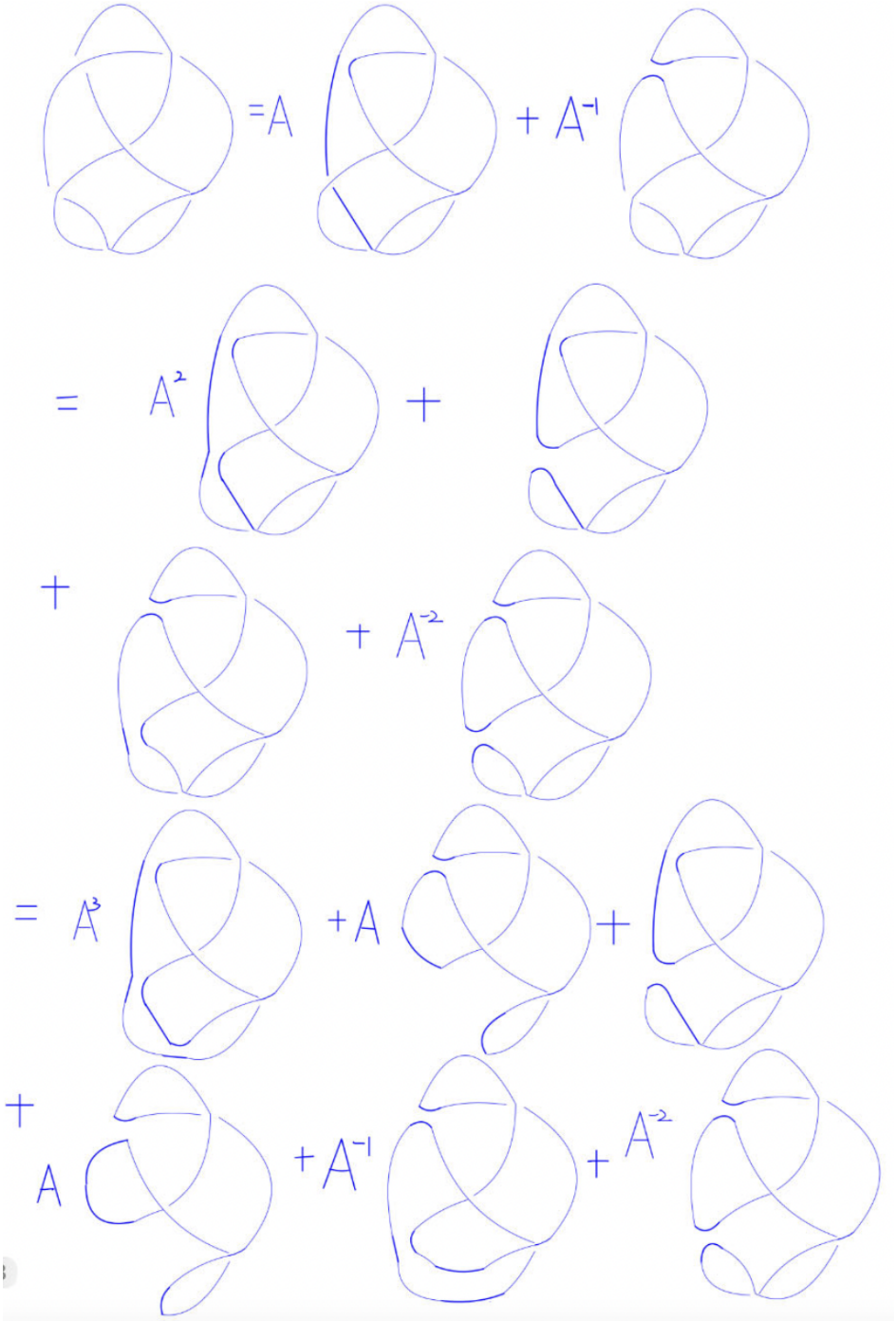
Next, we compute the X polynomial of the knot 6_1.

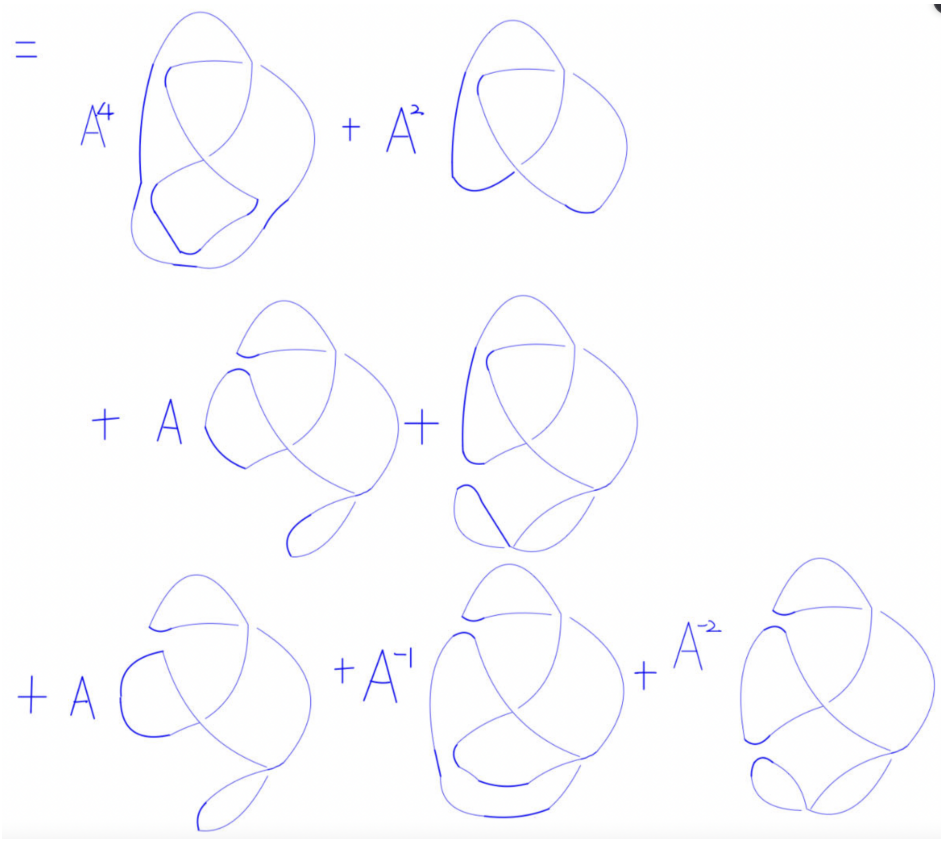
$$\begin{aligned}\left(-A^{-3}\right)^{\mathrm{w(L)}} \quad \langle L\rangle &= \left(-A^{-3}\right)^2 \cdot \left(A^{14} - A^{10} + 2A^6 - 2A^2 - A^{-6} + A^{-2} + A - 10\right)\\ &= A^8 - A^4 + 2A^0 - 2A^{-4} - A^{-12} + A^{-8} + A - 16\end{aligned}$$

We replace A by $t^{-\frac{1}{4}}$ to obtain the Jones Polynomial of the knot 6_1 given below.

$$V_{6_1}(t) = t^{-2} - t^{-1} + 2 - 2 * t + t^2 - t^3 + t^4$$

Example 2.15. *We compute the Jones polynomial of the knot* 6_2.





First, we compute the bracket polynomial of the knot 6_2.

$$\langle L \rangle = A^{10} - A^6 + 2A^2 - 2A^{-2} + 2A^{-8} - 2A^{-10} + A^{-14}$$

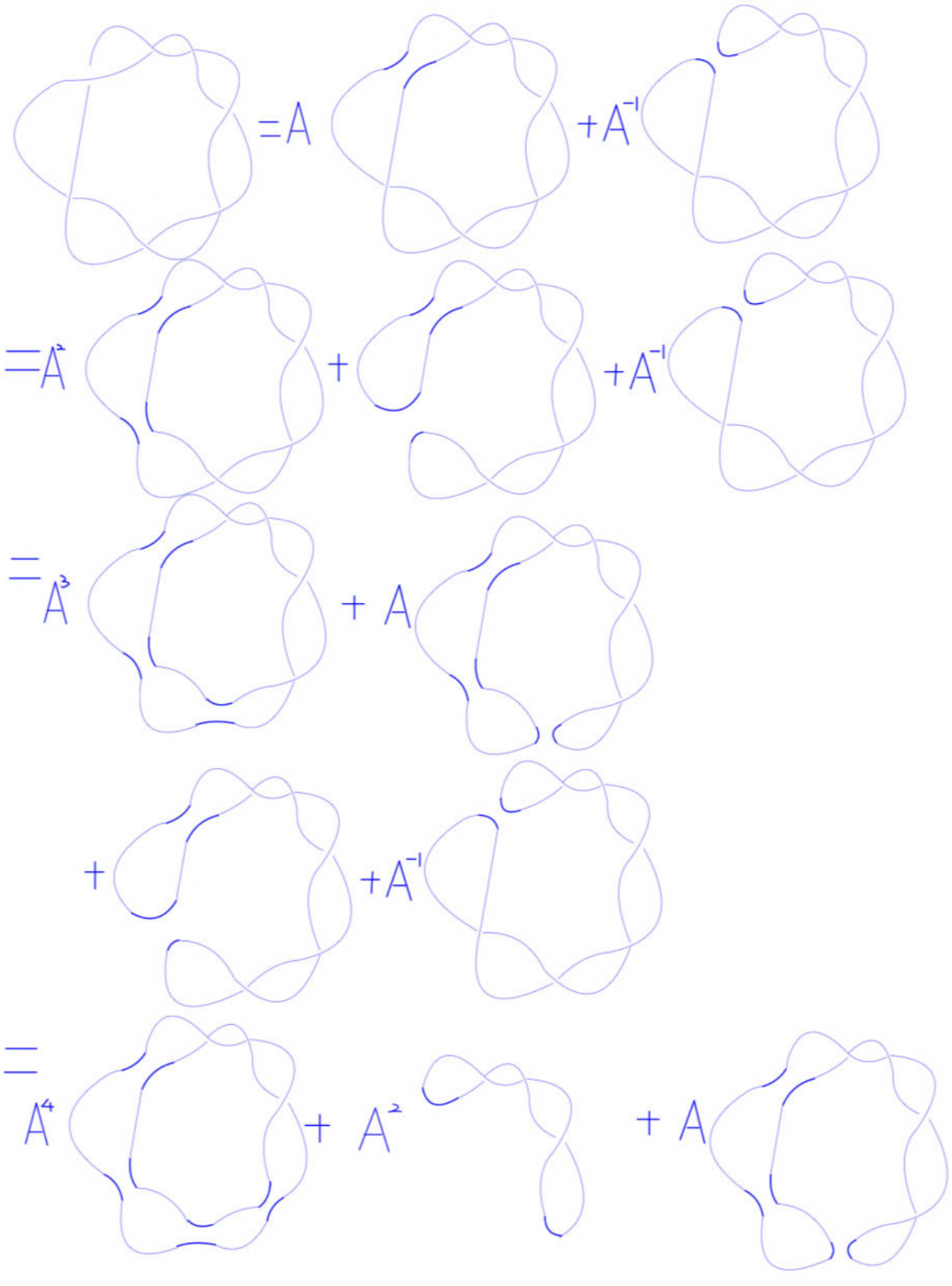
Now we compute the X polynomial of the knot 6_2.

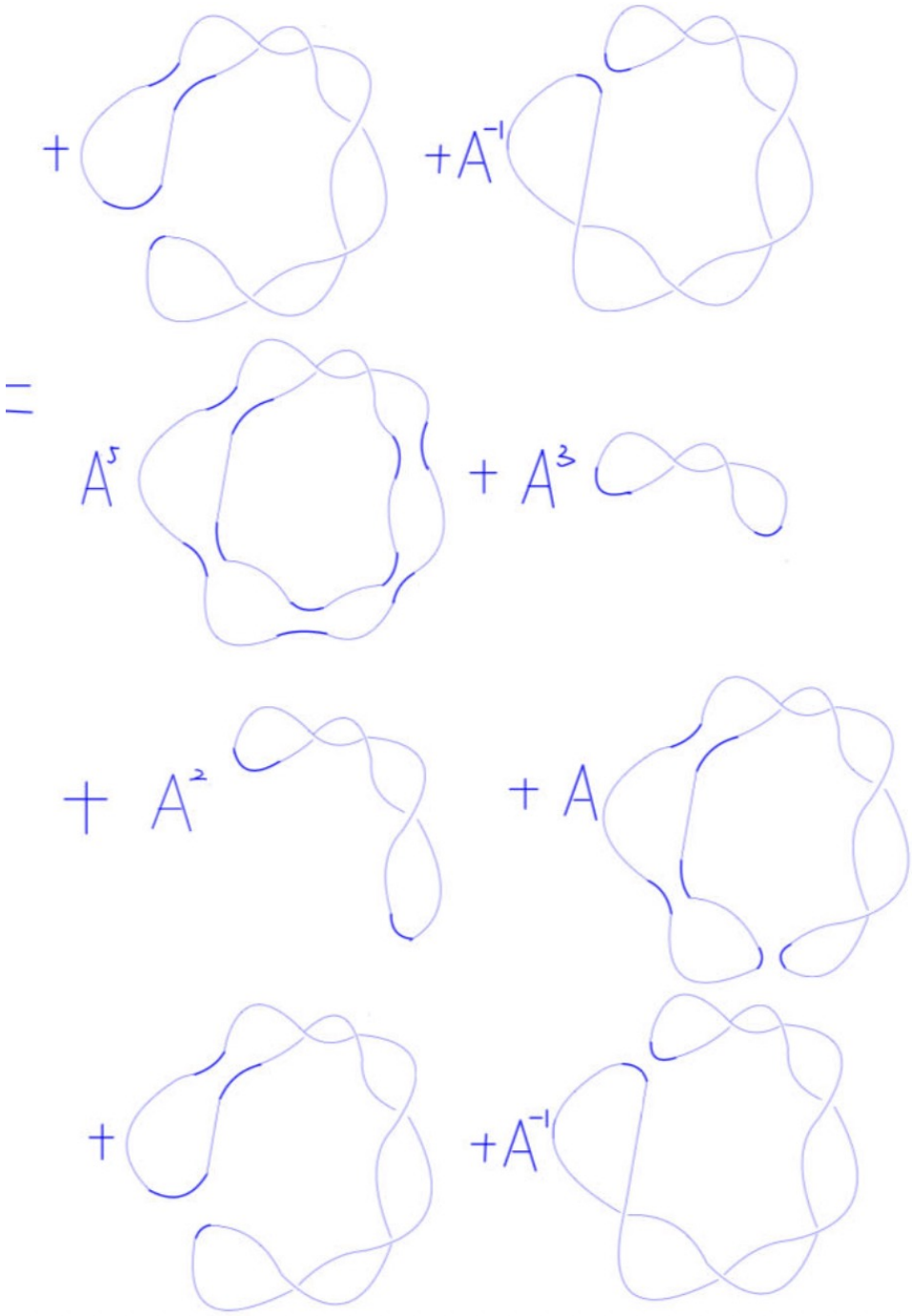
$$\begin{aligned}\left(-A^{-3}\right)^{\mathrm{w(L)}} \langle L \rangle &= \left(-A^{-3}\right)^2 \cdot \left(A^{10} - A^6 + 2A^2 - 2A^{-2} + 2A^{-6} - 2A^{-10} + A^{-14}\right) \\ &= A^4 - 1 + 2A^{-4} - 2A^{-8} + 2A^{-12} - 2A^{-16} + A^{-20}\end{aligned}$$

We replace A by $t^{-\frac{1}{4}}$ to obtain the Jones Polynomial of the knot 6_2 given below.

$$V_{6_2}(t) = t^{-1} - 1 + 2t - 2t^2 + 2t^3 - 2t^4 + t^5$$

Example 2.16. *We compute the Jones polynomial of the knot* 7_1.




+
+A^-1
=
A^5
+ A^3
+ A^2
+ A
+
+A^-1

First, we compute the bracket polynomial of knot 7_1.

$$\begin{aligned}\langle L\rangle &= A^5(-A^4 - A^{-4}) + A^3(-A^{-3})^2 + A^2(-A^{-3})^3 \\ &\quad + A(-A^{-3})^4 + (-A^{-3})^5 + A(-A^{-3})^6 \\ &= -A^9 - A + A^{-3} - A^{-7} + A^{-11} - A^{-15} + A^{-19}\end{aligned}$$

Next, we compute the X polynomial of knot 7_1.

$$\begin{aligned}\left(-A^{-3}\right)^{\mathrm{w(L)}} \quad \langle L\rangle &= \left(-A^{-3}\right)^7 \cdot \left(-A^9 - A + A^{-3} - A^{-7} + A^{-11} - A^{-15} + A^{-19}\right) \\ &= -A^{-12} - A^{-20} + A^{-24} - A^{-28} + A^{-32} - A^{-36} + A^{-40}\end{aligned}$$

We replace A by $t^{-\frac{1}{4}}$ to obtain the Jones Polynomial of the knot 7_1 given below.

$$V_{7_1}(t) = t^3 + t^5 - t^6 + t^7 - t^8 + t^9 - t^{10}$$

3. Kei

Definition 3.1. A *Kei* is a nonempty set X with a binary operation $*$ that satisfies the following three axioms:

(i) *Idempotency:* $x * x = x$ for all $x \in X$

(ii) *Right multiplication is self-inverse:* $(x * y) * y = x$ for all $x, y \in X$

(iii) *Self-distributivity:* $(x * y) * z = (x * z) * (y * z)$ for all $x, y, z \in X$

Idempotency: The first Kei axiom states that for every element x in a set X, applying the operation to x with itself returns x (i.e., $x * x = x$). This property ensures that each element is unchanged when operated on by itself, similar to how an idempotent matrix A satisfies $A^2 = A$.

