Congruences in Racks and Quandles

A thesis presented in partial fulfilment
of the requirements for the degree of

Doctor of Philosophy
in
Mathematics

at Massey University, Manawatū Campus
Palmerston North
New Zealand

Wayne John Burrows

2022

Dedicated to my parents:

Walter David (Dave) Burrows;

Maureen Elsie Burrows (née Oliver).

Abstract

Racks and quandles are related algebraic structures based on axioms of invertibility and self-distributivity, and in the case of quandles, an additional idempotence axiom — thus every quandle is a rack. They have practical application as the three quandle axioms algebraically encode the Reidemeister moves of knot theory. However, racks and quandles are interesting and worthy of study in their own right and that is what we do here. Congruences are a means of distilling patterns of behaviour within algebraic structures. They allow us to form a quotient that gives us a coarser view of the structure from which we can discern interesting properties. Congruences need to respect the operations in the algebraic structure.

Racks, although often defined in terms of only one binary operation, necessarily, as a result of the invertibility axiom, have two binary operations — a primary rack operation and an inverse rack operation. We have a rack in the quotient only when the congruence respects both operations. A congruence that respects both operations we call a rack congruence or a quandle congruence. Congruences defined in terms of only one of the binary operations may not preserve the rack structure in the quotient. This raises the question of whether congruences that respect only one rack operation — half congruences — can exist. We show they can by constructing examples of half congruences that do not induce a rack in the quotient.

For weighted average quandles on $\mathbb{Q}$ we completely characterise congruences in terms of certain subgroups of $\mathbb{Q}$. Depending on the weight, congruences can exhibit one of three possible behaviours. Weighted average quandles are a special case of the more general Alexander quandle. For Alexander quandles, we characterise when a congruence induces an Alexander quandle in the quotient. In weighted average quandles every congruence comes from a subgroup of $\mathbb{Q}$. In Alexander quandles, there are additional congruences that do not come from a subgroup. We give examples of congruences that exhibit that more complex behaviour.

Acknowledgements

Firstly, I would like to thank Massey University for giving me the opportunity to study for this Doctor of Philosophy. I have been supported in part through a Massey University Vice Chancellor's Scholarship and in the early stages of my study through employment as a part-time Graduate Assistant in the Department of Mathematics at Massey University.

In addition, the support from Massey University staff has been above and beyond what might have been expected in my case. I am particularly thankful for the kindness and support that I have received from Professor Kathryn Stowell and Associate Professor Catherine Whitby who were Directors of Post-graduate Studies, and more recently, from Associate Professor Anuradha Mathrani who is now the Postgraduate Lead, and Associate Professor Winston Sweetman, the Postgraduate Coordinator for Mathematics, in various schools and colleges throughout Massey University — I can't keep up with the restructures. I have also be supported by two Postgraduate Administrators, Ann Truter and Lynh Mills. I also had incredibly good support from Professor Tracy Riley, Dean, Research at Massey University.

I have enjoyed support, which I have appreciated from all of the lecturing staff in the Department of Mathematics over the time that I have been studying at Massey University which goes back to 2012.

Particular thanks must go to my associate supervisors, Dr Richard Brown (until 2020) and Distinguished Professor Robert McLachlan (since 2020) who have helped guide me through this process. My primary supervisor has been Dr Christopher Tuffley who has been extraordinarily helpful both mathematically and with patience and professionalism as I have worked through outside difficulties to complete this work. I cannot thank him enough for his efforts.

As alluded to, whilst negotiating this course of study, I have had to deal with life which has thrown me some significant curve balls. I would not be here today without the care, support, and expertise of a number of people in the wider community. They include Dr Jade Robertson and the other staff: doctors; nurses; and administrators at Massey University Student Health and Counselling. All of the staff there have treated me well. Dr Robertson has been incredibly supportive and professional and I cannot thank her enough for her care. Mr David Coomber, Senior Professional Clinician — Counselling and Guidance also offered invaluable support. In addition, Philip Straker, Counsellor at Manline Manawatū, has supported me on a regular basis. Without his invaluable support I am not sure how I would have survived over the past few years.

Another haven, that has been especially helpful to me during my study, has been the Massey University Recreation Centre. The staff there has been fantastic and the facilities are great. I would especially like to acknowledge the Les Mills Body Balance Instructors — sorry I didn't keep coming to your classes.

Finally, I would like to thank my family, friends, and neighbours. I will not name any of you — for fear of missing someone out or embarrassing someone. Your support has been big and small, direct and indirect, and knowing and unknowing. I am forever grateful.

My main passion in life is playing bridge — it has always been great to get away from the stress of life to play some cards. It is great when life and study have been so stressful to retreat and lose myself in the world of pasteboards, finesses, coups, squeezes, slams, games, and part-scores with great partners, fantastic team mates, and against friends who for that moment have been opponents.

To my closest friends and family, I can say no more than “thank you”.

Contents

List of Figures

Chapter 1

Introduction

1.1 Introduction to racks and quandles

This is a study of algebraic structures known as racks and quandles. For our purposes an algebraic structure is a set with one or more operations. In racks and quandles there are two binary operations. The binary operations obey two axioms in the case of a rack and three axioms in the case of a quandle. A quandle is, in fact, a rack with the constraint of an additional axiom. The axioms can be thought of as identities that are satisfied by the binary operations. The axioms will be formally given later in Definition 2.1.1. In summary, the axioms on a set X with a binary operation, $*$, are:

1. Idempotence: For all $x \in X$, $x * x = x$.
2. Invertibility: For all $y, z \in X$, the equation $x * y = z$ has a unique

solution, $x \in X$.

3. Self-distributivity: For all $x, y, z \in X$ we have the following distributivity identity $(x * y) * z = (x * z) * (y * z)$.

Note the axioms are in terms of only one binary operation but we will see that as a consequence of the second axiom there is necessarily a related second binary operation. Thus every rack or quandle can be viewed as a set together with two binary operations.

A quandle obeys all three axioms. A rack obeys the latter two. We will also encounter structures that obey just the third axiom, which are called shelves, and structures that just obey the first and third axioms, which are called spindles.

We will be interested in congruences in racks and quandles. For our purposes a congruence is an equivalence relation on our set that respects one or both binary operations. From a congruence we will be interested in forming quotients. A quotient gives us a coarser view of the original structure from which we can deduce common properties. When a congruence respects only one operation the quotient formed loses some of the structure of the rack or quandle from which it originated. Effectively, the loss of structure is manifested by the loss one of the identities or axioms, specifically the invertibility axiom, that the rack or quandle obeyed.

When there is loss of the invertibility axiom, the algebraic structure of a resulting quotient is known as either a shelf or a spindle depending on whether it emanates from a rack or a quandle respectively. The quotient in those cases is an algebraic structure with only one binary operation that does not satisfy the invertibility axiom.

1.2 History

Quandles were independently introduced by Joyce [16] in his PhD Thesis, *An Algebraic Approach to Symmetry with Applications to Knot Theory* (1979) and by Matveev [19], using the descriptive term "distributive groupoids", in a Russian paper entitled *Distributive Groupoids in Knot Theory* (1982). Their association with knot theory is because the quandle axioms can be motivated by the Reidemeister moves of knot theory. Effectively, the three quandle axioms are an algebraic encoding of the three Reidemeister moves which are used to determine knot invariants. We will discuss this further in Section 1.3.

There had been earlier work on racks — an algebraic structure satisfying only the second and third quandle axioms, by Conway and Wraith [10] (1959) in unpublished correspondence. Conway coined the name **Wrack** as a play on Wraith's name and because this is the "wrack and ruin" of a group when everything except conjugation is thrown away. Later the "W" was dropped and the spelling **rack** became standard. We will discuss racks in further detail in Section 2.3.2.

Wraith [31] himself describes first encountering these structures as a schoolboy and he gave them the name **sequentials**. First he noticed that his sequentials obeyed the rule[1] $(xy)y = x$, which is an involutory property — see Definition 2.2.34 — which is a special case of invertibility where the inverse is obtained by acting on x twice by the same element y. Wraith then discovered that sequentials obeyed idempotence, $xx = x$ and right self-distributivity $(xy)z = (xz)(yz)$. Many years later Fenn asked him if he had seen the self-distributivity law and when Wraith explained his work with Conway, Fenn saw that he needed a more general invertibility axiom than that afforded by the involutory rule. Fenn called the more general structures **racks** so as to distinguish them from wracks which were what are now known as involutory quandles.