Self-Inverse: The second Kei axiom indicates that for any elements x and y in X, applying the operation to x and y, followed by applying y again, returns x (i.e., $(x * y) * y = x$). This means that y acts as its own inverse when used in the operation,

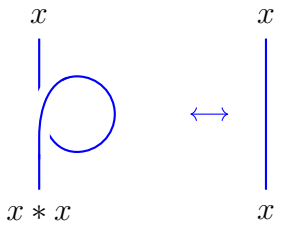


FIGURE 3. The Reidemeister move I correspond to idempotency

analogous to an involution in mathematics, where applying an operation twice undoes the effect.

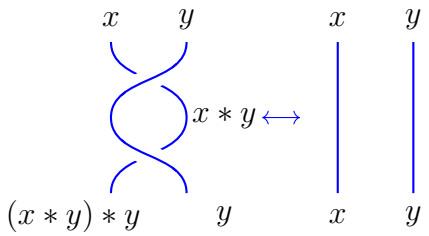


FIGURE 4. The Reidemeister move II correspond to self-inverse

Self-distributivity: The third Kei axiom requires that for all x, y, and z in X, the operation distributes over itself (i.e., $(x * y) * z = (x * z) * (y * z)$). This means the operation is self-distributive, similar to how multiplication distributes over addition.

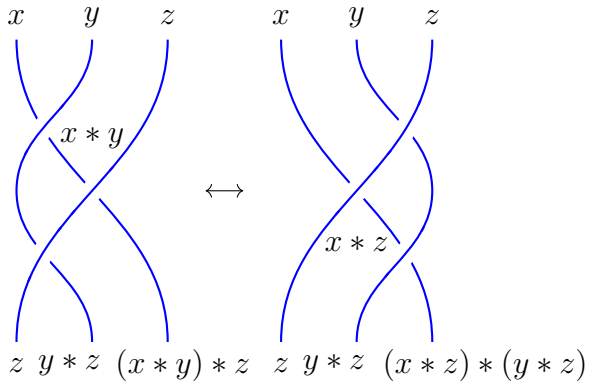


FIGURE 5. The Reidemeister move III correspond to self-distributivity

Example 3.2. *Let $X = \mathbb{Z}$ or $X = \mathbb{Z}_n$, and define the operation $*$ by:*

$$x * y = 2y - x$$

If $X = \mathbb{Z}_n$, then $2y - x$ is computed modulo n. Then, X is a Kei, called the Takasaki Kei or the dihedral Kei, as explained below.

(i) *For all $x \in X$, $x * x = 2x - x = x$.*

(ii) *For all $x, y \in X$, $(x * y) * y = (2y - x) * y = 2y - (2y - x) = 2y - 2y + x = x$.*

(iii) *For all $x, y, z \in X$,*

$$(x * y) * z = 2z - (x * y) = 2z - (2y - x) = 2z - 2y + x$$

while

$$(x*z)*(y*z) = 2(y*z) - (x*z) = 2(2z-y) - (2z-x) = 4z - 2y - 2z + x = 2z - 2y + x.$$

Example 3.3. *Take $X = \mathbb{Z}_3$ and $x * y = 2y - x \pmod 3$. Then the multiplication table of the dihedral Kei $(X, *)$ of order 3 is given by*

$*$	0	1	2
0	0	2	1
1	2	1	0
2	1	0	2

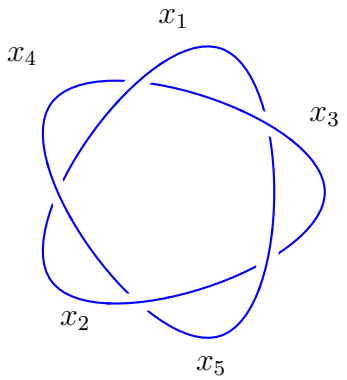
Example 3.4. *Take $X = \mathbb{Z}_4$ and $x * y = 2y - x \pmod 4$. Then the multiplication table of the dihedral Kei $(X, *)$ of order 4 is given by*

$*$	0	1	2	3
0	0	2	0	2
1	3	1	3	1
2	2	0	2	0
3	1	3	1	3

3.1. **Fundamental Kei of a Knot.** The *fundamental kei* of a knot K is an algebraic structure associated with each knot, link, or tangle, described by a set X with a kei operation $*$.

Example 3.5. *We compute the fundamental Kei of the pentafoil knot. This fundamental kei, denoted $K(K)$, is derived from the knot diagram. Let $X = \{x_1, x_2, x_3, x_4, x_5\}$. The fundamental Kei of the pentafoil knot as follows based on teh crossing relations and the three axioms of a Kei.*

$$\mathcal{K}(K) = \{x_1, x_2, x_3, x_4, x_5 \mid x_3 * x_1 = x_4,\ x_1 * x_4 = x_2,\ x_4 * x_2 = x_5,\ x_2 * x_5 = x_3\ x_5 * x_3 = x_1\}.$$



Here is the presentation matrix we get by the fundamental kei and the idempotency:

$*$	x_1	x_2	x_3	x_4	x_5
x_1	x_1	x_3	x_5	x_2	x_4
x_2	x_5	x_2	x_4	x_1	x_3
x_3	x_4	x_1	x_3	x_5	x_2
x_4	x_3	x_5	x_2	x_4	x_1
x_5	x_2	x_4	x_1	x_3	x_5

3.2. **Kei Homomorphism.**

Definition 3.6. A *kei homomorphism* is a function between two keis that preserves the kei structure. More formally, let $(X, *)$ and $(Y, \cdot)$ be two keis. A map $f : X \to Y$

is a kei homomorphism if for all elements $a, b \in X$, the following condition holds:

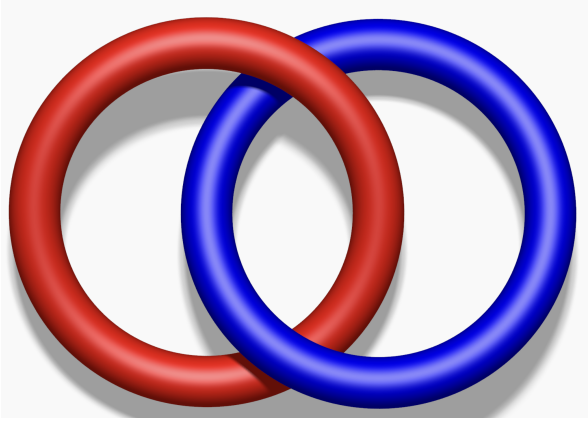
$$f(a * b) = f(a) \cdot f(b)$$

This means that the operation in the kei X is preserved under the map f when applied to the elements in Y.

3.3. **Kei Counting Invariant.**

Definition 3.7. The *kei counting invariant* is an algebraic invariant used in knot theory to distinguish between different knots and links. It is derived by counting the number of homomorphisms from the fundamental kei of a knot (or link) to a finite kei. This number is denoted as $\phi(K, X)$ and provides a way to distinguish between different knots and links. Formally, let K be a knot and X be a finite kei. The kei counting invariant $\phi(K, X)$ is the number of homomorphisms from the fundamental kei $\mathcal{K}(K)$ of the knot K to the kei X.

Example 3.8.



Let us compute the kei counting invariant for the Hopf link with respect to the four element Takasaki kei $\mathbb{Z}_4$. *The crossing relations* R_1 *and* R_2 *are* $x * y = x$ *and* $y * x = y$. *Then we have*

$*$	0	1	2	3
0	0	2	0	2
1	3	1	3	1
2	2	0	2	0
3	1	3	1	3

$f(x)$	$f(y)$	R_1	R_2	$f(x)$	$f(y)$	R_1	R_2
0	0	✓	✓	2	0	✓	✓
0	1			2	1		
0	2	✓	✓	2	2	✓	✓
0	3			2	3	✓	✓
1	0			3	0	✓	✓
1	1	✓	✓	3	1		
1	2			3	2		
1	3	✓	✓	3	3	✓	✓

Thus, we have $|\mathrm{Hom}(\mathcal{K}(K), \mathbb{Z}_4)| = 8$.

4. Quandles

4.1. **Quandle.**

Definition 4.1. *Quandle* is an algebraic structure used in knot theory to study the properties of knots and links. It is a set X equipped with a binary operation $* : X \times X \to X$ that satisfies the following axioms:

(i) *Idempotence:* For all $a \in X$, $a * a = a$.

(ii) *Right Invertibility:* For all $a, b \in X$, the map $\beta_b : X \to X$ defined by $\beta_b(a) = a*b$ is invertible.

(iii) *Self-distributivity:* For all $a, b, c \in X$, $(a * b) * c = (a * c) * (b * c)$.

4.2. **Latin Quandle.**

Definition 4.2. A quandle is called *Latin* if, for every element $a \in X$, the map $\lambda_a : X \to X$ defined by $\lambda_a(b) = a * b$ is a bijection. In other words, a quandle X is *Latin* if the rows and columns of its operation table are permutations.

4.3. **Orbit of a Quandle.**

Definition 4.3. The *orbit* of an element x in a quandle X, denoted by $\mathrm{Orb}(x)$, is the set of elements $y \in X$ such that there exists an inner automorphism $f \in \mathrm{Inn}(X)$ mapping x to y. In other words, the *orbit* of x in X comprises of all elements that can be reached from x by the right multiplication.

4.4. **Dihedral Quandle.**

Definition 4.4. Let $X = \{b, ab, a^2b, \ldots, a^{n-1}b\}$. The set X is the subset of all reflections of the dihedral group D_n of order $2n$. Define the conjugation operation $*$ as follows:

$$x * y = yxy^{-1}$$

where

$$x = a^i b \quad \text{for some} \quad 0 \leq i \leq n-1,$$

$$y = a^j b \quad \text{for some} \quad 0 \leq j \leq n-1.$$

Let's compute $x * y$:

$$x * y = yxy^{-1} = (a^j b)(a^i b)(a^j b)^{-1}$$

$$= (a^j b)(a^i b)(b^{-1}a^{-j})$$

$$= a^j (b a^i) a^{-j}$$

$$= a^j (a^{-i} b) a^{-j}$$

$$= a^{j-i}ba^{-j}$$

$$= a^{j-i}a^{j}b$$

$$= a^{2j-i}b$$

Thus, we have shown that the quandle operation $x * y = yxy^{-1}$ in the set X translates to $x * y = a^{2j-i}b$. By considering the one-to-one correspondence $a^i v \leftrightarrow i$ between the set of reflections of X and $\mathbb{Z}_n$, we can transfer the quandle operation from the set of reflections of X to $\mathbb{Z}_n$ by defining $a * b = 2b - a \mod n$ for $a, b \in \mathbb{Z}_n$ (integers modulo n). The set $\mathbb{Z}_n$ with this quandle structure is called the *dihedral quandle*, denoted by R_n.

4.5. **Alexander Quandle.**

Definition 4.5. An *Alexander quandle* is defined using a module over the ring of Laurent polynomials $\mathbb{Z}[t, t^{-1}]$. Specifically, an Alexander quandle Q is constructed as follows:

(1) **Module Structure**: Consider a module M over the ring $\mathbb{Z}[t, t^{-1}]$.

(2) **Binary Operation**: The quandle operation is defined for elements $x, y \in M$ by:

$$x * y = tx + (1 - t)y$$

where t is a fixed element in $\mathbb{Z}[t, t^{-1}]$.

Example 4.6. *In the Alexander quandle $A = \Lambda_3/(2 + t + t^2)$, we have $2 + t + t^2 = 0$ which implies $t^2 = -2 - t = 1 + 2t$ (since we have $\mathbb{Z}_3$ coefficients). Then the elements of A are $\{0, 1, 2, t, 1 + t, 2 + t, 2t, 1 + 2t, 2 + 2t\}$. The multiplication table of the Alexander*

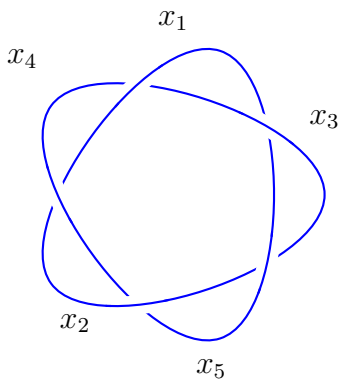
quandle is:

$*$	0	1	2	t	$1+t$	$2+t$	$2t$	$1+2t$	$2+2t$
0	0	$1+2t$	$2+t$	$2+2t$	$2t$	1	$1+t$	2	$2t$
1	t	1	$2+2t$	2	0	$1+t$	$2+t$	$1+2t$	0
2	$2t$	$1+t$	2	$2+t$	t	$1+2t$	1	$2+2t$	t
t	$1+2t$	$2+t$	0	t	$1+2t$	$2+2t$	2	$2t$	$1+t$
$1+t$	1	$2+2t$	t	$2t$	$1+t$	2	$2+t$	0	$1+2t$
$2+t$	$1+t$	2	$2t$	0	1	$2+t$	$2+2t$	t	1
$2t$	$2+t$	t	$1+2t$	1	2	t	$2t$	$1+2t$	$2+t$
$1+2t$	$2+2t$	$2t$	1	$1+t$	$2+t$	$2t$	0	1	$2+2t$
$2+2t$	2	0	$1+t$	$1+2t$	$2+2t$	0	t	$1+t$	2

4.6. **Alexander Polynomial.**

Definition 4.7. The *Alexander Polynomial* is a knot invariant. This is a Laurent polynomial which means the variable t can have negative powers. The way to compute the Alexander polynomial is to take the determinant of an $(n-1)\times(n-1)$ minor of the presentation matrix A. After we normalize it by getting rid of the negative power and make the constant term positive, we will get our *normalized polynomial*.

Example 4.8. *We first compute the Alexander polynomial of the Pentafoil Knot.*



We derive the following equations based on the crossing relations:

$$t^{-1}x_3 + (1-t^{-1})x_1 = x_4$$

$$t^{-1}x_1 + (1-t^{-1})x_4 = x_2$$

$$t^{-1}x_4 + (1-t^{-1})x_2 = x_5$$

$$t^{-1}x_2 + (1-t^{-1})x_5 = x_3$$

$$t^{-1}x_5 + (1-t^{-1})x_3 = x_1$$

We form the presentation matrix based on the equations above.

$$A = \begin{pmatrix} (1-t^{-1}) & 0 & t^{-1} & -1 & 0 \\ t^{-1} & -1 & 0 & (1-t^{-1}) & 0 \\ 0 & (1-t^{-1}) & 0 & t^{-1} & -1 \\ 0 & t^{-1} & -1 & 0 & (1-t^{-1}) \\ -1 & 0 & (1-t^{-1}) & 0 & t^{-1} \end{pmatrix}$$

The 4×4 *minor of* A *is:*

$$\begin{pmatrix} (1-t^{-1}) & 0 & t^{-1} & -1 \\ t^{-1} & -1 & 0 & (1-t^{-1}) \\ 0 & (1-t^{-1}) & 0 & t^{-1} \\ 0 & t^{-1} & -1 & 0 \end{pmatrix}$$

The determinant of the minor of A is given by

$$(1-t^{-1})\cdot\begin{vmatrix} -1 & 0 & (1-t^{-1}) \\ (1-t^{-1}) & 0 & t^{-1} \\ t^{-1} & -1 & 0 \end{vmatrix} + 0\cdot\begin{vmatrix} t^{-1} & 0 & (1-t^{-1}) \\ 0 & 0 & t^{-1} \\ 0 & -1 & 0 \end{vmatrix}$$

$$+ t^{-1}\cdot\begin{vmatrix} t^{-1} & -1 & (1-t^{-1}) \\ 0 & (1-t^{-1}) & t^{-1} \\ 0 & t^{-1} & 0 \end{vmatrix} - (-1)\cdot\begin{vmatrix} t^{-1} & -1 & 0 \\ 0 & (1-t^{-1}) & 0 \\ 0 & t^{-1} & -1 \end{vmatrix}$$

$$= (1-t^{-1})(-1) + t^{-1}(-t^{-3}) - (-1)(-t^{-1}+t^{-2})$$

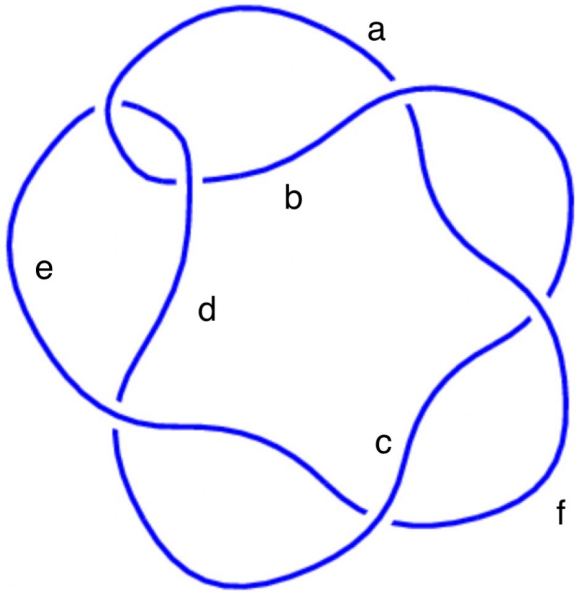
$$= (1-t^{-1})(-1) + t^{-1}(-t^{-3}) - (t^{-1}-t^{-2})$$

$$= -1 + t^{-1} - t^{-1}\cdot t^{-3} - t^{-1} + t^{-2}$$

Multiply by $-t^4$ to obtain the Alexander polynomial:

$$1 - t + t^2 - t^3 + t^4$$

Example 4.9.



We derive the following equations based on the crossing relations:

$$t^{-1}a + (1 - t^{-1})d = b$$

$$tb + (1 - t)f = c$$

$$tc + (1 - t)e = d$$

$$t^{-1}d + (1 - t^{-1})a = e$$

$$te + (1 - t)c = f$$

$$tf + (1 - t)b = a$$

$$A = \begin{pmatrix} t^{-1} & -1 & 0 & (1 - t^{-1}) & 0 & 0 \\ 0 & t & -1 & 0 & 0 & (1 - t) \\ 0 & 0 & t & -1 & (1 - t) & 0 \\ (1 - t^{-1}) & 0 & 0 & t^{-1} & -1 & 0 \\ 0 & 0 & 1 - t & 0 & t & -1 \\ -1 & 1 - t & 0 & 0 & 0 & t \end{pmatrix}$$

The 5×5 *minor of* A *is:*

$$\begin{pmatrix} t^{-1} & -1 & 0 & 1 - t^{-1} & 0 \\ 0 & t & -1 & 0 & 0 \\ 0 & 0 & t & -1 & 1 - t \\ 1 - t^{-1} & 0 & 0 & t^{-1} & -1 \\ 0 & 0 & 1 - t & 0 & t \end{pmatrix}$$

The determinant of the minor of A is given by

$$= t^{-1}\begin{vmatrix} t & -1 & 0 & 0 \\ 0 & t & -1 & 1-t \\ 0 & 0 & t^{-1} & -1 \\ 0 & 1-t & 0 & t \end{vmatrix} - (-1)\begin{vmatrix} 0 & -1 & 0 & 0 \\ 0 & t & -1 & 1-t \\ 1-t^{-1} & 0 & t^{-1} & -1 \\ 0 & 1-t & 0 & t \end{vmatrix}$$

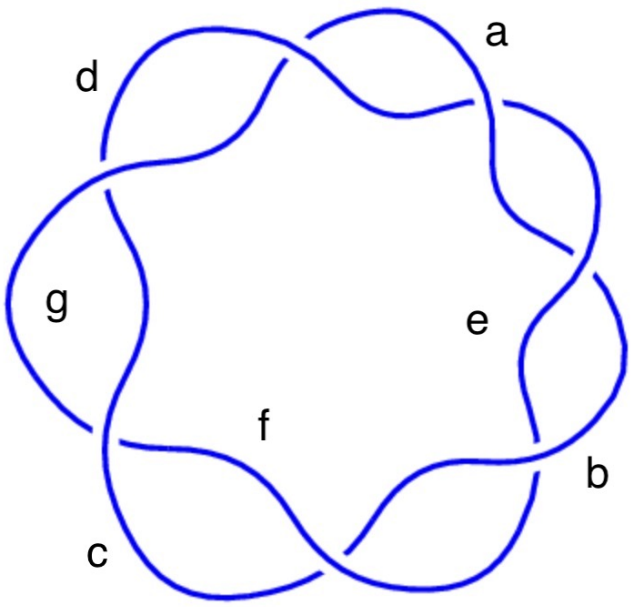
$$+ 0 - (1-t^{-1})\begin{vmatrix} 0 & t & -1 & 0 \\ 0 & 0 & t & 1-t \\ 1-t^{-1} & 0 & t^{-1} & -1 \\ 0 & 0 & 0 & t \end{vmatrix} + 0$$

$$= -2t^2 + 5t - 2$$

Multiply by -1 to obtain the Alexander polynomial:

$$2t^2 - 5t + 2$$

Example 4.10.



We derive the following equations based on the crossing relations:

$$ta + (1-t)e = b$$

$$tb + (1-t)f = c$$

$$tc + (1-t)g = d$$

$$td + (1-t)a = e$$

$$te + (1-t)b = f$$

$$tf + (1-t)c = g$$

$$tg + (1-t)d = a$$

We form the presentation matrix based on the equations above.

$$A = \begin{pmatrix} t & -1 & 0 & 0 & (1-t) & 0 & 0 \\ 0 & t & -1 & 0 & 0 & (1-t) & 0 \\ 0 & 0 & t & -1 & 0 & 0 & (1-t) \\ (1-t) & 0 & 0 & t & -1 & 0 & 0 \\ 0 & (1-t) & 0 & 0 & t & -1 & 0 \\ 0 & 0 & (1-t) & 0 & 0 & t & -1 \\ -1 & 0 & 0 & (1-t) & 0 & 0 & t \end{pmatrix}$$

The 6×6 *minor of* A *is:*

$$\begin{pmatrix} t & -1 & 0 & 0 & (1-t) & 0 \\ 0 & t & -1 & 0 & 0 & (1-t) \\ 0 & 0 & t & -1 & 0 & 0 \\ (1-t) & 0 & 0 & t & -1 & 0 \\ 0 & (1-t) & 0 & 0 & t & -1 \\ 0 & 0 & (1-t) & 0 & 0 & t \end{pmatrix}$$

The determinant of the minor of A is given by

$$t^6 - t^5 + t^4 - t^3 + t^2 - t + 1,$$

which is the Alexander Polynomial of the knot 7_1.

4.7. **Quandle polynomial.**

Definition 4.11. Let X be a finite quandle. For elements $x, y \in X$, let

$$r(x) = |\{y \in X \mid x * y = x\}|$$

and

$$c(x) = |\{y \in X \mid y * x = y\}|$$

For any element $x \in X$, we have a pair $(r(x), c(y))$ of integers. We now define a two-variable polynomial $P(X)$ is defined as:

$$P(X) = \sum_{x,y \in X} t^{r(x)} s^{c(y)}$$

The polynomial $P(X)$ is called the *quandle polynomial* of the quandle X.

Example 4.12. *Let X be the quandle of order 4 whose multiplication table is given by*

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

Calculations for $r(x)$ and $c(x)$ are given by

$$r(1) = 4 \quad c(1) = 2$$

$$r(2) = 2 \quad c(2) = 4$$

$$r(3) = 2 \quad c(3) = 4$$

$$r(4) = 4 \quad c(4) = 2$$

The quandle polynomial is

$$P(X) = 2t^4s^2 + 2t^2s^4$$

Example 4.13. *The following table contains quandle polynomials of all quandles of order 4 and 5:*

Quandle	*Quandle Polynomial*
$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 \\ 3 & 3 & 3 & 3 \\ 4 & 4 & 4 & 4 \end{pmatrix}$	$P(X) = 4t^4 * s^4$
$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 3 \\ 3 & 3 & 3 & 2 \\ 4 & 4 & 4 & 4 \end{pmatrix}$	$P(X) = t^4 * s^4 + 2t^3 * s^4 + t^4 * s^2$

$\begin{pmatrix} 1 & 1 & 1 & 2 \\ 2 & 2 & 2 & 3 \\ 3 & 3 & 3 & 1 \\ 4 & 4 & 4 & 4 \end{pmatrix}$	$P(X) = 3t^3 * s^4 + t^4 * s^1$
$\begin{pmatrix} 1 & 1 & 2 & 2 \\ 2 & 2 & 1 & 1 \\ 3 & 3 & 3 & 3 \\ 4 & 4 & 4 & 4 \end{pmatrix}$	$P(X) = 2t^2 * s^4 + 2t^4 * s^2$
$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 2 & 4 & 3 \\ 3 & 4 & 3 & 2 \\ 4 & 3 & 2 & 4 \end{pmatrix}$	$P(X) = t^4 * s^4 + 3t^2 * s^2$
$\begin{pmatrix} 1 & 1 & 2 & 2 \\ 2 & 2 & 1 & 1 \\ 4 & 4 & 3 & 3 \\ 3 & 3 & 4 & 4 \end{pmatrix}$	$P(X) = 4t^2 * s^2$

$\begin{pmatrix} 1 & 4 & 2 & 3 \\ 3 & 2 & 4 & 1 \\ 4 & 1 & 3 & 2 \\ 2 & 3 & 1 & 4 \end{pmatrix}$	$P(X) = 4t * s$
$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 & 2 \\ 3 & 3 & 3 & 3 & 3 \\ 4 & 4 & 4 & 4 & 4 \\ 5 & 5 & 5 & 5 & 5 \end{pmatrix}$	$P(X) = 5 * t^5 * s^5$
$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 & 3 \\ 3 & 3 & 3 & 3 & 4 \\ 4 & 4 & 4 & 4 & 2 \\ 5 & 5 & 5 & 5 & 5 \end{pmatrix}$	$P(X) = t^5 * s^5 + 3t^4 * s^5 + t^5 * s^2$
$\begin{pmatrix} 1 & 1 & 1 & 1 & 2 \\ 2 & 2 & 2 & 2 & 3 \\ 3 & 3 & 3 & 3 & 4 \\ 4 & 4 & 4 & 4 & 1 \\ 5 & 5 & 5 & 5 & 5 \end{pmatrix}$	$P(X) = 2t^4 * s^5 + t^3 * s^5 + t^4 * s^4 + t^5 * s^1$

$\begin{pmatrix} 1 & 1 & 1 & 2 & 2 \\ 2 & 2 & 2 & 3 & 3 \\ 3 & 3 & 3 & 1 & 1 \\ 4 & 4 & 4 & 4 & 4 \\ 5 & 5 & 5 & 5 & 5 \end{pmatrix}$	$P(X) = 3t^3 * s^5 + 2t^5 * s^2$
$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 & 2 \\ 3 & 3 & 3 & 5 & 4 \\ 4 & 4 & 5 & 4 & 3 \\ 5 & 5 & 4 & 3 & 5 \end{pmatrix}$	$P(X) = 2t^5 * s^5 + 3t^3 * s^3$
$\begin{pmatrix} 1 & 1 & 2 & 2 & 2 \\ 2 & 2 & 1 & 1 & 1 \\ 3 & 3 & 3 & 3 & 3 \\ 4 & 4 & 4 & 4 & 4 \\ 5 & 5 & 5 & 5 & 5 \end{pmatrix}$	$P(X) = 2t^2 * s^5 + 3t^5 * s^3$

$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 & 2 \\ 3 & 3 & 3 & 3 & 4 \\ 4 & 4 & 4 & 4 & 3 \\ 5 & 5 & 5 & 5 & 5 \end{pmatrix}$	$P(X) = 2t^5 * s^5 + 2t^4 * s^5 + t^5 * s^3$
$\begin{pmatrix} 1 & 1 & 1 & 1 & 2 \\ 2 & 2 & 2 & 2 & 1 \\ 3 & 3 & 3 & 3 & 4 \\ 4 & 4 & 4 & 4 & 3 \\ 5 & 5 & 5 & 5 & 5 \end{pmatrix}$	$P(X) = 4t^4 * s^5 + t^5 * s$
$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 3 & 3 \\ 3 & 3 & 3 & 2 & 2 \\ 4 & 4 & 4 & 4 & 4 \\ 5 & 5 & 5 & 5 & 5 \end{pmatrix}$	$P(X) = t^5 * s^5 + 2t^3 * s^5 + 2t^5 * s^3$

$\begin{pmatrix} 1 & 1 & 1 & 2 & 3 \\ 2 & 2 & 2 & 3 & 1 \\ 3 & 3 & 3 & 1 & 2 \\ 4 & 4 & 4 & 4 & 4 \\ 5 & 5 & 5 & 5 & 5 \end{pmatrix}$	$P(X) = 4t^4 * s^5 + t^5 * s$
$\begin{pmatrix} 1 & 1 & 1 & 2 & 2 \\ 2 & 2 & 2 & 1 & 1 \\ 3 & 3 & 3 & 3 & 3 \\ 4 & 4 & 5 & 4 & 4 \\ 5 & 5 & 4 & 5 & 5 \end{pmatrix}$	$P(X) = 2t^3 * s^5 + t^5 * s^3 + 2t^4 * s^3$
$\begin{pmatrix} 1 & 1 & 2 & 2 & 2 \\ 2 & 2 & 1 & 1 & 1 \\ 3 & 3 & 3 & 3 & 4 \\ 4 & 4 & 4 & 4 & 3 \\ 5 & 5 & 5 & 5 & 5 \end{pmatrix}$	$P(X) = 2t^2 * s^5 + 2t^4 * s^3 + t^5 * s$

$\begin{pmatrix} 1 & 1 & 2 & 2 & 2 \\ 2 & 2 & 1 & 1 & 1 \\ 3 & 3 & 3 & 5 & 4 \\ 4 & 4 & 5 & 4 & 3 \\ 5 & 5 & 4 & 3 & 5 \end{pmatrix}$	$P(X) = 2t^2 * s^5 + 3t^3 * s$
$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 5 & 3 & 4 \\ 3 & 4 & 3 & 5 & 2 \\ 4 & 5 & 2 & 4 & 3 \\ 5 & 3 & 4 & 2 & 5 \end{pmatrix}$	$P(X) = t^5 * s^5 + 4t^2 * s^2$
$\begin{pmatrix} 1 & 1 & 1 & 2 & 2 \\ 2 & 2 & 2 & 3 & 3 \\ 3 & 3 & 3 & 1 & 1 \\ 5 & 5 & 5 & 4 & 4 \\ 4 & 4 & 4 & 5 & 5 \end{pmatrix}$	$P(X) = 3t^3 * s^3 + 2t^2 * s^2$

$\begin{pmatrix} 1 & 1 & 2 & 2 & 2 \\ 2 & 2 & 1 & 1 & 1 \\ 4 & 5 & 3 & 5 & 4 \\ 5 & 3 & 5 & 4 & 3 \\ 3 & 4 & 4 & 3 & 5 \end{pmatrix}$	$P(X) = 2t^2 * s^2 + 3t * s$
$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 3 & 3 \\ 3 & 3 & 3 & 2 & 2 \\ 4 & 5 & 5 & 4 & 4 \\ 5 & 4 & 4 & 5 & 5 \end{pmatrix}$	$P(X) = t^5 * s^5 + 4t^3 * s^3$
$\begin{pmatrix} 1 & 1 & 2 & 2 & 2 \\ 2 & 2 & 1 & 1 & 1 \\ 3 & 3 & 3 & 3 & 3 \\ 5 & 5 & 5 & 4 & 4 \\ 4 & 4 & 4 & 5 & 5 \end{pmatrix}$	$P(X) = 4t^2 * s^3 + t^5 * s$

$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 3 & 3 \\ 3 & 3 & 3 & 2 & 2 \\ 5 & 5 & 5 & 4 & 4 \\ 4 & 4 & 4 & 5 & 5 \end{pmatrix}$	$P(X) = t^5 * s^3 + 2t^3 * s^3 + 2t^2 * s^3$
$\begin{pmatrix} 1 & 3 & 4 & 5 & 2 \\ 3 & 2 & 5 & 1 & 4 \\ 4 & 5 & 3 & 2 & 1 \\ 5 & 1 & 2 & 4 & 3 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix}$	$P(X) = 5t * s$
$\begin{pmatrix} 1 & 4 & 5 & 3 & 2 \\ 3 & 2 & 4 & 5 & 1 \\ 2 & 5 & 3 & 1 & 4 \\ 5 & 1 & 2 & 4 & 3 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix}$	$P(X) = 5t * s$

$\begin{pmatrix} 1 & 4 & 5 & 2 & 3 \\ 3 & 2 & 1 & 5 & 4 \\ 4 & 5 & 3 & 1 & 2 \\ 5 & 3 & 2 & 4 & 1 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix}$	$P(X) = 5t * s$

5. The Meeting Point of Quandles and Groups

5.1. **The Groups Generated by the Columns of Quandles.** The group generated by the columns of a quandle refers to the subgroup of the **symmetric group** (or, more generally, the **automorphism group**) that is generated by the permutations induced by the columns of the quandle operation table.