Prior to that work, Takasaki [29] (1943) had worked with essentially the same algebraic structure that he called a **kei**. A kei satisfies the quandle axioms with the additional condition that $(x \triangleright y) \triangleright y = x$ and so is identical to what Wraith called a sequential, and according to Fenn, was called a wrack. That is, a kei is an involutary quandle as defined in Definition 2.2.34. Takasaki's work was built on earlier work with rack-like structures by Thomsen [30].

Burstin and Mayer [8] (1929) studied finite distributive groups (Distributive Gruppen von endlicher Ordnung.) An English translation of their work has been made by Ansgar Wenzel [9] and is available online. Burstin and Mayer defined axioms similar to the second and third quandle axioms but that were two sided in nature. That is, they required unique solutions to both: $a \cdot x = b$ and $y \cdot a = b$. This is a classical axiom of group theory — where left and right inverses exist and in the case of a classical group are equal. In racks and

---

[1] Here Wraith used juxtaposition rather than explicitly indicating a set operation.

quandles we do not have inverse elements but rather the invertibility of the binary operation. Similarly, Burstin and Mayer required the distributivity axiom to be satisfied both from the left and the right. That is,

$$(a \cdot b) \cdot c = (a \cdot c) \cdot (b \cdot c) \text{ and } c \cdot (a \cdot b) = (c \cdot a) \cdot (c \cdot b).$$

Burstin and Mayer do not state idempotence as an axiom but it is a consequence of the two-sided invertibility and distributivity axioms. We will show this later in Section 2.2.30.

Peirce [24] (1880) had done earlier work on self-distributive algebra in the context of the algebra of logic. More recently Przytycki [25] (2011) has surveyed ideas from self-distributive groups including a discussion of the nomenclature used by Crans below.

Subsequently, Crans [11] worked with structures that did not require the invertibility axioms of racks. Crans coined the term **shelf** as being part of a rack. When a shelf also obeyed idempotence she called the structure a **spindle**. We use Crans' terminology in this regard.

1.3 Reidemeister moves

In 1927 Reidemeister [26] determined that two knot diagrams represent the same knot if and only if they can be transformed from one to the other by a sequence made up of three elementary moves, together with planar isotopy. These three moves are known as the Reidemeister moves and are illustrated

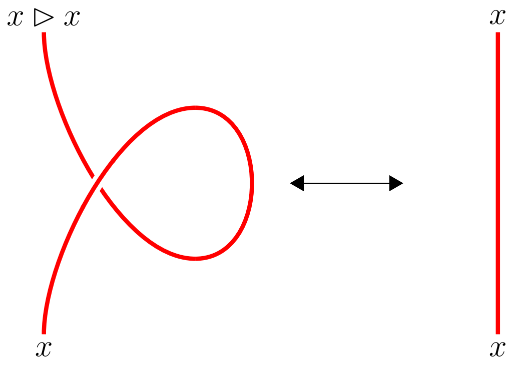

Figure 1.1: Reidemeister I

in Figures 1.1, 1.2 and 1.3.

The three quandle axioms correspond to the three Reidemeister moves. The first Reidemeister move, Figure 1.1, is a loop where a portion of a knot loops under itself. This loop can be untwisted to form an unknotted segment. Here a strand going 'under' itself corresponds to the quandle operation $x \triangleright x$, which in this context could be read as "x under x", which is equivalent to a single strand x and so gives us the idempotence axiom.

The second Reidemeister move, Figure 1.2, is where a strand crosses under (or over) and then recrosses under (respectively over) another strand. By sliding the top strand over we can remove both crossings to have two single strands. Here we need to think of the strands as having an orientation, using a right hand rule, so that one crossing has the opposite orientation to the other. One strand goes under ($\triangleright$), the other, and then goes back under ($\triangleleft$). We can encode from this the second quandle axiom in its alternative form, which we will see later in Axiom Q2a.

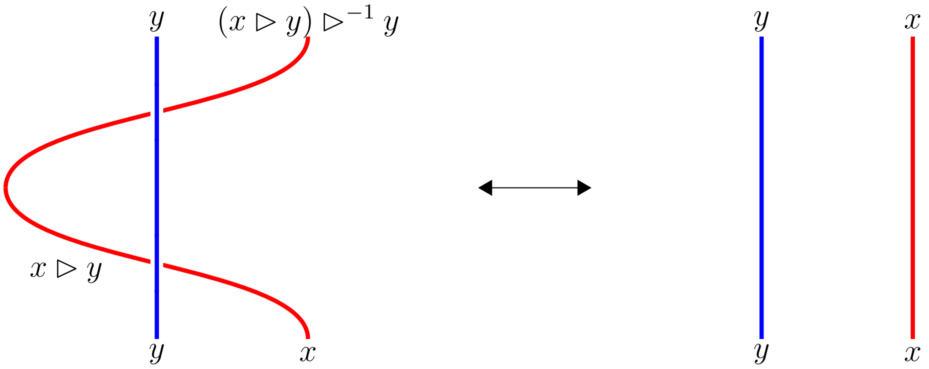

Figure 1.2: Reidemeister II

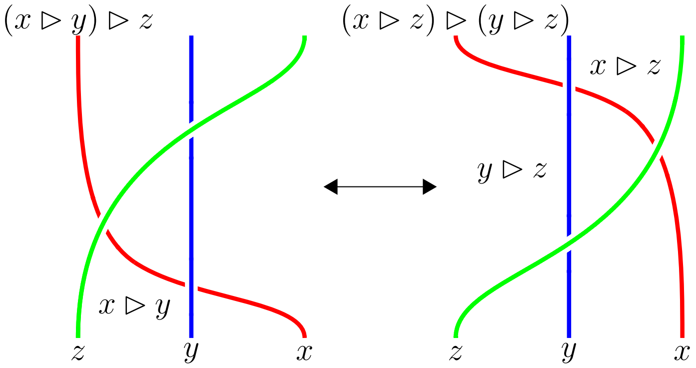

Figure 1.3: Reidemeister III

The third Reidemeister move, Figure 1.3, is where one strand passes under two other strands, which also cross. We can slide the former two crossings so that they are above or below the later crossing. From this diagram we see that strand x going ‘under’ strand y and then going ‘under’ strand z is equivalent to strand x going ‘under’ strand z, and then this strand going ‘under’ the result of strand y going ‘under’ strand z, which is encoded in the self-distributivity axiom.

The quandle axioms algebraically encode the Reidemeister moves. As such, the Reidemeister moves are motivational for studying quandles. Quandles can be used to give an invariant on knots.

1.4 Summary

We will begin by summarising the work in this thesis. The main work is an investigations of congruences in racks and quandles.[2] In particular, we look at situations in which a congruence respects one of the rack operations but not the other. We call those congruences half congruences. We prove the existence of half congruences by giving examples where a congruence only respects only one of the quandle operations. We have a more in depth look at a particular type of quandle called an Alexander quandle and more particularly, two special cases of Alexander quandles — the averaging quandle and weighted average quandles on $\mathbb{Q}$. In those cases, we characterise the conditions under which a congruence respects only one or both quandle operations. In the final chapter, we look at the more general case of Alexander quandles. We characterise when the quotient is also an Alexander quandle and we give examples of half congruences. Those examples show that we can see more complex behaviour than what we saw in the weighted average quandles.

That is an overview, now we will give a little more detail chapter by chapter.

---

[2] Since every quandle is a rack, with an additional axiom — idempotence — satisfied, we will frequently use the term rack in an inclusive sense. That is, rack will not preclude the possibility that the rack is a quandle.

Summary — Chapter Two: Preliminaries

In Chapter 2 we set out the basic definitions that we will use, and prove some of the basic properties of racks and quandles. Many of these properties are likely to be well-known but we present our own proofs.

There are alternative ways to view the quandle axioms. Those are discussed. In particular, the invertibility axiom can be viewed as defining a permutation or symmetry, or an automorphic function on a rack. This view is often helpful when investigating the properties of racks. It is a consequence of the invertibility axiom that there is necessarily a second rack operation. We discuss the inverse rack operation.