(1) **Columns as Permutations:**

Let Q be a quandle with a binary operation $*$ satisfying:

- Idempotency: $x * x = x$ for all $x \in Q$.
- Right-invertibility: For each $a \in Q$, the map $f_a : Q \to Q$ defined by $f_a(x) = x * a$ is bijective.
- Self-distributivity: $(x * y) * z = (x * z) * (y * z)$ for all $x, y, z \in Q$.

Each element $a \in Q$ induces a permutation f_a, where the columns of the quandle operation table correspond to these permutations.

(2) **Group Generated by Columns:**

Consider the set of permutations $\{f_a \mid a \in Q\}$, which act on Q. The group generated by these permutations is the subgroup of the symmetric group S_Q given by:

$$G = \langle f_a \mid a \in Q \rangle \subseteq S_Q.$$

(3) **Connection to the Inner Automorphism Group:**

If the quandle is a **rack** (i.e., every right multiplication f_a is bijective), then these permutations naturally form a subgroup of $\mathrm{Sym}(Q)$. This subgroup is often called the **inner automorphism group**, denoted as:

$$\mathrm{Inn}(Q) = \langle f_a \mid a \in Q \rangle.$$

Example 5.1. *The following table contains the cycle structure of column permutation, inner automorphism group $Inn(Q)$ and automorphism group $Aut(Q)$ of all quandles of order 3, 4, and 5. We denote the dihedral group of order $2n$ by D_n.*

Quandle	*Column cycles*	*Inn(Q)*	*Aut(Q)*
$\begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 3 & 3 & 3 \end{pmatrix}$	$\{(1)\}$	$\{(1)\}$	S_3
$\begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \\ 2 & 1 & 3 \end{pmatrix}$	$\{(2\ 3), (1\ 3), (1\ 2)\}$	S_3	S_3

$\begin{pmatrix} 1 & 1 & 1 \\ 3 & 2 & 2 \\ 2 & 3 & 3 \end{pmatrix}$	$\{(1), (2\ 3)\}$	$\mathbb{Z}_2$	$\mathbb{Z}_2$
$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 \\ 3 & 3 & 3 & 3 \\ 4 & 4 & 4 & 4 \end{pmatrix}$	$\{(1)\}$	$\{(1)\}$	S_4
$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 3 \\ 3 & 3 & 3 & 2 \\ 4 & 4 & 4 & 4 \end{pmatrix}$	$\{(1), (2\ 3)\}$	$\mathbb{Z}_2$	$\mathbb{Z}_2$
$\begin{pmatrix} 1 & 1 & 1 & 2 \\ 2 & 2 & 2 & 3 \\ 3 & 3 & 3 & 1 \\ 4 & 4 & 4 & 4 \end{pmatrix}$	$\{(1), (2\ 3\ 1)\}$	$\mathbb{Z}_3$	$\mathbb{Z}_3$
$\begin{pmatrix} 1 & 1 & 2 & 2 \\ 2 & 2 & 1 & 1 \\ 3 & 3 & 3 & 3 \\ 4 & 4 & 4 & 4 \end{pmatrix}$	$\{(1), (1\ 2)\}$	$\mathbb{Z}_2$	$\mathbb{Z}_2 \bigoplus \mathbb{Z}_2$

$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 2 & 4 & 3 \\ 3 & 4 & 3 & 2 \\ 4 & 3 & 2 & 4 \end{pmatrix}$	$\{(1), (3\ 4), (2\ 4), (2\ 3)\}$	S_3	S_3
$\begin{pmatrix} 1 & 1 & 2 & 2 \\ 2 & 2 & 1 & 1 \\ 4 & 4 & 3 & 3 \\ 3 & 3 & 4 & 4 \end{pmatrix}$	$\{(1\ 2), (3\ 4)\}$	$\mathbb{Z}_2 \bigoplus \mathbb{Z}_2$	D_4
$\begin{pmatrix} 1 & 4 & 2 & 3 \\ 3 & 2 & 4 & 1 \\ 4 & 1 & 3 & 2 \\ 2 & 3 & 1 & 4 \end{pmatrix}$	$\{(2\ 3\ 4), (1\ 4\ 3), (1\ 2\ 4), (1\ 3\ 2)\}$	A_4	A_4
$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 & 2 \\ 3 & 3 & 3 & 3 & 3 \\ 4 & 4 & 4 & 4 & 4 \\ 5 & 5 & 5 & 5 & 5 \end{pmatrix}$	$\{(1)\}$	$\{(1)\}$	S_5

$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 & 3 \\ 3 & 3 & 3 & 3 & 4 \\ 4 & 4 & 4 & 4 & 2 \\ 5 & 5 & 5 & 5 & 5 \end{pmatrix}$	$\{(1), (2\ 3\ 4)\}$	$\mathbb{Z}_3$	$\mathbb{Z}_3$
$\begin{pmatrix} 1 & 1 & 1 & 1 & 2 \\ 2 & 2 & 2 & 2 & 3 \\ 3 & 3 & 3 & 3 & 4 \\ 4 & 4 & 4 & 4 & 1 \\ 5 & 5 & 5 & 5 & 5 \end{pmatrix}$	$\{(1), (1\ 2\ 3\ 4)\}$	$\mathbb{Z}_4$	$\mathbb{Z}_4$
$\begin{pmatrix} 1 & 1 & 1 & 2 & 2 \\ 2 & 2 & 2 & 3 & 3 \\ 3 & 3 & 3 & 1 & 1 \\ 4 & 4 & 4 & 4 & 4 \\ 5 & 5 & 5 & 5 & 5 \end{pmatrix}$	$\{(1), (1\ 2\ 3)\}$	$\mathbb{Z}_3$	$\mathbb{Z}_3 \bigoplus \mathbb{Z}_2$

$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 & 2 \\ 3 & 3 & 3 & 5 & 4 \\ 4 & 4 & 5 & 4 & 3 \\ 5 & 5 & 4 & 3 & 5 \end{pmatrix}$	$\{(1), (4\ 5), (3\ 5), (3\ 4)\}$	D_3	D_6
$\begin{pmatrix} 1 & 1 & 2 & 2 & 2 \\ 2 & 2 & 1 & 1 & 1 \\ 3 & 3 & 3 & 3 & 3 \\ 4 & 4 & 4 & 4 & 4 \\ 5 & 5 & 5 & 5 & 5 \end{pmatrix}$	$\{(1), (1\ 2)\}$	$\mathbb{Z}_2$	D_6
$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 & 2 \\ 3 & 3 & 3 & 3 & 4 \\ 4 & 4 & 4 & 4 & 3 \\ 5 & 5 & 5 & 5 & 5 \end{pmatrix}$	$\{(1), (3\ 4)\}$	$\mathbb{Z}_2$	$\mathbb{Z}_2 \bigoplus \mathbb{Z}_2$

$\begin{pmatrix} 1 & 1 & 1 & 1 & 2 \\ 2 & 2 & 2 & 2 & 1 \\ 3 & 3 & 3 & 3 & 4 \\ 4 & 4 & 4 & 4 & 3 \\ 5 & 5 & 5 & 5 & 5 \end{pmatrix}$	$\{(1), (1\ 2)(3\ 4)\}$	$\mathbb{Z}_2$	D_4
$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 3 & 3 \\ 3 & 3 & 3 & 2 & 2 \\ 4 & 4 & 4 & 4 & 4 \\ 5 & 5 & 5 & 5 & 5 \end{pmatrix}$	$\{(1), (2\ 3)\}$	$\mathbb{Z}_2$	$\mathbb{Z}_2 \bigoplus \mathbb{Z}_2$
$\begin{pmatrix} 1 & 1 & 1 & 2 & 3 \\ 2 & 2 & 2 & 3 & 1 \\ 3 & 3 & 3 & 1 & 2 \\ 4 & 4 & 4 & 4 & 4 \\ 5 & 5 & 5 & 5 & 5 \end{pmatrix}$	$\{(1), (1\ 2\ 3),$ $(1\ 3\ 2)\}$	$\mathbb{Z}_3$	D_3

$\begin{pmatrix} 1 & 1 & 1 & 2 & 2 \\ 2 & 2 & 2 & 1 & 1 \\ 3 & 3 & 3 & 3 & 3 \\ 4 & 4 & 5 & 4 & 4 \\ 5 & 5 & 4 & 5 & 5 \end{pmatrix}$	$\{(1), (4\ 5), (1\ 2)\}$	$\mathbb{Z}_2 \bigoplus \mathbb{Z}_2$	$\mathbb{Z}_2 \bigoplus \mathbb{Z}_2$
$\begin{pmatrix} 1 & 1 & 2 & 2 & 2 \\ 2 & 2 & 1 & 1 & 1 \\ 3 & 3 & 3 & 3 & 4 \\ 4 & 4 & 4 & 4 & 3 \\ 5 & 5 & 5 & 5 & 5 \end{pmatrix}$	$\{(1), (1\ 2), (1\ 2)(3\ 4)\}$	$\mathbb{Z}_2 \bigoplus \mathbb{Z}_2$	$\mathbb{Z}_2 \bigoplus \mathbb{Z}_2$
$\begin{pmatrix} 1 & 1 & 2 & 2 & 2 \\ 2 & 2 & 1 & 1 & 1 \\ 3 & 3 & 3 & 5 & 4 \\ 4 & 4 & 5 & 4 & 3 \\ 5 & 5 & 4 & 3 & 5 \end{pmatrix}$	$\{(1), (1\ 2), (1\ 2)(3\ 4)\}$	$\mathbb{Z}_2 \bigoplus \mathbb{Z}_2$	D_6

$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 5 & 3 & 4 \\ 3 & 4 & 3 & 5 & 2 \\ 4 & 5 & 2 & 4 & 3 \\ 5 & 3 & 4 & 2 & 5 \end{pmatrix}$	$\{(1), (3\ 4\ 5), (2\ 5\ 4), (2\ 3\ 5), (2\ 4\ 3)\}$	A_4	A_4
$\begin{pmatrix} 1 & 1 & 1 & 2 & 2 \\ 2 & 2 & 2 & 3 & 3 \\ 3 & 3 & 3 & 1 & 1 \\ 5 & 5 & 5 & 4 & 4 \\ 4 & 4 & 4 & 5 & 5 \end{pmatrix}$	$\{(1), (4\ 5), (1\ 2\ 3)\}$	Z_6	Z_6
$\begin{pmatrix} 1 & 1 & 2 & 2 & 2 \\ 2 & 2 & 1 & 1 & 1 \\ 4 & 5 & 3 & 5 & 4 \\ 5 & 3 & 5 & 4 & 3 \\ 3 & 4 & 4 & 3 & 5 \end{pmatrix}$	$\{(1), (3\ 4\ 5), (3\ 5\ 4), (1\ 2)(4\ 5), (1\ 2)(3\ 5), (1\ 2)(3\ 4)\}$	D_3	D_3

$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 3 & 3 \\ 3 & 3 & 3 & 2 & 2 \\ 4 & 5 & 5 & 4 & 4 \\ 5 & 4 & 4 & 5 & 5 \end{pmatrix}$	$\{(1), (4\ 5), (2\ 3)\}$	$\mathbb{Z}_2 \bigoplus \mathbb{Z}_2$	D_4
$\begin{pmatrix} 1 & 1 & 2 & 2 & 2 \\ 2 & 2 & 1 & 1 & 1 \\ 3 & 3 & 3 & 3 & 3 \\ 5 & 5 & 5 & 4 & 4 \\ 4 & 4 & 4 & 5 & 5 \end{pmatrix}$	$\{(1), (1\ 2), (4\ 5)\}$	$\mathbb{Z}_2 \bigoplus \mathbb{Z}_2$	D_4
$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 3 & 3 \\ 3 & 3 & 3 & 2 & 2 \\ 5 & 5 & 5 & 4 & 4 \\ 4 & 4 & 4 & 5 & 5 \end{pmatrix}$	$\{(1), (2\ 3), (4\ 5)\}$	$\mathbb{Z}_2 \bigoplus \mathbb{Z}_2$	$\mathbb{Z}_2 \bigoplus \mathbb{Z}_2$

$\begin{pmatrix} 1 & 3 & 4 & 5 & 2 \\ 3 & 2 & 5 & 1 & 4 \\ 4 & 5 & 3 & 2 & 1 \\ 5 & 1 & 2 & 4 & 3 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix}$	{(2 3 4 5), (1 3 5 4), (1 4 2 5), (1 5 3 2), (1 2 4 3)}	D_{10}	D_{10}
$\begin{pmatrix} 1 & 4 & 5 & 3 & 2 \\ 3 & 2 & 4 & 5 & 1 \\ 2 & 5 & 3 & 1 & 4 \\ 5 & 1 & 2 & 4 & 3 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix}$	{(2 3)(4 5), (1 4)(3 5), (1 5)(2 4), (1 3)(2 5), (1 2)(3 4)}	D_5	D_{10}
$\begin{pmatrix} 1 & 4 & 5 & 2 & 3 \\ 3 & 2 & 1 & 5 & 4 \\ 4 & 5 & 3 & 1 & 2 \\ 5 & 3 & 2 & 4 & 1 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix}$	{(2 3 4 5), (1 4 3 5), (1 5 4 2), (1 2 5 3), (1 3 2 4)}	D_{10}	D_{10}

5.2. **The Fundamental Group.** Let X be a topological space and let $x_0 \in X$ be a chosen base point. The *fundamental group* of X at x_0, denoted $\pi_1(X, x_0)$, is the set of all homotopy classes of loops based at x_0.

A **loop** is a continuous map $\gamma : [0, 1] \to X$ such that $\gamma(0) = \gamma(1) = x_0$.

Two loops γ_1 and γ_2 based at x_0 are said to be **homotopic** (written $\gamma_1 \simeq \gamma_2$) if there exists a continuous map

$$H : [0,1] \times [0,1] \to X$$

such that:

$$H(0,t) = \gamma_1(t), \quad H(1,t) = \gamma_2(t), \quad H(s,0) = H(s,1) = x_0 \quad \text{for all } s \in [0,1].$$

The group operation on $\pi_1(X, x_0)$ is given by **concatenation of loops**, and the identity element is the constant loop at x_0. The inverse of a loop is the same path traversed in the reverse direction.

5.3. **Braid Groups.** The *braid group* on n strands, denoted B_n, is a group that describes the motion of n distinguishable strands in three-dimensional space such that they return to their original positions but may be interwoven.

Definition. The braid group B_n has the following **presentation**:

$$B_n = \left\langle \sigma_1, \sigma_2, \ldots, \sigma_{n-1} \mid \begin{array}{l} \sigma_i\sigma_j = \sigma_j\sigma_i, \quad \text{for} |i-j| \geq 2, \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, \quad \text{for } 1 \leq i \leq n-2 \end{array} \right\rangle,$$

where

- σ_i represents a **braid generator**, corresponding to exchanging the i-th and $(i+1)$-th strands with a right-handed crossing.
- The first relation $\sigma_i\sigma_j = \sigma_j\sigma_i$ (for $|i-j| \geq 2$) states that non-adjacent crossings commute.
- The second relation $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ (the **braid relation**) describes how adjacent crossings interact.

Geometric Interpretation. A braid can be visualized as a collection of n strands connecting n fixed points on the top to n fixed points on the bottom, such that the strands do not backtrack.

5.4. **Quandles and Quasigroups.**

Definition 5.2. A **quasigroup** is a set Q equipped with a binary operation $*$ such that for every pair of elements $a, b \in Q$, there exist unique elements $x, y \in Q$ satisfying:

$$x * a = b \quad \text{and} \quad a * y = b.$$

That is, the equations

$$x * a = b \quad \text{(left division)}$$

$$a * y = b \quad \text{(right division)}$$

always have unique solutions for x and y in Q.

A quasigroup can also be viewed as a *Latin square structure*, meaning that in the operation table of Q, each element appears exactly once in every row and every column.

- A *loop* is a quasigroup that has an identity element e such that $e * x = x * e = x$ for all $x \in Q$.
- A *group* is a loop where the binary operation is associative, i.e., $(x * y) * z = x * (y * z)$ for all $x, y, z \in Q$.

6. Rack

Definition 6.1. A *rack* is a generalization of a quandle. A racks is a set R with a binary operation $* : R \times R \to R$ satisfying:

(i) For all $y \in R$, the map $\beta_y : R \to R$ defined by $\beta_y(x) = x * y$ is invertible.

(ii) For all $x, y, z \in R$, $(x * y) * z = (x * z) * (y * z)$.

Example 6.2. *The multiplication table of a rack of order 3 is given by*

$*$	0	1	2
0	2	2	2
1	0	0	0
2	1	1	1

6.1. **Rack polynomial.**

Definition 6.3. If X is a rack in Definition 4.11, then the polynomial is the rack polynomial.