In the literature racks and quandles have been represented by a range of terminologies and notations. Following on from the brief discussion of terminology in Chapter 1 we indicate the terminologies and notations that we will adopt. Since racks are in general not associative we also give precedence conventions that we will use in resolving ambiguities.

One key notation that we primarily, but not exclusively, use with racks and quandles is that we use the symbols $\triangleright$ and $\triangleleft$ to represent the rack operation and the inverse rack operation respectively.

We give some introductory examples of racks and quandles. Generally, these will be well-known. Of course, we introduce the examples of an averaging quandle (Example 2.2.28), weighted average quandles (Example 2.2.29), an Alexander quandles (Definition 2.2.20) which will be used in more detail later in the thesis. Alexander quandles come from $\mathbb{Z}[t, t^{-1}]$ modules with the quandle operation given by $x \triangleright y = tx + (1 - t)y$.

Another useful example is that any bijection on a set can be used to define a rack operation on the set. We use that example later in the thesis to construct examples to illustrate, in particular half congruences.

We show that whenever we have a rack $(R, \triangleright)$ that n-fold application of the rack operation also defines a quandle, that is, $(R, \triangleright^n)$ is also a rack. This result is likely to be known but we provide a proof. In the proof there is a result that will have wider use, in that we proved a more general distributivity identity that $(x \triangleright^m y) \triangleright^n z = (x \triangleright^n z) \triangleright^m (y \triangleright^n z)$. Moreover, if negative powers are defined via the inverse quandle operation the identity extends over the range $m, n \in \mathbb{Z}$.

Related to an Alexander quandle is an Alexander spindle. Dehornoy [12] claims that an Alexander spindle is a quandle if and only if $t \in R$, a ring, is invertible, which would allow the solution of the equation in the quandle operation $x \triangleright a = tx + (1 - t)a = b$. We provide a counterexample, where t is not in invertible in the ring but acts invertibly and the Alexander spindle is a quandle. We also provide a proof that it is both necessary and sufficient for t to act invertibly in order for an Alexander spindle to be a quandle.

The concept of a dual rack, in which the two rack operations are interchanged is well-known. It seems to be well known that the dual rack is a rack but it is sometimes stated without proof or reference. We provide a proof that a dual rack is a rack.

Joyce [16] stated but did not prove some mixed operation distributivity identities. These are similar to the self-distributivity axiom but involving both the rack operation and the inverse rack operation:

$$(x \triangleright y) \triangleleft z = (x \triangleleft z) \triangleright (y \triangleleft z),$$

and

$$(x \triangleleft y) \triangleright z = (x \triangleright z) \triangleleft (y \triangleright z).$$

We prove these identities and their analogues with m-fold and n-fold rack operations.

Another well-known result is that for a subset of a rack to be a rack, in other words a subrack, it is necessary for the subset to be closed under both rack operations. There is a little confusion in the literature with some authors claiming that closure under the rack operation is sufficient. Although, elsewhere, for example [2, 17] there are known examples of subsets that are closed under the rack operation but that are not racks. We provide a proof of the necessity for closure under both rack operations. We also provide some common situations in which closure under the rack operation implies closure under the inverse rack operation so that only one operation would need to be checked.

Nelson and Wong [22] show that the intersection of two quandles is a subquandle and they introduce a concept of Q-complement, that the complement of a subquandle is also a subquandle. They show that the intersection of Q-complemented subquandles is itself Q-complemented. Their proof is valid for finite subquandles but is easily extended to infinite subquandles and we show that.

Summary — Chapter Three: Congruences and Quotients

In Chapter 3 we define and describe the related concepts of congruences, quotients, and homomorphisms as they will be used in this thesis. There are close parallels with the corresponding theory for groups and rings, and many of the results in this chapter are likely to be known or at least assumed to be true. However, a key result Theorem 3.2.7 is sometimes stated incorrectly and without proof, so we present proofs of these results in order to provide a firm foundation for what we do next in Chapters 4–6.

We give a meta-definition of congruence in Definition 3.1.1 that a congruence is any equivalence relation on a set that respects an n-ary operation on that set. In the context of racks and quandles this leads to the definition of $\triangleright$-congruences and $\triangleleft$-congruences, which respect one of the operations but not necessarily the other, and we further define rack congruences and quandle congruences as congruences that respect both operations. Finally we define a half congruence which is a congruence that respects one but not the other rack operation. We will be highlighting that such half congruences exist in Chapter 4 so it is important that we define each of these terms.

Some authors have claimed that a congruence that respects the rack operation can be used to define a rack on the quotient. We show in Theorem

3.2.7 that a rack on the quotient is induced when we have a rack congruence, which respects both operations, and we show in Lemma 3.2.6 that in that case the operations are well defined on the congruences classes in the quotient. We show a similar result for quandles in Theorem 3.2.9 that a quandle congruence induces a quandle in the quotient.

We show that the image of a homomorphism from $R \to R_*$ is a subrack of R_*. Finally, in Chapter 3 we prove an isomorphism theorem that shows that we can define an equivalence relation based on a rack homomorphism, $\phi : R \to R_*$, where $x \sim y$ if and only if $\phi(x) = \phi(y)$, and then the image of ϕ is a subrack of the R_*; the equivalence relation is a rack congruence; and the function $\psi([x]) = \phi(x)$ is an isomorphism from the quotient to the image of the homomorphism, that is: $R/\sim \to \phi(R)$. This isomorphism theorem is a rack and quandle version of the first isomorphism theorem for groups and rings.

Summary — Chapter Four: Existence of Half Congruences

In Chapter 4 we prove the existence of half congruences by way of examples. Given that we have shown in Chapter 3 that a rack congruence and a quandle congruence induce a rack and a quandle in the quotient respectively, a natural question that arises is whether or not a half congruence can exist. The first result we show in Theorem 4.1.2 is that for a rack a congruence is a half congruence if and only if the quotient is not a rack. This leaves open the possibility that when we have a $\triangleright$-congruence, a congruence that only respects the primary rack operation, that the quotient may not be a rack. In Theorem 4.2.3, we give a sufficient condition on the rack operation that a $\triangleright$-congruence will induce a rack in the quotient. The condition is that for each y in the rack there exists some $n \in \mathbb{N}$ such that $x \triangleright^n y = \big((x \triangleright y) \triangleright y \cdots\big) \triangleright y = x$ for all x in the rack. That is, when there is some cyclic behaviour in the repeated application of the rack operation, we necessarily get a rack in the quotient. This property is always present in a finite rack and we show that as a corollary of this theorem.

We then give some examples of $\triangleright$-congruences that do not induce a rack in the quotient, thereby proving the existence of half congruences. In Example 4.3.1 we have a rack on $\mathbb{Z} \times \mathbb{Z}$ in which the rack operation maps two congruence classes into one congruence class. This necessarily means that when we try to solve the equation $[x]\triangleright[y] = [z]$ in the quotient that we lose uniqueness and thus the quotient is not a rack.

In Example 4.3.3 we present an example based on what we define as bi-infinite binary Cantor sequences. This example is on a rack that is not a quandle. The congruence is based on the positively indexed portions of the sequence being identical. The rack operations are left and right shifts of the sequence by one place. In the quotient, there are equations that do not have unique solutions and therefore the quotient is not a rack.

In Example 4.3.4 we adapt Example 4.3.3 to produce an example that is a quandle and has a similar behaviour where there are equations in the quotient that do not have unique solutions and therefore the quotient is not a quandle.

Another example that is based on the same principle but with a decimal shift on the real numbers is given in Example 4.3.7.

The final example, Example 4.3.8 is a countably infinite example that we show has the property that it has a finite presentation.

Summary — Chapter Five: Averaging Quandles on $\mathbb{Q}$

In Chapter 5 we investigate averaging quandles. We work in $\mathbb{Q}$ and begin with an investigation of a quandle based on the simple arithmetic mean of two elements, which is called the averaging quandle with the quandle operation defined by $x \triangleright y = \frac{x+y}{2}$. This is then generalised to a weighted average of two elements, $x \triangleright y = tx + (1-t)y$ for some weight $t \neq 0$.

In the simple average case, it is shown that the congruence classes are of two forms, either: singletons; or sets that are dense in $\mathbb{Q}$. We build up dense sets by showing that whenever we have two elements in a congruence class the arithmetic mean of those elements is also in the congruence class. By repeated application of this principle we show the congruence class is dense on the interval between the two elements. This interval can be extended in contiguous steps on either side indefinitely thus building up density in $\mathbb{Q}$.