7. Shelf

Definition 7.1. A **shelf** is a set S equipped with a binary operation $* : S \times S \to S$ such that for all $x, y, z \in S$, they hold the self-distributivity:

$$x * (y * z) = (x * y) * (y * z).$$

Example 7.2. *The multiplication table of a shelf of order 3 is given by*

$*$	0	1	2
0	0	1	2
1	0	1	2
2	0	1	2

7.1. **Shelf polynomial.**

Definition 7.3. If X is a shelf in Definition 4.11, then the polynomial is called a shelf polynomial.

8. Quandle Rings and Rack Rings

Definition 8.1. Let Q be a quandle and R an associative ring with unity. Let $R[Q]$ be the set of all formal finite R-linear combinations of elements of Q.

$$R[Q] := \Big\{ \sum_i \alpha_i x_i \,|\, \alpha_i \in R,\, x_i \in Q \Big\}$$

$R[Q]$ is an additive abelian group with coefficient-wise addition. Define multiplication in $R[Q]$ by setting

$$\Big(\sum_i \alpha_i x_i\Big) \cdot \Big(\sum_j \beta_j x_j\Big) := \sum_{i,j} \alpha_i \beta_j \,(x_i * x_j).$$

Then, $R[Q]$ is a non-associative ring with coefficients in R.

8.1. **Idempotents in Quandle Rings.** We give a complete classification of the idempotents and tripotents in quandle rings $\mathbb{Z}_p[Q]$, where Q is a connected quandle and p is prime.

9. Idempotents in $\mathbb{Z}_p[Q]$, where $|Q| = 3$

In this section, we study idempotents in quandle rings where Q is of order 3. We also give a formula for the number of idempotents in terms of $|Q|$ and p. There is only one connected quandle of order 3 whose multiplication table is given by

$*$	X_0	X_1	X_2
X_0	X_0	X_2	X_1
X_1	X_2	X_1	X_0
X_2	X_1	X_0	X_2

Let $r = \alpha_0 X_0 + \alpha_1 X_1 + \alpha_2 X_2$, and set $r^2 = r$. That is,

$$(\alpha_0 X_0 + \alpha_1 X_1 + \alpha_2 X_2)^2 = \alpha_0 X_0 + \alpha_1 X_1 + \alpha_2 X_2.$$

$$\begin{aligned}(\alpha_0X_0+\alpha_1X_1+\alpha_2X_2)^2 &= (\alpha_0X_0+\alpha_1X_1+\alpha_2X_2)\cdot(\alpha_0X_0+\alpha_1X_1+\alpha_2X_2)\\ &= (\alpha_0^2+\alpha_1\alpha_2+\alpha_2\alpha_1)X_0+(\alpha_1^2+\alpha_0\alpha_2+\alpha_2\alpha_0)X_1\\ &+ (\alpha_2^2+\alpha_0\alpha_1+\alpha_1\alpha_0)X_2\end{aligned}$$

Thus

$$\alpha_0X_0+\alpha_1X_1+\alpha_2X_2 = (\alpha_0^2+\alpha_1\alpha_2+\alpha_2\alpha_1)X_0+(\alpha_1^2+\alpha_0\alpha_2+\alpha_2\alpha_0)X_1+(\alpha_2^2+\alpha_0\alpha_1+\alpha_1\alpha_0)X_2$$

By comparing the coefficients, we obtain the following set of equations:

$$\alpha_0^2+\alpha_1\alpha_2+\alpha_2\alpha_1 = \alpha_0$$

$$\alpha_1^2+\alpha_0\alpha_2+\alpha_2\alpha_0 = \alpha_1$$

$$\alpha_2^2+\alpha_0\alpha_1+\alpha_1\alpha_0 = \alpha_2$$

Let α_0, α_1, and α_2 be x, y, and z, respectively. Then the above set of equations can be written as

$$x^2-x+2yz = 0$$

$$y^2-y+2xz = 0$$

$$z^2-z+2xy = 0$$

Now we consider three cases: $p = 2$, $p = 3$, and $p > 3$. We will first discuss the case $p > 3$.

9.0.1. $p > 3$.

$$f_1 = x^2 - x + 2yz$$

$$f_2 = y^2 - y + 2xz$$

$$f_3 = z^2 - z + 2xy$$

Let $p = \{f_1,\, f_2,\, f_3\}$. Let $p > 3$ and $x > y > z$ (Lex order).

$$f_1 = x^2 - x + 2yz$$

$$f_2 = 2xz + y^2 - y$$

$$f_3 = 2xy + z^2 - z$$

Gröbner basis for the ideal generated by $f_1,\, f_2,\, f_3$.

$$\begin{aligned} s(f_1, f_2) &= \frac{x^2 z}{x^2}\left(y^2 - y - x + 2yz\right) - \frac{x^2 z}{2xz}\left(2xz + y^2 - y\right) \\ &= x^2 z - xz + 2yz^2 - x^2 z - \frac{1}{2}xy^2 + \frac{1}{2}xy \\ &= -\frac{1}{2}xy^2 + \frac{1}{2}xy - xz + 2yz^2 \end{aligned}$$

$$s(f_1, f_2) = 0 \cdot f_1 + \left(-\frac{1}{2}\right) \cdot f_2 + \left(\frac{1}{4} - \frac{y}{4}\right) \cdot f_3 + \frac{1}{4}\left(-2y + 2y^2 + z - yz - z^2 + 4yz^2\right)$$

We have

$$\overline{s(f_1, f_2)^p} \neq 0$$

Let $f_4 = \frac{1}{4}(-2y + 2y^2 + z - yz - z^2 + 4yz^2)$, and add it to the set $p = \{f_1, f_2, f_3, f_4\}$

Then, we have

$$f_4 = \frac{1}{2}y^2 + \frac{9}{4}yz^2 - \frac{1}{4}yz - \frac{1}{2}y - \frac{1}{4}z^2 + \frac{z}{4}.$$

None of the leading monomials of $f_1,\ f_2,\ f_3$ divides $\mathrm{LM}(f_4)$, and thus $\overline{s(f_1, f_2)}^p = 0$.

Now, let's compute $s(f_1, f_3)$.

$$\begin{aligned} s(f_1, f_3) &= \frac{x^2y}{x^2}\left(x^2 - x + 2yz\right) - \frac{x^2y}{2xy}\left(2xy + z^2 - z\right) \\ &= -xy - \frac{1}{2}xz^2 + \frac{1}{2}xz + 2y^2z \end{aligned}$$

$$\begin{aligned} s(f_1, f_3) = 0 \cdot f_1 + \left(\frac{1}{4} - \frac{z}{4}\right) \cdot f_2 + \left(-\frac{1}{2}\right) \cdot f_3 + \left(-\frac{1}{2} + \frac{9z}{2}\right) \cdot f_4 \\ + \left(-\frac{3}{8}\right) \cdot (z - 5yz + 2z^2 - 6yz^2 - 3z^3 + 27yz^3) \end{aligned}$$

which gives us

$$\overline{s(f_1, f_3)} = \left(-\frac{3}{8}\right) \cdot (z - 5yz + 2z^2 - 6yz^2 - 3z^3 + 27yz^3)$$

Clearly, $\overline{s(f_1, f_3)}^p \neq 0$, and we let it to be f_5 and add it to p.

Thus

$$p = \{f_1, f_2, f_3, f_4, f_5\}.$$

None of the leading monomials of $f_1,\ f_2,\ f_3,\ f_4$ divides $\mathrm{LM}(f_5)$, and therefore $\overline{s(f_1, f_3)}^p = 0$.

$$\begin{aligned} s(f_1, f_4) &= \frac{x^2y^2}{x^2}\left(x^2 - x + 2yz\right) - \frac{x^2y^2}{\left(\frac{1}{2}y^2\right)}\left(\frac{1}{2}y^2 + \frac{9}{4}yz^2 - \frac{1}{4}yz - \frac{1}{2}y - \frac{1}{4}z^2 + \frac{z}{4}\right) \\ &= -\frac{9}{2}x^2yz^2 + \frac{1}{2}x^2yz + x^2y + \frac{1}{2}x^2z^2 - \frac{1}{2}x^2z - xy^2 + 2y^3z \end{aligned}$$

$$= q_1 \cdot f_1 + q_2 \cdot f_2 + q_3 \cdot f_3 + q_4 \cdot f_4 + q_5 \cdot f_5 + f_6,$$

where

$$q_1 = \frac{1}{2}\left(2y - z + yz + z^2 - 9yz^2\right),$$

$$q_2 = \frac{1}{2}\left(-\frac{1}{2} + \frac{y}{2} + \frac{z}{2} - \frac{9yz}{2}\right),$$

$$q_3 = \frac{y}{2},$$

$$q_4 = 2\left(\frac{1}{4} - \frac{y}{4} - \frac{33}{8} + \frac{17yz}{4} + \frac{9z^2}{4} - \frac{81z^3}{8}\right),$$

$$q_5 = 4\left(-\frac{1}{36} + \frac{z}{8} - \frac{9z^2}{8}\right),$$

$$f_6 = \overline{s(f_1, f_4)}^f = \frac{1}{12}\left(4z - 2yz - z^2 - 6yz^2 - 30z^3 + 27z^4\right).$$

Let

$$p = \{f_1, f_2, f_3, f_4, f_5, f_6\}.$$

$$\begin{aligned} s(f_1, f_5) &= \frac{x^2yz^3}{x^2}\left(x^2 - x + 2yz\right) \\ &\quad - x^2yz^3\left(-\frac{81}{8}\right)yz^3\left(-\frac{81}{8}yz^3 + \frac{18}{8}yz^2 + \frac{15}{8}yz + \frac{9}{8}z^3 - \frac{6}{8}z^2 - \frac{3}{8}z\right) \\ &= \frac{18}{81}xyz^2 + \frac{15}{81}xyz + \frac{9}{81}xz^3 - \frac{6}{81}xz^2 - \frac{3}{81}x^2z - xyz^3 + 2y^2z^4 \\ &= q_1 \cdot f_1 + q_2 \cdot f_2 + q_3 \cdot f_3 + q_4 \cdot f_4 + q_5 \cdot f_5 + q_6 \cdot f_6 + f_7, \end{aligned}$$

where

$$q_1 = \frac{1}{27}\left(-z + 5yz - 27z^2 + 6yz^2 + 3z^3\right),$$

$$q_2 = \frac{1}{27}\left(-\frac{1}{2} + \frac{5y}{2} - z + 3yz + \frac{3z^2}{2} - \frac{27yz^2}{2}\right),$$

$$q_3 = 0,$$

$$q_4 = \frac{4}{27}\left(\frac{1}{4} - \frac{5y}{4} - \frac{z}{8} - \frac{3yz}{2} - \frac{7z^2}{8} + \frac{27yz^2}{4} + \frac{33z^3}{8} - \frac{27z^4}{8}\right),$$

$$q_5 = \frac{8}{27}\left(\frac{13}{972} - \frac{11z}{216} + \frac{5z^2}{12} - \frac{33z^3}{8}\right),$$

$$q_6 = -\frac{8}{729}, \quad \text{and}$$

$$R = \overline{s(f_2, f_5)}^f = \frac{1}{486}\left(-2z + 5z^2 + 15z^3 - 45z^4 + 27z^5\right)$$

Note that $486 \neq 0$ since $p > 3$ because $486 = 2 \cdot 3^5$.

$$f_7 = \overline{s(b_1, f_3)}^f = \frac{1}{486}\left(27z^5 - 45z^4 + 15z^3 + 5z^2 - 2z\right) \neq 0$$

We have

$$p = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7\}$$

and

$$\overline{s(f_2, f_5)}^f = 0.$$

We have already computed

$$s(f_1, f_2),\ s(f_1, f_3),\ s(f_1, f_4),\ s(f_2, f_4),\ s(f_2, f_5).$$

Let's compute other S-polynomials.

$$s(f_i, f_j), \text{ where } i < j \text{ and } i, j \in \{1, 2, \ldots, 7\}.$$

$$\begin{aligned} s(f_1, f_6) &= \frac{x^2yz^2}{x^2}\left(x^2 - x + 2yz\right) - \frac{x^2yz^2}{-\frac{1}{2}yz^2}\left(-\frac{1}{2}yz^2 - \frac{1}{6}yz + \frac{9}{4}z^4 - \frac{5}{2}z^3 - \frac{1}{12}z^2 + \frac{1}{2}z\right) \\ &= x^2yz^2 - xyz^2 + 2y^2z^3 - x^2yz^2 - \frac{1}{2}x^2yz + \frac{9}{2}x^2z^4 - 5x^2z^3 - \frac{1}{6}x^2z^2 + \frac{2}{3}x^2z \end{aligned}$$

After simplifying terms, we get

$$s(f_1, f_6) = -\frac{1}{3}x^2yz + \frac{9}{2}x^2z^4 - 5x^2z^3 - \frac{1}{6}x^2z^2 + \frac{2}{3}x^2z - 6yz^2 + 2y^2z^3$$

Thus we have

$$\overline{s(f_1, f_6)}^f = 0.$$

Now we compute $s(f_1, f_7)$.

$$\begin{aligned} s(f_1, f_7) &= \frac{x^2z^5}{x^2}\left(x^2 - x + 2yz\right) - x^2z^5\left(\frac{1}{18}z^5 - \frac{5}{54}z^4 + \frac{5}{162}z^3 + \frac{5}{486}z^2 - \frac{1}{243}z\right) \\ &= x^2z^5 - xz^5 + 2yz^6 - 18x^2\left(\frac{1}{18}z^5 - \frac{5}{54}z^4 + \frac{5}{162}z^3 + \frac{5}{486}z^2 - \frac{1}{243}z\right) \\ &= -x^2z^5 + 2yz^6 + \frac{5}{3}x^2z^4 - \frac{5}{9}x^2z^3 - \frac{5}{27}x^2z^2 + \frac{2}{27}x^2z \end{aligned}$$

After simplifying terms, we get

$$s(f_1, f_7) = \frac{5}{3}x^2z^4 - \frac{5}{9}x^2z^3 - \frac{5}{27}x^2z^2 + \frac{2}{27}x^2z - xz^5 + 2yz^6 = 0.$$

Now we have

$$\overline{s(f_2, f_2)}^f = \overline{s(f_2, f_3)}^f = \overline{s(f_2, f_4)}^f = \overline{s(f_2, f_5)}^f = \overline{s(f_2, f_6)}^f = \overline{s(f_2, f_7)}^f = 0.$$

$$\overline{s(f_3, f_4)}^f = 0, \quad \overline{s(f_3, f_5)}^f = 0, \quad \overline{s(f_3, f_6)}^f = 0, \quad \overline{s(f_3, f_7)}^f = 0$$

$$\overline{s(f_4, f_5)}^f = 0, \quad \overline{s(f_4, f_6)}^f = 0, \quad \overline{s(f_4, f_7)}^f = 0$$

$$\overline{s(f_5, f_6)}^f = 0, \quad \overline{s(b_5, f_7)}^f = 0$$

$$\overline{s(f_6, f_7)}^f = 0$$

A Gröbner Basis for

$$G = \langle x^2 - x + 2yz,\ 20z + y^2 - y,\ 2xy + z^2 - z \rangle$$

is given by

$$\begin{cases} f_1 = x^2 - x + 2yz, \\ f_2 = 2xz + y^2 - y, \\ f_3 = 2xy + z^2 - z, \\ f_4 = \frac{1}{2}y^2 + \frac{9}{4}yz^2 - \frac{1}{4}yz - \frac{1}{2}y - \frac{1}{4}z^2 + \frac{1}{4}z, \\ f_5 = -\frac{81}{8}yz^3 + \frac{18}{8}yz^2 + \frac{15}{8}yz + \frac{9}{8}z^3 - \frac{6}{8}z^2 - \frac{3}{8}z, \\ f_6 = -\frac{1}{2}yz^2 - \frac{1}{6}yz + \frac{9}{4}z^4 - \frac{5}{2}z^3 - \frac{1}{12}z^2 + \frac{1}{2}z, \\ f_7 = \frac{1}{18}z^5 - \frac{5}{54}z^4 + \frac{5}{162}z^3 + \frac{5}{486}z^2 - \frac{1}{243}z. \end{cases}$$

Note that $p > 3$ in our computations. None of the denominators is zero since only 2 and 3 appear in their prime factorizations. So, the Gröbner basis above is well-defined.