In addition we show in Theorem 5.1.13 that the set of differences, $D_x = \{y - x : x \sim y\}$, is independent of x and is equal to the congruence class of 0. From which we were able to deduce in Theorem 5.1.14 that the set of differences which is equal to $[0]$ is a subgroup of $\mathbb{Q}$ and in Theorem 5.1.15 that all congruence classes are cosets of the form $r + [0]$, where $r \in \mathbb{Q}$ is any rational number and [0] is the congruence class of 0.

In Theorem 5.1.16 we see this set of differences for a $\triangleright$-congruence is closed under multiplication by $\frac{1}{2}$. Reciprocally, if there is a subgroup of $\mathbb{Q}$ that is closed under multiplication by $\frac{1}{2}$ we show that we can define a $\triangleright$-congruence.

For the quandle based on the arithmetic mean, in Theorem 5.1.17, we show that every $\triangleright$-congruence implies we have a quandle congruence, that is, the congruence respects the inverse quandle operation. Interestingly, this property is not reciprocated by the inverse quandle operation and we show in Theorem 5.1.18 by way of a counterexample that a congruence on the inverse operation is not necessarily a congruence on the primary quandle operation.

Chapter 5 continues with a discussion of similar features in the more general weighted average quandle, where the quandle operation is defined by $x \triangleright y = tx + (1-t)y$. Many similar properties to those in the averaging quandle are found. Ultimately, a characterisation of when congruences on one operation imply or do not imply a congruence on the other operation is give, which gives us insight into why in the averaging quandle a congruence that respects the primary quandle operation implies a congruence on the inverse quandle operation but this implication does not occur in reverse.

In the weighted average quandle we see in Theorem 5.2.8 that the sets of differences, $D_x = \{y - x : x \sim y\}$ are independent of x and are equal to [0], the congruence class of 0. We then present some equivalent results to the averaging quandle case. The set of differences is shown in Theorem 5.2.9 to be a subgroup of $\mathbb{Q}$ and in Theorem 5.2.10 as a direct consequence that the congruence class [0] is a subgroup of $\mathbb{Q}$ and that all congruence classes are cosets of [0] of the form $r + [0]$ for some $r \in Q$.

The result in the averaging quandle case that a $\triangleright$-congruence is equivalent to having a subgroup of $\mathbb{Q}$ that is closed under multiplication by $\frac{1}{2} = t$ suggests that we might require, in the more general case of weighted average quandles, that we have a subgroup of $\mathbb{Q}$ that was closed under multiplication by t. In fact, we prove a stronger result in Lemma 5.2.12 that where $t = \frac{p}{q}$ with $p, q \in \mathbb{Z}$ and relatively prime that we have a $\triangleright$-congruence if and only if there is a subgroup that is closed under multiplication by $\frac{1}{q}$. This result enabled us to show, in Theorem 5.2.13, that for a non-trivial congruence, by which we mean the congruence classes are not singletons, with $q > 1$ that the congruence classes were dense in $\mathbb{Q}$. At the beginning of Chapter 5 we indicate that most results can be extended to $\mathbb{R}$. This factor $\frac{1}{q}$ relies on $t \in \mathbb{Q}$. Nevertheless, some additional work not presented here suggests that for $t \in \mathbb{R} \setminus \mathbb{Q}$ we would get congruence classes that are dense in $\mathbb{R}$. Similar arguments apply to those presented here when $|t| < 1$ and for $|t| > 1$ our conjecture is that we can construct a quasi-weight, t_* with $|t_*| < 1$ that will give us density.

When the weight, t, was an integer, as is the case in the averaging quandle for the inverse quandle operation, where $t^{-1} = 2$ and the inverse quandle operation is $x \triangleleft y = 2x - y$, we show, in Lemma 5.2.15 that congruence classes are based on the class of 0, with for some $r \in \mathbb{Q}$, $D = [0] = \{nr : n \in \mathbb{Z}\}$.

Finally, in Chapter 5 we consolidate the results of the chapter in Theorem

5.2.16 in which we classify all congruences based on the value of the weight t. For weights: $t \in \mathbb{Z}\setminus\{0,1\}$ we have that every $\triangleleft$-congruence is a $\triangleright$-congruence; $\frac{1}{t} \in \mathbb{Z} \setminus \{0,1\}$ we have the opposite; and otherwise when $t \notin \mathbb{Z}$ and $\frac{1}{t} \notin \mathbb{Z}$ then neither a $\triangleright$-congruence nor a $\triangleleft$-congruence imply quandle congruences.

Summary — Chapter Six: Congruences in Alexander Quandles

In Chapter 6 we look at Alexander quandles. Weighted average quandles were examples of Alexander quandles. An Alexander quandle is a quandle with an underlying abelian group and quandle operation defined by $x \triangleright y = tx + (1-t)y$, which looks like the definition for a weighted average quandle but in an Alexander quandle t is an automorphic action on the abelian group. In the weighted average quandle the action of t is by normal multiplication and we rely on the invertibility of both t and $(1-t)$, $t \notin \{0,1\}$ for some of the results. In an Alexander quandle we do not necessarily have the invertibility of $(1-t)$. This results in some additional interesting behaviour in congruences in Alexander quandles.

In the weighted average quandle we were able to show that whenever for some $x \in \mathbb{Q}$ we had $x \sim x+d$ then for all $a \in \mathbb{Q}$ we had $a \sim a+d$. In the general Alexander quandle we are only able to prove the weaker relationship that $x \sim x+d$ implies for all $a \in \mathbb{Q}$ that $a \sim a+(1-t)d$. As a result where the difference sets constructed from congruences classes were all shown to be equal in a weighted average quandle, in general in an Alexander quandle those sets are not necessarily equal. However, the intersection of difference sets for congruences is shown to be a subgroup of $\mathbb{Q}$. This subgroup is shown in Lemma 6.2.13 to be closed under multiplication by t — technically the repeated automorphic action of t on the subgroup. As a result for there to be a quandle congruence, a congruence that respects both quandle operations, on an Alexander quandle we need the intersection of all difference sets to be closed under multiplication by both t and t^{-1}. Since the intersection of these difference sets is not necessarily equal to the differences, $D_x = \{y - x : x \sim y\}$ for every x we have the possibility of sets $D_x \neq D_y$ for elements x and y.

Conversely, if we have a subgroup that is closed under multiplication by either or both t and t^{-1} we can construct a congruence on the Alexander quandle. That is shown in Lemma 6.3.1 and its corollaries. In Theorem 6.3.6 we show that a quotient of an Alexander quandle is again an Alexander quandle if and only if the underlying congruence arises by this construction from a subgroup that is closed under multiplication by both t and t^{-1}.

In Sections 6.4 and 6.5 we give some examples based on the congruence classes of $\mathbb{Z}_n$ where different elements in an Alexander quandle have congruence classes based on different sets of differences. The congruence classes have a common set of differences and other sets of differences that are not shared by all other elements in the Alexander quandle. This shows that not every congruence on an Alexander quandle comes from the construction as described above and in Theorem 6.3.6.

Chapter 2

Definitions, Examples, and Preliminaries

2.1 Definitions

In this section we will give definitions of racks, quandles, shelves, and spindles. As noted the definitions are related. There are effectively three distinct axioms or identities. A quandle needs to obey all three axioms; a rack only the second and third axioms; a spindle only the first and third axioms; and a shelf only the third axiom. First we will list the three axioms, which we will refer to as the quandle axioms since a quandle requires all three axioms.

Definition 2.1.1. Quandle Axioms.

The following three axioms are defined on a set, X, together with a binary operation, $\triangleright : X \times X \to X$, usually written as $x \triangleright y$ with $x, y \in X$:

Q1 ***Idempotence*** — For all $x \in X$,

$$x \triangleright x = x;$$

Q2 ***Invertibility*** — For all $y, z \in X$, there exists a unique $x \in X$, such that

$$x \triangleright y = z;$$

Q3 ***Right Self-Distributivity*** — For all $x, y, z \in X$,

$$(x \triangleright y) \triangleright z = (x \triangleright z) \triangleright (y \triangleright z).$$

Now based on the definitions of those three quandle axioms we can define the structures that are known as quandles, racks, spindles, and shelves. These are standard definitions in the literature and are reproduced here for completeness. The quandle and rack definitions are consistent with definitions found in many places, for example, Elhamdadi and Nelson [13] - although they use the alternative form of Axiom Q2 that we give later in Definition 2.1.6 - define racks and quandles; Fenn and Rourke [14] and Nelson and Wong [22] use the invertibility form of Axiom Q2 described here; and Crans [11] and Dehornoy [12] give definitions of a shelf and a spindle.

Definition 2.1.2. Quandle, Rack, Spindle, and Shelf definitions.

We present definitions of the following algebraic structures:

1. A ***quandle*** is a set, Q, with a binary operation on the set, $\triangleright$, that satisfies Axioms Q1, Q2, and Q3;
2. A ***rack*** is a set, R, with a binary operation on the set, $\triangleright$, that satisfies Axioms Q2 and Q3;
3. A ***spindle*** is a set, P, with a binary operation on the set, $\triangleright$, that satisfies Axioms Q1 and Q3;
4. A ***shelf*** is a set, S, with a binary operation on the set, $\triangleright$, that satisfies Axiom Q3.

Remark 2.1.3. Note that these four algebraic structures: quandle; rack; spindle; and shelf, all satsify Axiom Q3. The four structures correspond to the four distinct subsets of the set of the first two axioms, $\{Q1, Q2\}$.

Remark 2.1.4. We indicate we are referring to a quandle, rack, spindle, or shelf by writing the set name together with the binary operation enclosed in parentheses. For example, we write $(X, \triangleright)$ to represent the structure of the set X combined with the binary operation $\triangleright$ and will describe it as a quandle, rack, spindle, or shelf as appropriate. As we will see later, racks and quandles effectively have two binary operations and therefore we will at times we will explicitly write the set together with both binary operations.

Remark 2.1.5 (Symmetries (Joyce [15, 16], Nelson [21])). A set X with a binary operation, $\triangleright$, that satisfies Axiom Q2 ensures that for each $y \in X$ there is a bijection $S_y : X \to X$, such that $xS_y = x \triangleright y$. Note, we write xS_y to mean S_y acting on x and which means precisely what is often represented by $S_y(x)$ in standard function notation. We choose to write xS_y rather than $S_y(x)$ to remind us that y is acting on x and for consistency with the ordering in binary operation notation, since $x \triangleright y = xS_y$. We will discuss these maps in more detail in Section 2.3.1. Here, we note that since S_y satisfies the invertibility axiom it is a bijection and therefore the inverse mapping necessarily exists and is also a bijection. That means that there exists an inverse function, which we denote by S_y^{-1} that we can use to define a second binary operation, which we will denote by $\triangleleft$, as

$$x \triangleleft y = xS_y^{-1}.$$

As a result of this observation, we can rewrite Axiom Q2 in an alternative form based on the two binary operations, $\triangleright$ and $\triangleleft$. Nelson and Wong [22] call the inverse operation the *dual operation* of Q.

Definition 2.1.6 (Alternative second quandle axiom). On a set, X, together with two binary operations, $\triangleright$ and $\triangleleft$ we define the following invertibility axiom, as an alternative to Axiom Q2:

Q2a **Invertibility** — For all $x, y \in X$,

$$(x \triangleright y) \triangleleft y = x.$$

This axiom can be rewritten in terms of the bijective function, S_y, defined by the primary binary operation, $\rhd$, as

$$xS_yS_y^{-1} = x.$$

That form has an almost trivially obvious meaning when we appreciate that the invertibility axiom defines the bijective functions $S_y : X \to X$ for each $y \in X$ and so $S_yS_y^{-1}$ will define the identity function.

Definition 2.1.7 (**Alternative quandle and rack definitions).** As an alternative to the definitions of a *rack* and *quandle* in Definition 2.1.2 we may equivalently define a quandle and a rack as follows:

1. A ***quandle*** is a set, Q, together with two binary operations, $\rhd$ and $\lhd$, that satisfy Axioms Q1, Q2a, and Q3;
2. A ***rack*** is a set, R, together with two binary operations, $\rhd$ and $\lhd$, that satisfy Axioms Q2a, and Q3.

Remark 2.1.8. Note that in this definition, the second binary operation, $\lhd$, is only used in Axiom Q2a. However, it turns out that Axioms Q1 and Q3 also apply to $\lhd$. That is, $(Q, \lhd)$ is a quandle in its own right. We prove this in Proposition 2.3.2. Following Nelson and Wong's usage of dual operation we will define the rack in which the roles of the rack operation and the inverse operation are swapped to be the dual rack.

Definition 2.1.9. Given a rack, $(R, \rhd, \lhd)$ the *dual rack* is the rack $(R, \lhd, \rhd)$ formed by swapping the roles of the two rack operations. If $R(\rhd, \lhd)$ is a quandle, that is if we have idempotence in the rack, then, as we will see, we have idempotence in the dual rack so we can refer to the dual rack as the *dual quandle* of the quandle, $R(\triangleright, \triangleleft)$.

Remark 2.1.10. Superficially, there is some ambiguity as to whether a quandle or rack is a set with one or two binary operations. In terms of the quandle axioms Q1 (only applicable to a quandle), Q2, and Q3 a rack is a set together with a single binary operation, which we write as the ordered pair $(R, \triangleright)$. However, if we instead think in terms of the alternative form Axiom Q2a then a rack is a set together with two binary operations, which we would write as the ordered triplet $(R, \triangleright, \triangleleft)$. However, there is some underlying redundancy in the second notation as the inverse rack operation, as we have seen, is completely determined by the primary rack operation. That is we can think of $(R, \triangleright) = (R, \triangleright, \triangleleft)$. Therefore, usually we will write the more compact $(R, \triangleright)$ to represent the rack with set R together with the binary operation $\triangleright$. We will, at times when we wish to emphasise the second rack operation, explicitly note its presence by using the equivalent ordered triplet notation, $(R, \triangleright, \triangleleft)$. Occasionally, when the rack operation is understood, we may omit the rack operations altogether and just write less formally the "rack R".

Remark 2.1.11. We think of $x \triangleright y$ as "x being *acted on* by y". Joyce [16] uses the terminology "*x through y*" and above in Section 1.3, in the concrete setting of knots and knot diagrams, we used and thought of the operation as "*x under y*".

Remark 2.1.12 (Convention). Since the binary operations we are dealing with are typically not associative, there is an ambiguity when we write $x \triangleright y \triangleright z$. That is, in general

$$(x \triangleright y) \triangleright z \neq x \triangleright (y \triangleright z).$$

To avoid this ambiguity, notationally, we adopt the convention that the ambiguity is resolved by performing the operations from left to right. That is, when the parentheses are omitted we will understand

$$x \triangleright y \triangleright z \text{ to mean } (x \triangleright y) \triangleright z,$$

and similarly with respect to the inverse operation we will understand

$$x \triangleleft y \triangleleft z \text{ to mean } (x \triangleleft y) \triangleleft z.$$

We also adopt this left to right precedence when we have a mix of rack operations. So that in both of the following expressions we will evaluate from the left as follows:

$$x \triangleright y \triangleleft z = (x \triangleright y) \triangleleft z;$$

and

$$x \triangleleft y \triangleright z = (x \triangleleft y) \triangleright z.$$

Remark 2.1.13 (Notation). The notation used for racks and quandles in the literature is far from standardised. We have adopted notation consistent with a set X together with a binary operation $\triangleright$ and write $x \triangleright y$ similarly to how group theorists write $x * y$, $x \cdot y$, or the juxtaposition xy in a multiplicative group; or $x + y$ in an additive group. We think of $x \triangleright y$ as y acting on x. In addition, we use $x \triangleleft y$ for the inverse operation.

Other authors have used a variety of notations. For example, Ryder [28] uses an exponential notation, x^y, as equivalent to what we write as $x \triangleright y$. In exponential notation sometimes the inverse operation is indicated by writing a bar over the element that is acting, that is $x^{\overline{y}} = x \triangleleft y$, and sometimes by writing the exponentiated element on the left, that is ${}^{y}x = x \triangleleft y$. Similarly, using the standard binary operation notation different authors write the inverse operation in different ways, for example by indicating directly on the operation that it is an inverse operation, $x \triangleright^{-1} y$ [7]. Another notation for the inverse operation is to decorate the operator with a bar, for example $x \mathbin{\overline{*}} y$ [20]. Others exchange the direction of the triangle operator symbol, so that $x \triangleleft y$ would mean y acting on x [23], and yet others write the action from the left so $y \triangleright x$ for y acting on x. For example, at the time of writing, in 2022, the ever changing Wikipedia article on quandles uses a left pointing triangle as the operator and the element acting is written on the left. That is, Wikipedia writes $y \triangleleft x$ to mean precisely what we mean by $x \triangleright y$. When the action is written from the left the self-distributivity axiom becomes $x \triangleright (y \triangleright z) = (x \triangleright y) \triangleright (x \triangleright z)$.