In $\mathbb{Z}_p$, the solutions of $f_7(z) = 0$ are

$$z = 0, \quad z = 1, \quad z = \frac{2}{3}, \quad z = \frac{1}{3}, \quad z = -\frac{1}{3}.$$

Now we have the roots of the last polynomial f_7 in the Gröbner basis. These are in $\mathbb{Z}_p$, for any $p \geq 3$. $f(z) \equiv 0 \Rightarrow z = 0, \quad z = 1, \quad z = \frac{2}{3}, \quad z = \frac{1}{3}, \quad z = -\frac{1}{3}$. Now, let's consider the fourth polynomial f_4 in the Gröbner basis.

$$f_4(y, z) = \frac{1}{2}y^2 + \frac{9}{4}yz^2 - \frac{1}{4}yz - \frac{1}{2}y - \frac{1}{4}z^2 + \frac{1}{4}z$$

Set $f_4 = 0$. The pairs (y, z) that satisfy the equation $f_4 = 0$ are

$$(0,0), \quad (1,0), \quad (0,1), \quad (-3,1), \quad \left(-\frac{1}{3}, \frac{2}{3}\right), \quad \left(\frac{1}{3}, \frac{1}{3}\right), \quad \left(-\frac{1}{3}, -\frac{1}{3}\right), \quad \left(\frac{2}{3}, -\frac{1}{3}\right).$$

In order to find all (x, y, z) satisfy our system of our Gröbner basis, we consider the polynomial f_5.

$$\begin{aligned}
f_5(0,0) &= 0, \\
f_5(1,0) &= 0, \\
f_5(0,1) &= 0, \\
f_5(-3,1) &= 18 \neq 0 \quad \text{for any } p > 3, \\
f_5\left(-\frac{1}{3}, \frac{2}{3}\right) &= 0, \\
f_5\left(\frac{1}{3}, \frac{1}{3}\right) &= 0, \\
f_5\left(-\frac{1}{3}, -\frac{1}{3}\right) &= 0, \\
f_5\left(\frac{2}{3}, -\frac{1}{3}\right) &= 0.
\end{aligned}$$

So we drop $(-3, 1)$ from the list of pairs. We now evaluate f_6 at the remaining points.

$$\begin{aligned} f_6(0,0) &= 0, \\ f_6(1,0) &= 0, \\ f_6(0,1) &= 0, \\ f_6\left(-\frac{1}{3}, \frac{2}{3}\right) &= 0, \\ f_6\left(\frac{1}{3}, \frac{1}{3}\right) &= 0, \\ f_6\left(-\frac{1}{3}, -\frac{1}{3}\right) &= 0, \\ f_6\left(\frac{2}{3}, -\frac{1}{3}\right) &= 0. \end{aligned}$$

Here are the ordered pairs (y, z) for which we still need to find x for:

$$\begin{aligned} (y,z) &= (0,0), \\ (y,z) &= (1,0), \\ (y,z) &= (0,1), \\ (y,z) &= (-\frac{1}{3}, \frac{2}{3}), \\ (y,z) &= (\frac{1}{3}, \frac{1}{3}), \\ (y,z) &= (-\frac{1}{3}, -\frac{1}{3}), \\ (y,z) &= (\frac{2}{3}, -\frac{1}{3}). \end{aligned}$$

Let's find x for those (y, z) pairs. For $(y, z) = (0, 0)$, equation f_1 yields

$$x^2 - x + 2yz = 0 \implies x^2 - x = 0 \implies x(x-1) = 0,$$

which gives us the triples

$$(0,0,0) \quad \text{or} \quad (1,0,0).$$

For $(y, z) = (1, 0)$, from equation $f_1 = 0$ gives us

$$x^2 - x + 2yz = 0 \implies x^2 - x = 0 \implies x(x-1) = 0,$$

which gives us the triples

$$(0, 1, 0) \quad , \quad (1, 1, 0).$$

From equation $f_3 = 0$, we get $x = 0$, which gives us the triple

$$(0, 1, 0).$$

From equation $f_1 = 0$, we get

$$x^2 - x - \frac{4}{9} = 0.$$

Factoring the quadratic polynomial gives us the equation

$$\left(x - \frac{4}{3}\right)\left(x + \frac{1}{3}\right) = 0.$$

Therefore, we have

$$x = -\frac{1}{3} \quad , \quad x = \frac{4}{3}.$$

This gives us the triples

$$\left(-\frac{1}{3}, -\frac{1}{3}, \frac{2}{3}\right) \quad \text{and} \quad \left(\frac{4}{3}, -\frac{1}{3}, \frac{2}{3}\right).$$

From equation $f_2 = 0$, we obtain the same result:

$$x = -\frac{1}{3}, \quad \text{leading to the same triple} \quad \left(-\frac{1}{3}, -\frac{1}{3}, \frac{2}{3}\right).$$

From equation $f_3 = 0$, we also get

$$x = -\frac{1}{3}, \quad \text{leading to the same triple} \quad \left(-\frac{1}{3}, -\frac{1}{3}, \frac{2}{3}\right).$$

Let's find x for $(y, z) = \left(\frac{1}{3}, \frac{1}{3}\right)$.

From equation $f_1 = 0$, we obtain

$$x^2 - x + 2yz = 0.$$

Substituting $y = \frac{1}{3}$ and $z = \frac{1}{3}$, we get:

$$x^2 - x + 2\left(\frac{1}{3} \cdot \frac{1}{3}\right) = 0,$$

which simplifies to

$$x^2 - x + \frac{2}{9} = 0.$$

Factoring the quadratic polynomial gives us the equation

$$\left(x - \frac{1}{3}\right)\left(x - \frac{2}{3}\right) = 0,$$

which gives us the following two solutions for x:

$$x = \frac{1}{3} \quad , \quad x = \frac{2}{3}.$$

This gives us the triples:

$$\left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right) \quad , \quad \left(\frac{2}{3}, \frac{1}{3}, \frac{1}{3}\right)$$

From equation $f_2 = 0$, we get the same result:

$$x = \frac{1}{3}, \quad \text{leading to the same triple} \quad \left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right).$$

From equation $f_3 = 0$, we also find

$$x = \frac{1}{3}, \quad \text{leading to the same triple} \quad \left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right).$$

Let's find x for $(y, z) = \left(-\frac{1}{3}, -\frac{1}{3}\right)$.

From equation $f_1 = 0$, we get

$$x^2 - x + 2yz = 0.$$

Substituting $y = -\frac{1}{3}$ and $z = -\frac{1}{3}$, we get

$$x^2 - x + 2\left(-\frac{1}{3} \cdot -\frac{1}{3}\right) = 0,$$

which simplifies to

$$x^2 - x + \frac{2}{9} = 0.$$

Factoring the quadratic polynomial gives us the equation

$$\left(x - \frac{1}{3}\right)\left(x - \frac{2}{3}\right) = 0,$$

which yields

$$x = \frac{1}{3}, x = \frac{2}{3}.$$

This gives the triples:

$$\left(\frac{1}{3}, -\frac{1}{3}, -\frac{1}{3}\right), \left(\frac{2}{3}, -\frac{1}{3}, -\frac{1}{3}\right).$$

From equation f_2 and equation f_3, we obtain the same result:

$$x = \frac{1}{3}, \quad \text{leading to the same triple:} \quad \left(\frac{2}{3}, -\frac{1}{3}, -\frac{1}{3}\right).$$

$(y, z) = \left(\frac{2}{3}, -\frac{1}{3}\right)$: We can solve for x From Equation (1):

$$x^2 - x + 2yz = 0.$$

Substituting $y = \frac{2}{3}$ and $z = -\frac{1}{3}$, we get:

$$x^2 - x + 2\left(\frac{2}{3} \cdot -\frac{1}{3}\right) = 0,$$

which simplifies to:

$$x^2 - x - \frac{4}{9} = 0.$$

Factoring this quadratic polynomial gives us the equation

$$\left(x + \frac{1}{3}\right)\left(x - \frac{4}{3}\right) = 0,$$

Therefore,

$$x = -\frac{1}{3} \quad , \quad x = \frac{4}{3}.$$

This gives us the triples:

$$\left(-\frac{1}{3}, \frac{2}{3}, -\frac{1}{3}\right) \quad , \quad \left(\frac{4}{3}, \frac{2}{3}, -\frac{1}{3}\right).$$

From Equations (2) and (3), we obtain the same result:

$$x = -\frac{1}{3}, \quad \text{leading to the same triple:} \quad \left(-\frac{1}{3}, \frac{2}{3}, -\frac{1}{3}\right).$$

The triples we have are:

$$(0,0,0),$$

$$(1,0,0),\ (0,1,0),\ (0,0,1),$$

$$(1,1,0),\ (1,0,1),\ (0,1,1),$$

$$\left(-\frac{1}{3}, -\frac{1}{3}, \frac{2}{3}\right),\ \left(\frac{2}{3}, -\frac{1}{3}, -\frac{1}{3}\right),\ \left(\frac{2}{3}, \frac{1}{3}, \frac{1}{3}\right),$$
$$\left(-\frac{1}{3}, \frac{2}{3}, -\frac{1}{3}\right),\ \left(\frac{4}{3}, -\frac{1}{3}, \frac{1}{3}\right),\ \left(\frac{2}{3}, -\frac{1}{3}, -\frac{1}{3}\right)$$
$$\left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right),$$

We need to find triples that are roots of equations 1, 2, and 3: Clearly, the following triples are roots of f_1, f_2, and f_3:

$$(0,0,0),$$

$$(1,0,0),$$

$$(0,1,0),$$

$$(0,0,1).$$

A straightforward computation shows that the triple $\left(-\frac{1}{3}, -\frac{1}{3}, \frac{2}{3}\right)$ is also a root of f_1, f_2, and f_3.

Thus, its cyclic shifts are also roots:

$$\left(\frac{2}{3}, -\frac{1}{3}, -\frac{1}{3}\right),$$
$$\left(-\frac{1}{3}, \frac{2}{3}, -\frac{1}{3}\right).$$

Similarly, a straightforward computation shows that

$$\left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right).$$

We now have 8 triples that satisfy $f_1 = 0, f_2 = 0, f_3 = 0$. They are

$$(0,0,0), \quad (1,0,0), \quad (0,1,0), \quad (0,0,1), \quad \left(-\frac{1}{3}, -\frac{1}{3}, \frac{2}{3}\right), \quad \left(\frac{2}{3}, -\frac{1}{3}, -\frac{1}{3}\right),$$
$$\left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right), \quad \left(-\frac{1}{3}, \frac{2}{3}, -\frac{1}{3}\right).$$

Recall the triple

$$\left(\frac{4}{3}, -\frac{1}{3}, \frac{2}{3}\right).$$

For this triple, we have:

$$f_2\left(\frac{4}{3}, -\frac{1}{3}, \frac{2}{3}\right) = \frac{20}{9} \neq 0 \quad \text{when } p > 3,$$
$$f_3\left(\frac{4}{3}, -\frac{1}{3}, \frac{2}{3}\right) = -\frac{10}{9} \quad \text{when } p > 3.$$

Thus, when $p = 5$, the triple becomes

$$\left(-\frac{1}{3}, -\frac{1}{3}, \frac{2}{3}\right),$$

which we already have as a solution. Next, consider the triple

$$\left(\frac{4}{3}, \frac{2}{3}, -\frac{1}{3}\right).$$

For this triple, we have:

$$f_2\left(\frac{4}{3}, \frac{2}{3}, -\frac{1}{3}\right) = -\frac{10}{9} \quad \text{when } p > 3,$$
$$f_3\left(\frac{4}{3}, \frac{2}{3}, -\frac{1}{3}\right) = \frac{20}{9} \neq 0 \quad \text{when } p > 3.$$

Thus, when $p = 5$, the triple becomes

$$\left(-\frac{1}{3}, \frac{2}{3}, -\frac{1}{3}\right),$$

which we already have as a solution.

The triple

$$\left(\frac{2}{3}, \frac{1}{3}, \frac{1}{3}\right)$$
$$f_2\left(\frac{2}{3}, \frac{1}{3}, \frac{1}{3}\right) = \frac{2}{9} \neq 0 \quad \text{for any } p > 3$$
$$f_3\left(\frac{2}{3}, \frac{1}{3}, \frac{1}{3}\right) = \frac{2}{9} \neq 0 \quad \text{for any } p > 3$$

which means it is not solutions to our system. The triple:

$$\left(\frac{1}{3}, -\frac{1}{3}, -\frac{1}{3}\right)$$
$$f_2\left(\frac{1}{3}, -\frac{1}{3}, -\frac{1}{3}\right) = \frac{2}{9} \neq 0 \quad \text{for any } p > 3$$
$$f_3\left(\frac{1}{3}, -\frac{1}{3}, -\frac{1}{3}\right) = \frac{2}{9} \neq 0 \quad \text{for any } p > 3$$

which means it is not solutions to our system

The system:

$$x^2 - x + 2yz = 0$$

$$y^2 - y + 2xz = 0$$

$$z^2 - z + 2xy = 0$$

has exactly 8 solutions for any $p > 3$.

Remark 9.1. *If one of the cyclic shifts of a triple is a solution, the other shifts are also solutions.*

9.0.2. $p = 2$. When $p = 2$, our system of equations becomes

Proof.

$$x^2 - x = 0$$

$$y^2 - y = 0$$

$$z^2 - z = 0$$

Solving this system of equations in characteristic 2 gives us the following triples:

$$(0, 0, 0),$$

$$(1, 0, 0),\ (0, 1, 0),\ (0, 0, 1),$$

$$(1, 1, 0),\ (1, 0, 1),\ (0, 1, 1),$$

$$(1, 1, 1).$$

□

9.0.3. $p = 3$. The idempotents when $p = 3$ are

$$(0, 0, 0),$$

$$(1, 0, 0),\ (0, 1, 0),\ (0, 0, 1),$$

10. Number of Idempotents in Quandle Rings

There are 3 quandles of order 3 up to isomorphism:

$*$	0	1	2
0	0	0	0
1	1	1	1
2	2	2	2

$*$	0	1	2
0	0	2	1
1	2	1	0
2	1	0	2

$*$	0	1	2
0	0	0	0
1	2	1	1
2	1	2	2

Let's name these quandles Q_{31}, Q_{32}, and Q_{33}, respectively.

Question: How many idempotents do the quandle rings $\mathbb{Z}_p[Q_{31}]$, $\mathbb{Z}_p[Q_{32}]$ and $\mathbb{Z}_p[Q_{33}]$ have?

Theorem 10.1. *Number of idempotents in* $\mathbb{Z}_p[Q_{31}] \;=\; p^2+1$.

Proof.

$$Q_{31} = \begin{array}{c|ccc} * & X_0 & X_1 & X_2 \\ \hline X_0 & X_0 & X_0 & X_0 \\ X_1 & X_1 & X_1 & X_1 \\ X_2 & X_2 & X_2 & X_2 \end{array}$$

Let $r = \alpha_0 X_0 + \alpha_1 X_1 + \alpha_2 X_2$, and set $r^2 = r$. That is,

$$(\alpha_0 X_0 + \alpha_1 X_1 + \alpha_2 X_2)^2 = \alpha_0 X_0 + \alpha_1 X_1 + \alpha_2 X_2.$$

$$\begin{aligned}(\alpha_0 X_0 + \alpha_1 X_1 + \alpha_2 X_2)^2 &= (\alpha_0 X_0 + \alpha_1 X_1 + \alpha_2 X_2)\cdot(\alpha_0 X_0 + \alpha_1 X_1 + \alpha_2 X_2) \\ &= (\alpha_0^2 + \alpha_0\alpha_1 + \alpha_0\alpha_2)X_0 + (\alpha_1^2 + \alpha_1\alpha_0 + \alpha_1\alpha_2)X_1 \\ &\quad + (\alpha_2^2 + \alpha_2\alpha_0 + \alpha_2\alpha_1)X_2\end{aligned}$$

By comparing the coefficients, we obtain the following set of equations:

$$\alpha_0^2 + \alpha_0\alpha_1 + \alpha_0\alpha_2 = \alpha_0$$

$$\alpha_1^2 + \alpha_1\alpha_0 + \alpha_1\alpha_2 = \alpha_1$$

$$\alpha_2^2 + \alpha_2\alpha_0 + \alpha_2\alpha_1 = \alpha_2$$

Let α_0, α_1, and α_2 be x, y, and z, respectively. Then the above set of equations can be written as

$$x^2 - x + xy + xz = 0$$

$$y^2 - y + xy + yz = 0$$

$$z^2 - z + xz + yz = 0$$

$$x \cdot (x + y + z - 1) = 0 \Rightarrow x = 0 \quad \text{or} \quad x + y + z = 1,$$

$$y \cdot (x + y + z - 1) = 0 \Rightarrow y = 0 \quad \text{or} \quad x + y + z = 1,$$

$$z \cdot (x + y + z - 1) = 0 \Rightarrow z = 0 \quad \text{or} \quad x + y + z = 1.$$

We need to find (x, y, z) that satisfies

$$x = 0 \quad \text{or} \quad x + y + z = 1,$$

$$y = 0 \quad \text{or} \quad x + y + z = 1,$$

and

$$z = 0 \quad \text{or} \quad x + y + z = 1.$$

Case 1: x = 0.

- $\boxed{1.1}$ x = 0, y = 0
  - $\boxed{1.1.1}$ x = y = z = 0 (0, 0, 0)
  - $\boxed{1.1.2}$ x = 0, y = 0, x + y + z = 1 (0, 0, 1)

- $\boxed{1.2}$ x = 0, x + y + z = 1
  - $x = 0$ and $y + z = 1$
  - $\boxed{1.2.1}$ x = 0, y + z = 1, z = 0 (0, 1, 0)
  - $\boxed{1.2.2}$ x = 0, y + z = 1 (0, y, z), where y + z = 1

Case 2: $x \neq 0$.