As we saw in Remark 2.1.5, yet another notation is based on the fact that the invertibility axiom implies the existence of a permutation or symmetry function S_y at every point y in the set X. These functions are discussed in more detail in Section 2.3.1 below. So $x \triangleright y$ is thought of as the symmetry at y, S_y, acting on x, that is, in standard function notation $S_y(x)$. Often though, as we did earlier, in this style, the function is written juxtaposed to the right of the element it is acting on as xS_y. Given S_y is a bijection, the inverse operation can be thought of as the inverse function, S_y^{-1} for what we write as $x \triangleright y$ and therefore the inverse operation is written xS_y^{-1} for what we write as $x \triangleleft y$.

Obviously, the wide variety of notations used and especially combined with the fact that some alternative notations effectively have the opposite meanings of others means that the reader needs to take special care when reading on this subject to understand the writer's definitions of what notation is in use.

For the most part, we have adopted the basic notation from *Quandles, An Introduction to the Algebra of Knots* by Elhamdadi and Nelson [13]. So, as indicated above, we write $x \triangleright y$ for x being acted on by the symmetry at y. However, Elhamdadi and Nelson use $x \triangleright^{-1} y$ for the inverse operation. For the most part, we have used the more compact $x \triangleleft y$. At times, when it is convenient to do so, for example, when we are considering either $x \triangleright y$ or $x \triangleleft y$ we have adopted $x \triangleright^{-1} y$ as a special case of the more general $x \triangleright^k y$ with $k \in \mathbb{Z}$.

2.2 Examples

In this section we give some examples of racks and quandles. The examples here range from a trivial example in which the operation has (trivially) no action, to examples from familiar contexts that the reader may not have throught of as quandles or racks. These examples are all well-known in the literature.

2.2.1 Trivial quandle

It is hard to imagine anything more trivial than a function or operation that does nothing. It turns out that such an operation satisfies the quandle axioms. So we present as our first example the *trivial quandle* on any set.

Example 2.2.1 (Trivial quandle). For any set, X, define the quandle operation by, for all $x, y \in X$, $x \rhd y = x$. That is, for all $x \in X$, the action of y, for all $y \in X$, has no affect on x.

It is easy to check the quandle axioms for the trivial quandle:

- Q1 — $x \rhd x = x$ by definition;
- Q2 — for all $y, z \in X$, $x \rhd y = z$ has the unique solution $x = z$;
- Q3 — for all $x, y, z \in X$, $(x \rhd y) \rhd z = (x \rhd y) = x = (x \rhd z) = (x \rhd z) \rhd (y \rhd z)$.

Therefore the trivial quandle on any set satisfies the quandle axioms and so is a quandle.

2.2.2 Racks from bijections

The invertibility axiom in a quandle or a rack requires that there exists a function S_y at each point y that is a bijection. For a quandle the bijections, S_y, need to satisfy the idempotence property $yS_y = y$ for each y in the quandle.

Conversely, from any bijection we can define a rack. Note here we are considering the case where there is one bijection, that is $S_y = S$ is independent of y. Except in the special case where the bijection is the identity we will not have idempotence and so we will not get a quandle; and in that special case the quandle will be the trivial quandle.

Example 2.2.2 (Any bijection defines a rack). Let X be a set and let $f : X \to X$ be a bijection. Define the binary operation $\triangleright$ by

$$x \triangleright y = f(x).$$

Then $(X, \triangleright)$ is a rack.

We need to check the rack axioms. As is often the case it is easier to check the equivalent Axiom Q2a rather than Axiom Q2.

- Axiom Q2a: For all $y, z \in X$ the equation $x \triangleright y = z$ is equivalent to $f(x) = z$, which has the unique solution $x = f^{-1}(z)$ since f is a bijection.

- Axiom Q3: We need to show self-distributivity,

  $$(x \triangleright y) \triangleright z = (x \triangleright z) \triangleright (y \triangleright z).$$

  For all $x, y, z \in X$ and working with the left hand side we have,

  $$(x \triangleright y) \triangleright z = f(x) \triangleright z = f\left(f(x)\right).$$

  On the other hand, working with the right hand side we have,

  $$(x \triangleright z) \triangleright (y \triangleright z) = f(x) \triangleright f(y) = f\left(f(x)\right).$$

  Therefore

  $$(x \triangleright y) \triangleright z = (x \triangleright z) \triangleright (y \triangleright z).$$

Remark 2.2.3 (Trivial quandle). The trivial quandle in Example 2.2.1 is a special case of a bijection defining a rack. It is the special case using the identity function

$$x \triangleright y = f(x) = x.$$

Note that the identity function is the only function, $f(x)$, that will define a quandle. For if $f(x) \neq x$ for some x in the rack then we lose idempotence as $x \triangleright x = f(x) \neq x$ and therefore we cannot have a quandle.

Example 2.2.4 (Trivial shelf). If the function $f(x)$ in Example 2.2.2 is not a bijection then we lose the invertibility property but we retain self-distributivity and we have a shelf. A shelf created in this way is known as a *trivial shelf.*

Let X be a set and let $f : X \to X$ be a function. Define the binary operation $\triangleright$ by

$$x \triangleright y = f(x).$$

Then $(X, \triangleright)$ is a shelf. We only need to prove the distributivity axiom and that proof is identical to the proof in Example 2.2.2.

2.2.3 Conjugation quandles

There are a family of examples of quandles based on conjugation in a group. Conway is said to have thought of quandles as what is left from a group when you throw away everything except conjugation.

In the first of these examples we start with any group and investigate the quandle axioms as applied to a binary operation defined as conjugation in the group. At the end of this section we will generalise conjugation to n-fold conjugation which in turn will be generalised in Section 2.2.4.

Example 2.2.5 (Conjugation quandle). In any group, $(G, *)$, define the quandle operation by conjugation. That is, $x \triangleright y = y^{-1} * x * y$, where y^{-1} is the normal inverse element of y in the group G. Then $(G, \triangleright)$ is a quandle.

Again checking the quandle axioms we see:

- Q1 — $x \triangleright x = x^{-1} * x * x = x$;
- Q2 — for all $y, z \in X$, $x \triangleright y = y^{-1} * x * y = z$ has the unique solution

$x = y * z * y^{-1}$;

- Q3 — for all $x, y, z \in X$,

$$\begin{aligned}
(x \triangleright y) \triangleright z &= (y^{-1} * x * y) \triangleright z \\
&= z^{-1} * y^{-1} * x * y * z \\
&= z^{-1} * y^{-1} * (z * z^{-1}) * x * (z * z^{-1}) * y * z \\
&= (z^{-1} * y^{-1} * z) * (z^{-1} * x * z) * (z^{-1} * y * z) \\
&= (z^{-1} * y * z)^{-1} * (z^{-1} * x * z) * (z^{-1} * y * z) \\
&= (y \triangleright z)^{-1} * (x \triangleright z) * (y \triangleright z) \\
&= (x \triangleright z) \triangleright (y \triangleright z).
\end{aligned}$$

Therefore using conjugation in any group, $(G, *)$, as the quandle operation defines a quandle on the set, G.

Obviously, using conjugation as the quandle operation is only interesting if the group is non-abelian. If the group is abelian then conjugation collapses

$$x \triangleright y = y^{-1} * x * y = x * (y^{-1} * y) = x$$

and we get the trivial quandle.

There is a similar conjugation where the roles of y and y^{-1} are exchanged. More precisely, conjugation as described above can be thought of as *right-conjugation.* Equivalently, *left-conjugation* defined by $x \triangleright y = y * x * y^{-1}$, by the analogous arguments, also satisfies the quandle axioms and so also defines a quandle.

Example 2.2.6 (Left-conjugation quandle). In any group, $(G, *)$, define the quandle operation by left-conjugation. That is, $x \triangleright y = y * x * y^{-1}$, where y^{-1} is the normal inverse element of y in the group G. Then $(G, \triangleright)$ is a quandle.

As noted the demonstration of this mimics the demonstration that right-conjugation is a quandle and so will not be repeated.

It is easily seen that left-conjugation is the inverse quandle operation for right-conjugation and vice versa. If we let $\triangleright$ be the binary operation of right-conjugation so that $x \triangleright y = y^{-1} * x * y$, and $\triangleleft$ the binary operation of left-conjugation so that $x \triangleleft y = y * x * y^{-1}$, then we can see that

$$\begin{aligned}
(x \triangleright y) \triangleleft y &= y * (y^{-1} * x * y) * y^{-1} \\
&= (y * y^{-1}) * x * (y * y^{-1}) \\
&= x,
\end{aligned}$$

as is required for inverse quandle operations.

Example 2.2.7 (n-fold conjugation). The conjugation example can be generalised to n-fold conjugation. In any group $(G, *)$, define

$$x \triangleright y = y^{-n} * x * y^{n}.$$

By a similar check to that in Example 2.2.5 with y and y^{-1} replaced by y^n and y^{-n} respectively we can see that $\triangleright$ defines a quandle operation and hence $(G, \triangleright)$ is a quandle on the group elements, G.

As with left and right-conjugation this example can be thought of as right n-fold conjugation and the example can be extended to left n-fold conjugation. As in the simpler case, left n-fold conjugation is the inverse quandle operation to right n-fold conjugation and vice versa.

Remark 2.2.8. Note, again, that the conjugation quandle and its extensions to n-fold conjugation and left and right-conjugation are only interesting if the underlying group is non-Abelian. If the group is Abelian then

$$x \triangleright y = y^{-n} x y^n = y^n x y^{-n} = x$$

because of the commutativity in the underlying group and all conjugation type calculations collapse and we are left with the trivial quandle.

2.2.4 n-Fold quandle operations

The n-fold conjugation example can be considered to be repeatedly applying conjugation n times. The n-fold application of a quandle operation can be generalised to any quandle operation. That is, as we will show, if $(Q, \triangleright)$ is a quandle then so is $(Q, \triangleright^n)$ where $x \triangleright^n y = (\cdots((x \triangleright y) \triangleright y) \cdots y)$ is repeatedly acting on x, by the symmetry at y, n times. We will use that as a formal definition of $\triangleright^n$.

Definition 2.2.9. Let $(S, \triangleright)$ be a set, S, with a binary operation $\triangleright$ then we define the binary operation $\triangleright^n$ with $n \in \mathbb{N}$ to mean repeated action on the right by a particular quandle element. We define this inductively for $n \in \mathbb{N}$ by

$$x \triangleright^1 y = x \triangleright y,$$

and

$$x \triangleright^{n+1} y = (x \triangleright^n y) \triangleright y. \tag{2.2.1}$$

Additionally, if we have invertibility from Axiom Q2 and so have an inverse operation $\triangleleft$ then we may write $\triangleright^{-n}$ to mean n times repeated action on the right by the inverse quandle operation. That is, the operators $\triangleleft^n$ and $\triangleright^{-n}$ are equivalent.

In that context, we may want to use $\triangleright^0$ or $\triangleleft^0$. Those symbols will be interpreted as there being no operation by the right hand variable. That is, $x \triangleright^0 y = x \triangleleft^0 y = x$ for all $x, y \in S$. So $(S, \triangleright^0) = (S, \triangleleft^0)$ will both be the trivial quandle.

Remark 2.2.10. This is precisely what is happening with n-fold conjugation. We know that conjugation defines a quandle on any group. If we define the binary operation, $\triangleright$, to be conjugation then $\triangleright^n$ is n-fold conjugation.

Proposition 2.2.11 (**n-fold operation**)**.** *Given a set, S, with a binary operation, $\triangleright$, then for $n \in \mathbb{N}$:*

1. *If $(S, \triangleright)$ is a shelf then $(S, \triangleright^n)$ is a shelf.*

2. *If* $(S, \triangleright)$ *is a spindle then* $(S, \triangleright^n)$ *is a spindle.*

3. *If* $(S, \triangleright)$ *is a rack then* $(S, \triangleright^n)$ *is a rack.*

4. *If* $(S, \triangleright)$ *is a quandle then* $(S, \triangleright^n)$ *is a quandle.*

The proposition will be proved below by a number of lemmas and their corollaries which relate to the preservation of the quandle axioms. Essentially, the axiomatic properties: idempotence; invertibility; and self-distributivity are preserved independently. Therefore, they can be proved independently. So the following lemmas will establish for each axiom that it is satisfied by the n-fold application of an operation that satisfies that axiom. That is, we will see that if a set, S, together with a binary operation, $\triangleright$, that has any of the three properties: idempotence; invertibility; or self-distributivity, then $(S, \triangleright^n)$ also has the corresponding properties. Therefore by combining the appropriate properties that are satisfied we will have that $(S, \triangleright^n)$ is a shelf, spindle, rack, or quandle as claimed.

It is relatively easy to verify that idempotence and invertibility are preserved in $(S, \triangleright^n)$ but less obvious that self-distributivity is preserved. We will show in Lemma 2.2.12 that if we have a set, S, with a binary operation, $\triangleright$, then whenever we have idempotence or invertibility in $(S, \triangleright)$ then those properties are preserved in $(S, \triangleright^n)$. To show that self-distributivity is preserved we will first prove in Lemma 2.2.13 a stronger result that self-distributivity is preserved over two binary operations, $\triangleright^m$ and $\triangleright^n$ generated from a self-distributive operation, $\triangleright$. Self-distributivity will follow immediately from that by setting $m = n$.

Lemma 2.2.12. *Given a set, S, with a binary operation, $\triangleright$. Then we have:*

1. *If $\triangleright$ is idempotent then $\triangleright^n$ is idempotent. That is, for all $x \in S$ and $n \in \mathbb{N}$, we have $x \triangleright^n x = x$.*

2. *If $\triangleright$ is invertible then $\triangleright^n$ is invertible. That is, for all $x \in S$ and $n \in \mathbb{N}$, we have $x \triangleright^n y = z$ has a unique solution $x \in S$.*

Proof. Let S be a set with a binary operation $\triangleright$ then we show by induction that if $\triangleright$ is idempotent or invertible then for any $n \in \mathbb{Z}$ we have that $\triangleright^n$ is idempotent or invertible respectively.

1. **Idempotence**: Assume $\triangleright$ is idempotent. Then we note that for $x \in S$, $x \triangleright^1 x = x \triangleright x = x$. Next assume for some $k \in \mathbb{N}$ and $x \in S$ that $x \triangleright^k x = x$. Now $x \triangleright^{k+1} x = (x \triangleright^k x) \triangleright x = x \triangleright x = x$. Therefore for all $n \in \mathbb{N}$ and $x \in S$ we have that $x \triangleright^n x = x$ is true and so $(S, \triangleright^n)$ is idempotent.

2. **Invertibility**: Assume $\triangleright$ is invertible. Then we note that $x \triangleright^1 y = z$ is equivalent to $x \triangleright y = z$ which has a unique solution for all $y, z \in S$. Next for some $k \in \mathbb{N}$ assume for all $y, z \in S$ that $x \triangleright^k y = z$ has a unique solution. Now we need to solve $x \triangleright^{k+1} y = z$. The left hand side is equivalent to $(x \triangleright^k y) \triangleright y = z$ which is of the form $w \triangleright y = z$ and therefore by assumption has a unique solution for w in S. Now we need to solve $x \triangleright^k y = w$ which has a unique solution by the inductive hypothesis. Therefore for all $n \in \mathbb{N}$ and $y, z \in S$ we have $x \triangleright^n y = z$ has a unique solution and so $(S, \triangleright^n)$ is invertible.

□

As foreshadowed, to show distributivity it is helpful to prove the more general distributivity result that, for all $m, n \in \mathbb{N}$,[1]

$$(x \triangleright^m y) \triangleright^n z = (x \triangleright^n z) \triangleright^m (y \triangleright^n z). \tag{2.2.2}$$

We will show that distributivity follows in the general setting of a shelf.