- $\boxed{2.1}$ $x \neq 0$, $y = 0$.
  - $x \neq 0$, $y = 0$, $x + y + z = 1$

    $(0, 0, z)$ where $x + z = 1$
- $\boxed{2.2}$ $x \neq 0$, $x + y + z = 1$, $z \neq 0$.
  - $(x, y, 0)$ with $x + z = 1$

Case 3: $x \neq 0$, $y \neq 0$, and $z \neq 0$.

We have

- $(0, 0, 0)$
- $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$
- $(0, y, z)$, where $y + z = 1$
- $(x, 0, z)$, where $x + z = 1$
- $(x, y, 0)$, where $x + y = 1$
- (x, y, z), where $x + y + z = 1$ and $x \neq 0$, $y \neq 0$, and $z \neq 0$

Any nonzero triple (a, b, c) of the system satisfies $a + b + c \equiv 1 \pmod{p}$. Let's start counting the number of idempotents.

We always have the following four solutions: $(0, 0, 0)$, $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$

We also have $(0, y, z), (x, 0, z), (x, y, 0)$ with cyclic shifts.

Consider a triple (a, b, c). Assume that exactly one of a, b, and c is zero. Without loss of generality (WLOG), say $a = 0$, so we have $(0, b, c)$.

We want $b + c \equiv 1 \pmod{p}$.

We can write such a triple as $(0, a, p+1-a)$, where $2 \leq a \leq p-1$. Each a gives a unique such triple. There are $3(p-2)$ such triples due to cyclic shifts. So far, we have $3(p-2)+4$ solutions, which simplifies to $3p-2$.

Let us count the solutions (x, y, z), where $x \neq 0$, $y \neq 0$, and $z \neq 0$.

For a, there are $(p-1)$ choices. Once a is chosen, $*$ has only one choice because of uniqueness.

In $(2, a, *)$, a has $(p-2)$ choices because a cannot be p.

In $(3, a, *)$, a has $(p-2)$ choices because a cannot be $p-2$.

In $(n, a, *)$, a has $(p-2)$ choices because a cannot be $p-(n-1)$.

Here are the patterns:

In $(1, a, *)$, there are $(p-1)$ choices for the solution.

In $(n, a, *)$, where $2 \leq n \leq p$, there are $(p-2)$ choices for the solution. For n we have $(p-2)$ choices because $2 \leq n \leq p$. For triples of the form $(n, a, *)$, where $2 \leq n \leq p$, we have a total of $(p-2)(p-2)$ choices.

We now consider triples of the form $(n, a, *)$, where $1 \leq n \leq p-1$.

Here, there are $(p-1)+(p-2)(p-2)$ such triples.

Let's do the final counting.

$$
\begin{aligned}
\text{Total number of triples: } &= (3p-2)+(p-1)+(p-2)(p-2) \\
&= 2p+(p-2)+(p-1)+(p-2)(p-2) \\
&= 2p+(p-2)\,[1+(p-2)]+(p-1) \\
&= 2p+(p-2)(p-1)+(p-1) \\
&= 2p+(p-1)\,[(p-2)+1] \\
&= 2p+(p-1)(p-1) \\
&= 2p+(p-1)^2 = 2p+p^2-2p+1 = p^2+1
\end{aligned}
$$

□

Theorem 10.2. *Number of idempotents in* $\mathbb{Z}_p[Q_{33}] = 2p$.

Proof.

$$Q_{33} = \begin{bmatrix} 0 & 0 & 0 \\ 2 & 1 & 1 \\ 1 & 2 & 2 \end{bmatrix} \qquad Q_{33} = \begin{bmatrix} x_0 & x_0 & x_0 \\ x_2 & x_1 & x_1 \\ x_1 & x_2 & x_2 \end{bmatrix}$$

Consider an arbitrary element a in the quandle ring, say $a = \alpha_0 x_0 + \alpha_1 x_1 + \alpha_2 x_2$, where $a \in \mathbb{Z}_p[Q_{33}]$.

Set $a^2 = a$.

$$\begin{aligned}(\alpha_0 x_0 + \alpha_1 x_1 + \alpha_2 x_2)^2 &= (\alpha_0 x_0 + \alpha_1 x_1 + \alpha_2 x_2)(\alpha_0 x_0 + \alpha_1 x_1 + \alpha_2 x_2) \\ &= (\alpha_0^2 + \alpha_1\alpha_2 + \alpha_2\alpha_1)x_0 + (\alpha_1^2 + \alpha_0\alpha_2 + \alpha_2\alpha_0)x_1 \\ &+ (\alpha_2^2 + \alpha_0\alpha_1 + \alpha_1\alpha_0)x_2\end{aligned}$$

$$\alpha_0^2 + \alpha_1\alpha_2 + \alpha_2\alpha_1 = \alpha_0$$

$$\alpha_1^2 + \alpha_0\alpha_2 + \alpha_2\alpha_0 = \alpha_1$$

$$\alpha_2^2 + \alpha_0\alpha_1 + \alpha_1\alpha_0 = \alpha_2$$

(10.1) $$\alpha_0^2 - \alpha_0 + \alpha_1\alpha_2 + \alpha_2\alpha_1 = 0 \quad (1)$$

(10.2) $$\alpha_1^2 - \alpha_1 + \alpha_0\alpha_2 + \alpha_2\alpha_0 = 0 \quad (2)$$

(10.3) $$\alpha_2^2 - \alpha_2 + \alpha_0\alpha_1 + \alpha_1\alpha_0 = 0 \quad (3)$$

From (1):

$$\alpha_0(\alpha_0 + \alpha_1 + \alpha_2 - 1) = 0 \Rightarrow \alpha_0 = 0 \quad \text{or} \quad \alpha_0 + \alpha_1 + \alpha_2 = 1$$

$$\alpha_1(\alpha_1 + \alpha_2 - 1) + \alpha_0\alpha_2 = 0$$

$$\alpha_2(\alpha_2 + \alpha_1 - 1) + \alpha_0\alpha_1 = 0$$

So:

$$\alpha_0 = 0 \quad \text{or} \quad \alpha_0 + \alpha_1 + \alpha_2 = 1 \quad \text{and}$$

Case: $\alpha_0 = 0$

$$\alpha_1(\alpha_1 + \alpha_2 - 1) = 0 \Rightarrow \alpha_1 = 0 \quad \text{or} \quad \alpha_1 + \alpha_2 = 1$$

1.1:

$$\alpha_0 = 0,\ \alpha_1 = 0 \Rightarrow \alpha_2 = 0 \quad \text{or} \quad \alpha_2 = 1 \Rightarrow (0,0,0) \quad \text{or} \quad (0,0,1)$$

1.2:

$$\alpha_0 = 0,\ \alpha_1 + \alpha_2 = 1 \Rightarrow (0, \alpha_1, \alpha_2) \quad \text{with} \quad \alpha_1 + \alpha_2 = 1$$

Case 2

$$\alpha_0 + \alpha_1 + \alpha_2 = 1$$

$$\alpha_1 + \alpha_2 = 1 - \alpha_0$$

$$\text{From } (2) \Rightarrow \alpha_1(1 - \alpha_0 - \alpha_1) + \alpha_0\alpha_2 = 0$$

$$\Rightarrow -\alpha_1^2 + \alpha_2\alpha_0 = 0$$

$$\Rightarrow \alpha_1(\alpha_2 - \alpha_0) = 0$$

$$\Rightarrow \alpha_1 = 0 \quad \text{or} \quad \alpha_2 = \alpha_0$$

$$(\alpha_0, \alpha_1, \alpha_2)$$

2.1 $\alpha_1 = 0,\ \alpha_0 + \alpha_2 = 1$

$$(0, 0, \alpha_2), \quad \text{where } \alpha_0 + \alpha_2 = 1$$

2.2 $\alpha_0 + \alpha_1 + \alpha_2 = 1, \quad \alpha_2 = \alpha_0$

$$(\alpha_0, \alpha_1, \alpha_0), \quad \text{where } \alpha_0 + \alpha_1 + \alpha_0 = 1$$

$$\Rightarrow 2\alpha_0 + \alpha_1 = 1$$

From (3):

$$\alpha_2(-\alpha_0) + \alpha_0\alpha_1 = 0$$

$$-\alpha_0\alpha_2 + \alpha_0\alpha_1 = 0$$

$$\alpha_0(\alpha_1 - \alpha_2) = 0 \Rightarrow \alpha_0 = 0 \quad \text{or} \quad \alpha_1 = \alpha_2$$

Always solutions:

$$(0, 0, 0), \quad (0, 0, 1), \quad (0, 1, 0), \quad (1, 0, 0)$$

$$(0, \alpha_1, \alpha_2), \quad \text{with } \alpha_1 + \alpha_2 = 1$$

$$(\alpha_0, \alpha_1, \alpha_2), \quad \text{where } \alpha_0 + \alpha_1 + \alpha_2 = 1,\ \alpha_1 = \alpha_2, \text{ and } \alpha_0, \alpha_1, \alpha_2 \neq 0$$

Note: $(0, 0, 0)$ is 1 triple.

Always solutions:

$$(0, 0, 1), \quad (0, 1, 0), \quad (1, 0, 0) \quad \text{— 3 triples}$$

Triples of the form $(0, \alpha_1, \alpha_2), \quad \alpha_1 + \alpha_2 = 1$

Once you choose α_1, then α_2 is fixed.

There are $(p-2)$ choices for α_1 because

$$1 \leq \alpha_1 \leq p-1$$

Triples of the form $\quad (\alpha_0, \alpha_1, \alpha_2), \quad \alpha_1 = \alpha_2, \quad \alpha_0 + \alpha_1 + \alpha_2 = 1$

With the additional condition: none of them is zero.

We are looking at **triples of the form**

$$(a, b, b) \quad \text{with } a + 2b = 1, \quad \text{none of them is zero}$$

Once you choose a, then b is fixed.

There are $(p-2)$ choices for a since

$$2 \leq a \leq p-1$$

Note: a cannot be 1 because in that case $b = 0$

Total number of idempotents:

$$= 1 + 3 + (p-2) + (p-2)$$

$$= 2p$$

□

What about $\mathbb{Z}_p[Q_{32}]$?

p	**Quandle**	**Number of Idempotents**
2	Q 32	8
3	Q 32	4
$p > 3$	Q 32	8
2	Q 51	12
3	Q 51	12
5	Q 51	6
$p > 5$	Q 51	12
2	Q 52	12
3	Q 52	12
5	Q 52	6
$p > 5$	Q 52	12

11. Idempotents in $\mathbb{Z}_p[Q]$, where $|Q| > 3$

In this section, we generalize our results in the previous section to any quandle ring where the quandle is of prime order. There are $p-2$ connected quandles of order p up to isomorphism: 1 connected quandle of order 3, 3 connected quandles of order 5, 5 connected quandles of order 7, and so on. We have listed the only connected quandles of order 3, and two connected quandles of order 3 and 7, each. Our computational results show that there are two connected quandles of order $p > 3$ up to isomorphism whose polynomial coefficients in Gröbner basis can be written in terms of the cardinality of the quandle. Interestingly, polynomial coefficients in the Gröbner basis when $p = 3$ follows the same pattern.

$*$	0	1	2
0	0	2	1
1	2	1	0
2	1	0	2

$*$	0	1	2	3	4
0	0	3	4	2	1
1	2	1	3	4	0
2	1	4	2	0	3
3	4	0	1	3	2
4	3	2	0	1	4

$*$	0	1	2	3	4
0	0	3	4	1	2
1	2	1	0	4	3
2	3	4	2	0	1
3	4	2	1	3	0
4	1	0	3	2	4

$*$	0	1	2	3	4	5	6
0	0	4	1	5	2	6	3
1	4	1	5	2	6	3	0
2	1	5	2	6	3	0	4
3	5	2	6	3	0	4	1
4	2	6	3	0	4	1	5
5	6	3	0	4	1	5	2
6	3	0	4	1	5	2	6

$*$	0	1	2	3	4	5	6
0	0	5	3	1	6	4	2
1	3	1	6	4	2	0	5
2	6	4	2	0	5	3	1
3	2	0	5	3	1	6	4
4	5	3	1	6	4	2	0
5	1	6	4	2	0	5	3
6	4	2	0	5	3	1	6

Let Q be one of those quandles from the previous two slides. Then the one variable polynomial in Gröbner basis is of the form

$$p(t) = |Q|^3t^5 - (2|Q|^3 - |Q|^2)t^4 + (|Q|^3 - |Q|^2 - |Q|)t^3 + (2|Q| - 1)t^2 + (1 - |Q|)t,$$

where $|Q|$ is the cardinality of the quandle Q.

Factorization of $p(t)$:

$$p(t) = t \cdot (t-1) \cdot (|Q|t - (|Q| - 1)) \cdot (|Q|t - 1) \cdot (|Q|t + 1)$$

Here are some of the other polynomials in the Gröbner basis needed to find all the solutions of the system of polynomial equations:

$$P(t) = -|Q|^3t^4+(|Q|^3+|Q|(|Q|-2))t^3+(|Q|(|Q|-1)(|Q|-2))t^2r+(|Q|(4-|Q|)-2)t^2+(|Q|-1)(|Q|-2)tr+2(1-|Q|)t$$

$$P(t) = -|Q|^3t^4+(|Q|^3+|Q|(|Q|-2))t^3+(|Q|(|Q|-1)(|Q|-2))t^2z+(|Q|(4-|Q|)-2)t^2+(|Q|-1)(|Q|-2)tz+2(1-|Q|)t$$

$$P(t) = -|Q|^3t^4+(|Q|^3+|Q|(|Q|-2))t^3+(|Q|(|Q|-1)(|Q|-2))t^2y+(|Q|(4-|Q|)-2)t^2+(|Q|-1)(|Q|-2)ty+2(1-|Q|)t$$

Due to computational complexity of computing Gröbner basis when $|Q| \geq 7$, for the rest of the section, we focus on connected quandles of order 5. There are 3 connected quandles of order 5 (up to isomorphism) which we name $Q51$, $Q52$, and $Q53$. We first focus on the quandle rings where the quandles are $Q51$ and $Q52$.

11.1. **The idempotent elements in quandle rings $\mathbb{Z}_p[Q51]$ and $\mathbb{Z}_p[Q52]$.** Here are our multiplication tables for quandles of Q51 and Q52.

$\triangleright$	0	1	2	3	4
0	0	3	4	2	1
1	2	1	3	4	0
2	1	4	2	0	3
3	4	0	1	3	2
4	3	2	0	1	4

$\triangleright$	0	1	2	3	4
0	0	3	4	1	2
1	2	1	0	4	3
2	3	4	2	0	1
3	4	2	1	3	0
4	1	0	3	2	4

Now we need to have the systems of equations to solve for the idempotent elements in quandles Q51 and Q52.

Here are the systems of equations solving for idempotents in Q51 and Q52 respectively

$$\begin{cases} x^2 - x + yz + yt + zr + rt = 0, \\ xr + xt + y^2 - y + zr + zt = 0, \\ xy + xt + yr + z^2 - z + rt = 0, \\ xy + xz + yt + zt + r^2 - r = 0, \\ xz + xr + yz + yr + t^2 - t = 0. \end{cases}$$

$$\begin{cases} x^2 - x + yr + yt + zr + zt = 0, \\ xz + xt + y^2 - y + zr + rt = 0, \\ xy + xr + yt + z^2 - z + rt = 0, \\ xy + xt + yz + zt + r^2 - r = 0, \\ xz + xr + yz + yr + t^2 - t = 0. \end{cases}$$

The two systems of equations have the same Gröbner Basis given below.

$$\{-4t + 9t^2 + 95t^3 - 225t^4 + 125t^5,$$

$$-8t + 12rt - 7t^2 + 60rt^2 + 140t^3 - 125t^4,$$

$$-12r + 12r^2 + 18t - 24rt + 7t^2 - 150t^3 + 125t^4,$$

$$-8t - 7t^2 + 140t^3 - 125t^4 + 12tz + 60t^2z,$$

$$6t - 24rt + 19t^2 - 150t^3 + 125t^4 + 24rz - 24tz,$$

$$18t + 7t^2 - 150t^3 + 125t^4 - 12z - 24tz + 12z^2,$$

$$-8t - 7t^2 + 140t^3 - 125t^4 + 12ty + 60t^2y,$$

$$6t - 24rt + 19t^2 - 150t^3 + 125t^4 + 24ry - 24ty,$$

$$6t + 19t^2 - 150t^3 + 125t^4 - 24ty - 24tz + 24yz,$$

$$18t + 7t^2 - 150t^3 + 125t^4 - 12y - 24ty + 12y^2,$$

$$-12t + 12rt - 13t^2 + 150t^3 - 125t^4 + 12tx + 12ty + 12tz,$$

$$-18t - 7t^2 + 150t^3 - 125t^4 + 24rx + 24ty + 24tz,$$

$$-18t + 24rt - 7t^2 + 150t^3 - 125t^4 + 24ty + 24tz,$$

$$-18t + 24rt - 7t^2 + 150t^3 - 125t^4 + 24ty + 24tz,$$

$$-6t + 24rt - 19t^2 + 150t^3 - 125t^4 - 12x + 12x^2 + 24ty + 24tz\}$$

To find out the idempotent elements we should find the solutions to this system of equations above.

We factoriaze the $-4t + 9t^2 + 95t^3 - 225t^4 + 125t^5$ in order to solve z first.

$$-4t + t^2 + t^3 - 225t^4 + 125t^5$$

$$-4t + 9t^2 + 95t^3 - 225t^4 + 125t^5$$

$$= t(t-1)(5t-4)(5t-1)(t+1)$$

$$t = 0, \quad t = 1, \quad t = \frac{4}{5}, \quad t = \frac{1}{5}, \quad t = -\frac{1}{5}$$

Now we need to plug in the z values to other equations to solve the other variables.

$$-12r + 12r^2 + 18t - 24rt + 7t^2 - 150t^3 + 125t^4 = 0$$

$$t = 0: \quad -12r^2 + 12t = 0 \Rightarrow 12t(t-1) = 0 \Rightarrow t = 1 \text{ or } t = 0$$

$$t = 1: \quad -12r^2 + 36t = 0 \Rightarrow 12t(t-3) \geq 0 \Rightarrow t = 3 \text{ or}$$

$$t = 4/5 : t = -1/5 \text{ or } t = 2.8$$

$$t = 1/5 : t = 1/5 \text{ or } t = 6/5$$

$$t = -1/5 : t = -1/5 \text{ or } t = 4/5$$

Since $-12r + 12r^2 + 18t - 24rt + 7t^2 - 150t^3 + 125t^4 = 0$, $-12y + 12y^2 + 18t - 24yt + 7t^2 - 150t^3 + 125t^4 = 0$ and $-12z + 12z^2 + 18t - 24zt + 7t^2 - 150t^3 + 125t^4 = 0$ are the same type of polynomial. We can get the same value for y and z for the same t.

Now we can use

$$f(t, r) = -8t + 12rt - 7t^2 + 60rt^2 + 140t^3 - 125t^4$$

To check:

$$t = 0, \quad r \geq 1 \quad f(t, r) = 0 \quad \checkmark$$

$$r = 0 \quad f(t, r) = 0 \quad \checkmark$$

$$t = 1, \quad r \geq 0$$

$$r = 1 \quad f(t, r) = -8 + 12 - 7 + 60 - 128 = 0 \quad \checkmark$$

$$f(t, r) = -8 + 12 - 7 + 60 + 14 - 128 = 72 \quad \times$$

$$t = \frac{4}{5}, \quad r = -\frac{1}{5} \quad f(t, r) = 0 \checkmark$$

$$r = 2.8 \quad f(t, r) = 144 \quad \times$$

$$t = \frac{1}{5}, \quad r = \frac{1}{5} \quad f(t, r) = 0 \quad \checkmark$$

$$r = 1.2 \quad f(t, r) = 48 \quad \times$$

Using the same way, we can also rule out some values for y and z. Now the values for t, r, z, y are in the table below.

t	r	y	z
0	0	0	0
0	0	0	1
0	0	1	0
0	0	1	1
0	1	0	0
0	1	0	1
0	1	1	0
0	1	1	1
1	0	0	0
$\frac{4}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$
$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$
$-\frac{1}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$
$-\frac{1}{5}$	$\frac{4}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$
$-\frac{1}{5}$	$\frac{4}{5}$	$\frac{4}{5}$	$-\frac{1}{5}$
$-\frac{1}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	$\frac{4}{5}$
$-\frac{1}{5}$	$-\frac{1}{5}$	$\frac{4}{5}$	$-\frac{1}{5}$
$-\frac{1}{5}$	$-\frac{1}{5}$	$\frac{4}{5}$	$\frac{4}{5}$
$-\frac{1}{5}$	$\frac{4}{5}$	$\frac{4}{5}$	$\frac{4}{5}$
$-\frac{1}{5}$	$-\frac{4}{5}$	$-\frac{1}{5}$	$\frac{4}{5}$

Now, we still can rule out some of these values by plug the (t, r, y, z) above into

$$f_1 = 6t - 24rt + 19t^2 - 150t^3 + 125t^4 + 24rz - 24tz,$$

$$f_2 = 6t - 24rt + 19t^2 - 150t^3 + 125t^4 + 24ry - 24ty,$$

and

$$f_3 = 6t + 19t^2 - 150t^3 + 125t^4 - 24ty - 24tz + 24yz.$$

t	r	y	z	f_1	f_2	f_3
0	0	0	0	✓	✓	✓
0	0	0	1	✓	✓	✓
0	0	1	0	✓	✓	✓
0	0	1	1	✓	×	✓
0	1	1	0	×	×	×
0	1	1	1	×	✓	✓
0	1	0	0	✓	✓	✓
1	0	0	0	✓	✓	✓
0	1	0	1	✓	✓	×
$\frac{4}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	✓	✓	✓
$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	✓	✓	✓
$-\frac{1}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	✓	✓	✓
$-\frac{1}{5}$	$\frac{4}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	✓	✓	✓
$-\frac{1}{5}$	$\frac{4}{5}$	$-\frac{4}{5}$	$-\frac{1}{5}$	×	✓	✓
$-\frac{1}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	$\frac{4}{5}$	✓	✓	✓
$-\frac{1}{5}$	$-\frac{1}{5}$	$\frac{4}{5}$	$-\frac{1}{5}$	✓	✓	✓
$-\frac{1}{5}$	$-\frac{1}{5}$	$\frac{4}{5}$	$\frac{4}{5}$	✓	×	✓
$-\frac{1}{5}$	$\frac{4}{5}$	$\frac{4}{5}$	$\frac{4}{5}$	×	×	×
$-\frac{1}{5}$	$-\frac{4}{5}$	$-\frac{1}{5}$	$\frac{4}{5}$	✓	✓	×

Next we will use the (t, r, z, y) values above and plug them into

$$-6t + 24rt - 19t^2 + 150t^3 - 125t^4 - 12x + 12x^2 + 24ty + 24tz$$

to solve for x.

t	r	y	z	x
0	0	0	0	$1, 0$
0	0	0	1	$1, 0$
0	0	1	0	$1, 0$
0	1	0	0	$1, 0$
$\frac{4}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}, \frac{6}{5}$
$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}, \frac{4}{5}$
$-\frac{1}{5}$	$\frac{4}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}, \frac{6}{5}$
$-\frac{1}{5}$	$-\frac{1}{5}$	$-\frac{4}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}, \frac{6}{5}$
$-\frac{1}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	$\frac{4}{5}$	$-\frac{1}{5}, \frac{6}{5}$
$-\frac{1}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	$\frac{4}{5}$	$\frac{6}{5}, \frac{1}{5}$

Now we let

$$f_4 = -18t - 7t^2 + 150t^3 - 125t^4 + 24rx + 24ty + 24tz,$$

$$f_5 = -18t + 24rt - 7t^2 + 150t^3 - 125t^4 + 24ty + 24tz,$$

and

$$f_6 = -18t + 24rt - 7t^2 + 150t^3 - 125t^4 + 24ty + 24tz,$$

and use the 3 equations to check all (t, r, z, y, x) values above.

t	r	y	z	x	f_4	f_5	f_6
0	0	0	0	1	✓	✓	✓
0	0	0	0	0	✓	✓	✓
0	0	0	1	1	✓	×	✓
0	0	0	1	0	✓	✓	✓
0	0	1	0	1	✓	✓	×
0	0	1	0	0	✓	✓	✓
0	1	0	0	1	×	✓	✓
0	1	0	0	0	✓	✓	✓
$\frac{4}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	✓	✓	✓
$\frac{4}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	$\frac{6}{5}$	×	×	×
$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	✓	✓	✓
$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{4}{5}$	×	×	×
$-\frac{1}{5}$	$\frac{4}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	✓	✓	✓
$-\frac{1}{5}$	$\frac{4}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	$\frac{6}{5}$	×	×	×
$-\frac{1}{5}$	$-\frac{1}{5}$	$-\frac{4}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	✓	✓	✓
$-\frac{1}{5}$	$-\frac{1}{5}$	$-\frac{4}{5}$	$-\frac{1}{5}$	$\frac{6}{5}$	×	×	×
$-\frac{1}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	$\frac{4}{5}$	$-\frac{1}{5}$	✓	✓	✓
$-\frac{1}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	$\frac{4}{5}$	$\frac{6}{5}$	×	×	×
$-\frac{1}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	$\frac{1}{5}$	×	×	×
$-\frac{1}{5}$	$-\frac{1}{5}$	$-\frac{1}{5}$	$\frac{4}{5}$	$\frac{1}{5}$	✓	✓	✓

The idempotents of quandle rings $\mathbb{Z}_p[Q51]$ and $\mathbb{Z}_p[Q52]$ are

$$(0,0,0,0,0)$$

$$\left(\frac{1}{5},\frac{1}{5},\frac{1}{5},\frac{1}{5},\frac{1}{5}\right)$$

$$\Big(\frac{4}{5},-\frac{1}{5},-\frac{1}{5},-\frac{1}{5},-\frac{1}{5}\Big),\Big(-\frac{1}{5},\frac{4}{5},-\frac{1}{5},-\frac{1}{5},-\frac{1}{5}\Big),$$
$$\Big(-\frac{1}{5},-\frac{1}{5},-\frac{4}{5},-\frac{1}{5},-\frac{1}{5}\Big),\Big(-\frac{1}{5},-\frac{1}{5},-\frac{1}{5},\frac{4}{5},-\frac{1}{5}\Big),\Big(-\frac{1}{5},-\frac{1}{5},-\frac{1}{5},-\frac{1}{5},\frac{4}{5}\Big)$$
$$(1,0,0,0,0),(0,1,0,0,0),(0,0,1,0,0),(0,0,0,1,0),(0,0,0,0,1)$$

11.2. **Number of idempotents in quandle ring $\mathbb{Z}_p[Q53]$.** $Q53$ is the symmetric connected quandle of order 5.

$\triangleright$	0	1	2	3	4
0	0	3	1	4	2
1	3	1	4	2	0
2	1	4	2	0	3
3	4	2	0	3	1
4	2	0	3	1	4

The number of idempotents in the quandle ring $\mathbb{Z}_p[Q53]$ for different p values is given in the following table.

p	**Quandle**	**Number of Idempotents**
2	Q 53	32
3	Q 53	12
5	Q 53	6
$(\frac{p}{15}) = 1$	Q 53	32
$(\frac{p}{15})$ = -1	Q 53	12

References

[Adams(2004)] Colin C. Adams, The knot book. An elementary introduction to the mathematical theory of knots. *Revised reprint of the 1994 original American Mathematical Society*, Providence, RI, 2004. xiv+307 pp.

[BPS(2019)] Valeriy G. Bardakov, Inder Bir S. Passi, and Mahender Singh, Quandle rings. *J. Algebra Appl.* 18 (2019), no. 8, 1950157, 23 pp.

[Bardakov, Passi, and Singh(2022)] Valeriy G. Bardakov, Inder Bir S. Passi, and Mahender Singh, Zero-divisors and idempotents in quandle rings, *Osaka Journal of Mathematics*, vol. 59, no. 3, 2022, pp. 611–637.

[Elhamdadi et al.(2022)] Mohamed Elhamdadi, Brandon Nunez, Mahender Singh, and Dipali Swain, Idempotents, free products and quandle coverings, *arXiv preprint*, arXiv:2204.11288v3, 2022. https://arxiv.org/abs/2204.11288

[Elhamdadi et al.(2019)] Mohamed Elhamdadi, Neranga Fernando, and Boris Tsvelikhovskiy, Ring theoretic aspects of quandles, *Journal of Algebra*, vol. 526, 2019, pp. 166–187. https://doi.org/10.1016/j.jalgebra.2019.02.011

[Elhamdadi and Swain(2024)] Mohamed Elhamdadi and Dipali Swain, State sum invariants of knots from idempotents in quandle rings, *arXiv preprint*, arXiv:2402.14661v2, 2024. https://arxiv.org/abs/2402.14661v2

[Elhamdadi and Nelson(2015)] Mohamed Elhamdadi and Sam Nelson, *Quandles: An Introduction to the Algebra of Knots*, Student Mathematical Library, Vol. 74, American Mathematical Society, Providence, RI, 2015.

[Ho and Neslon] Benita Ho and Sam Nelson, *Matrices and finite quandles*, Homology Homotopy Appl. 7, No. 1, 197 – 208 (2005).

[Gallian(2017)] Joseph A. Gallian, *Contemporary Abstract Algebra*, 9th ed., Cengage Learning, Boston, MA, 2017.

[Joyce (1982)] David Joyce, A classifying invariant of knots, the knot quandle, *J. Pure Appl. Algebra* 23 (1982), no. 1, 37–65.

[Livingston and Moore(2020)] C. Livingston and A. H. Moore, KnotInfo: Table of Knot Invariants, web site, 2020. Available at: `http://www.indiana.edu/~knotinfo`

[Macquarrie(2011)] Jennifer Macquarrie, Automorphism Groups of Quandles (2011). *USF Tampa Graduate Theses and Dissertations.*

[Matveev (1982)] S.V. Matveev, Distributive groupoids in knot theory, Mat. Sb. (N.S.) 119(161) (1) (1982) 78–88, 160 (in Russian). MR672410 (84e:57008).

[Neslon (2008)] Sam Nelson, *A polynomial invariant of finite quandles*, J. Algebra Appl. 7, No. 2, 263-273 (2008).

Appendix

Groups. A *group* is a set G with a binary operation $\cdot$ that combines any two elements a and b to form another element denoted $a \cdot b$. The set and operation, $(G, \cdot)$, must satisfy four fundamental properties known as the group axioms:

(1) **Closure:** For all $a, b \in G$, the result of the operation $a \cdot b$ is also in G.

$$\forall a, b \in G,\ a \cdot b \in G$$

(2) **Associativity:** For all $a, b, c \in G$, the equation $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ holds.

$$\forall a, b, c \in G,\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

(3) **Identity Element:** There exists an element $e \in G$ such that for every element $a \in G$, the equation $e \cdot a = a \cdot e = a$ holds.

$$\exists e \in G \text{ such that } \forall a \in G,\ e \cdot a = a \cdot e = a$$

(4) **Inverse Element:** For each $a \in G$, there exists an element $b \in G$ such that $a \cdot b = b \cdot a = e$, where e is the identity element.

$$\forall a \in G,\ \exists b \in G \text{ such that } a \cdot b = b \cdot a = e$$

Dihedral Groups. The dihedral group D_n is an non-abelian group $n \in \mathbb{Z}$ which contain the group of symmetries of a regular polygon with n sides. This is a group with order $2n$ includes n rotations and n reflections. The group can be presented in terms of

generators and relations as follows:

$$D_n = \langle r, s \mid r^n = s^2 = 1,\ srs = r^{-1} \rangle$$

where r represents a rotation by $\frac{360^\circ}{n}$ (or $\frac{2\pi}{n}$ radians), and s represents a reflection across a line that passes through one vertex and the center of the polygon.

Rings. A *Ring* is a set R equipped with two binary operations: addition $(+)$ and multiplication $(\cdot)$ such that:

(1) $(R, +)$ is an abelian group:

(2) Closure: For all $a, b \in R$, $a + b \in R$

(3) Associativity: $(a + b) + c = a + (b + c)$

(4) Identity: There exists $0 \in R$ such that $a + 0 = a$

(5) Inverses: For every $a \in R$, there exists $-a \in R$ such that $a + (-a) = 0$

(6) (iv) Commutativity: $a + b = b + a$

(7) Multiplication is associative: For all $a, b, c \in R$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(8) Distributive laws hold:

- Left distributive: $a \cdot (b + c) = a \cdot b + a \cdot c$
- Right distributive: $(a + b) \cdot c = a \cdot c + b \cdot c$

If the ring also satisfies:

- Multiplicative identity: There exists $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$

then it is called a *ring with unity* or a *unital ring.*

If multiplication is also commutative $(a \cdot b = b \cdot a)$, then it is called a *commutative ring.*

Example 11.1. *The set of integers $\mathbb{Z}$ with the usual addition and multiplication is a commutative ring with unity.*

Legendre symbol. Let p denote an odd prime. Then the Legendre symbol $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p, \\ 0 & \text{if } a \text{ is a multiple of } p. \end{cases}$$

Jacobi symbol. Let $n \in \mathbb{Z}^+$, and let

$$n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$$

be its prime factorization.

Let $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$. Then the *Jacobi symbol* $\left(\frac{a}{n}\right)$ is defined by:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \cdots \left(\frac{a}{p_m}\right)^{e_m}$$

where the symbols on the right-hand side are Legendre symbols.