Lemma 2.2.13. *Let* $(S, \triangleright)$ *be a shelf. For all* $x, y, z \in S$ *and* $m, n \in \mathbb{N}$*, the distributive relationship*

$$(x \triangleright^m y) \triangleright^n z = (x \triangleright^n z) \triangleright^m (y \triangleright^n z)$$

holds.

Proof. We prove this lemma by two inductions, first over m and then over n.

Let $(S, \triangleright)$ be a shelf and x, y, z be any elements in the shelf.

For all $m \in \mathbb{N}$ we proceed to show that $(x \triangleright^m y) \triangleright z = (x \triangleright z) \triangleright^m (y \triangleright z)$. We will then use that result as the base case in the second induction over n to show for all $m, n \in \mathbb{N}$ that $(x \triangleright^m y) \triangleright^n z = (x \triangleright^n z) \triangleright^m (y \triangleright^n z)$.

We note that we know that $(x \triangleright y) \triangleright z = (x \triangleright z) \triangleright (y \triangleright z)$ in the shelf since a shelf satisfies the distributivity axiom and so we have a base case for the

---

[1] We can and will, in Corollary2.2.17, extend this result to $m, n \in \mathbb{Z}$ by thinking of $\triangleright^{-k} = \triangleleft^k$ and $\triangleright^0$ as an operation with no action.

first induction that is true. Next we assume the inductive hypothesis that $(x \rhd^k y) \rhd z = (x \rhd z) \rhd^k (y \rhd z)$ is true for some $k \in \mathbb{N}$. We consider

$$(x \rhd^{k+1} y) \rhd z,$$

which by the definition of $\rhd^k$ is equivalent to

$$\Big((x \rhd^k y) \rhd y\Big) \rhd z.$$

Applying the distributivity Axiom Q3 in the shelf $(S, \rhd)$ that in turn is equivalent to:

$$\Big((x \rhd^k y) \rhd z\Big) \rhd (y \rhd z).$$

The expression in the big left hand parentheses is the left hand side of our induction hypothesis so this can be rewritten as:

$$\Big((x \rhd z) \rhd^k (y \rhd z)\Big) \rhd (y \rhd z).$$

Finally, we can rewrite this using the definition of $\rhd^n$ as

$$(x \rhd z) \rhd^{k+1} (y \rhd z).$$

From which we can conclude for all $m \in \mathbb{N}$ that

$$(x \rhd^m y) \rhd z = (x \rhd z) \rhd^m (y \rhd z). \tag{2.2.3}$$

Since this is now known to be true we can use the result as the base case for induction over n.

We begin the second induction by assuming that for some fixed m that for some $k \in \mathbb{N}$ $(x \triangleright^m y) \triangleright^k z = (x \triangleright^k z) \triangleright^m (y \triangleright^k z)$.

We proceed similarly to the first part of this proof and consider

$$(x \triangleright^m y) \triangleright^{k+1} z$$

which by definition is equivalent to

$$\Big((x \triangleright^m y) \triangleright^k z\Big) \triangleright z.$$

Applying the induction hypothesis to the term inside the big parentheses on the left we obtain:

$$\Big((x \triangleright^k z) \triangleright^m (y \triangleright^k z)\Big) \triangleright z.$$

We can now use the result from the first part of this Lemma in equation (2.2.3) to get:

$$\Big((x \triangleright^k z) \triangleright z\Big) \triangleright^m \Big((y \triangleright^k z) \triangleright z\Big).$$

Finally, as before, using the definition of $\triangleright^n$, this reduces to the required result:

$$(x \triangleright^{k+1} z) \triangleright^m (y \triangleright^{k+1} z).$$

Since this is true for any fixed $m \in \mathbb{N}$ we can conclude for all $m, n \in \mathbb{N}$ and for all $x, y, z \in S$ that

$$(x \triangleright^m y) \triangleright^n z = (x \triangleright^n z) \triangleright^m (y \triangleright^n z) \tag{2.2.4}$$

is true. □

As foreshadowed, we need the simplified result that comes from Lemma 2.2.13 by setting $m = n$. For clarity, we state that result here as a corollary.

Corollary 2.2.14. *If on a shelf* $(S, \triangleright)$ *for* $n \in \mathbb{N}$ *we define the binary operation* $\triangleright^n$ *by* $x \triangleright^n y = (\cdots(x \triangleright y) \triangleright y) \cdots \triangleright y)$ *with the action by* y *repeated* n *times then the binary operation* $\triangleright^n$ *is self-distributive. That is,*

$$(x \triangleright^n y) \triangleright^n z = (x \triangleright^n z) \triangleright^n (y \triangleright^n z).$$

Proof. The result follows immediately on applying Lemma 2.2.13 and putting $m = n$. □

Corollary 2.2.15. *If* $(S, \triangleright)$ *is a shelf then for all* $n \in \mathbb{N}$, $(S, \triangleright^n)$ *is a shelf. In addition,*

1. *If* $\triangleright$ *is idempotent then* $(S, \triangleright^n)$ *is a spindle.*

2. *If* $\triangleright$ *is invertible then* $(S, \triangleright^n)$ *is a rack.*

3. *If* $\triangleright$ *is idempotent and invertible then* $(S, \triangleright^n)$ *is a quandle.*

Proof. In order to show that $(S, \triangleright^n)$ is a shelf we only need to show that the distributivity axiom is satisfied. That follows immediately from Corollary 2.2.14.

Similarly, applying Lemma 2.2.12 establishes idempotence and invertibility whenever we have those properties in $(S, \triangleright)$.

The results follow immediately on applying the relevant parts of Lemma 2.2.12 to establish idempotence and invertibility where applicable. □

Remark 2.2.16. The results in Lemmas 2.2.12 and 2.2.13 and Corollaries 2.2.14 and 2.2.15 can be extended to the operations $\triangleright^{-n}$, for $n \in \mathbb{N}$ which are equivalent to $\triangleleft^n$ whenever the inverse operation exists as defined by the invertibility axiom. In particular, whenever we have a quandle or rack then by applying the above Lemmas and Corollaries to the dual quandle or rack we can extend the results to negative integer powers. Further, recall that we consider $\triangleright^0$ to mean that for all $x, y \in S$ we have $x \triangleright^0 y = x$, so that $(S, \triangleright^0)$ is the trivial quandle. Therefore these lemmas and corollaries can be extended to all $n \in \mathbb{Z}$ whenever that extension to non-positive n is sensible.

The proof will follow the above arguments and so we will state that extension as the corollary below without proof.

Corollary 2.2.17. *If $(R, \triangleright)$ is a rack then for all $n \in \mathbb{Z}$, $(R, \triangleright^n)$ is a rack. In addition, if $\triangleright$ is idempotent in $(R, \triangleright)$ then $(R, \triangleright^n)$ is a quandle.*

2.2.5 Alexander quandles

In this section we introduce Alexander quandles which will be used extensively later in this thesis, when we look at congruences in racks and quandles. There is some familiarity with the example of an Alexander quandle in that it looks like a weighted average,

$$W(x, y) = tx + (1 - t)y,$$

where $t, x, y \in \mathbb{Q}$ say with $t \in [0, 1]$. If we consider rational numbers with an equal weight, that is $t = 0.5$ then the weighted average is simply the arithmetic mean, $\mu(x, y)$, of two numbers:

$$W(x, y) = 0.5x + (1 - 0.5)y = \frac{x + y}{2} = \mu(x, y).$$

Alexander quandles are a generalisation of this concept with the quandle operation defined by

$$x \triangleright y = tx + (1 - t)y,$$

in a module over the Laurent ring $\mathbb{Z}[t, t^{-1}]$. A module is defined as follows:

Definition 2.2.18 (Module). Let R be a ring and X an abelian group. An action of R on X defined for all $r \in R$ and for all $x \in X$ by a binary operation (dot)

$$\cdot : R \times X \to X, (r, x) \mapsto r \cdot x,$$

defines a *(left) R-Module* if and only if for all $r, s \in R$ and for all $x, y \in X$ we have:

1. $1 \cdot x = x$;
2. $r \cdot (s \cdot x) = (rs) \cdot x$;
3. $(r + s) \cdot x = r \cdot x + r \cdot y$;
4. $r \cdot (x + y) = r \cdot x + r \cdot y$.

Remark 2.2.19. A module is a generalisation of the concept of vector space, in which the concept of scalar multiplication in a vector space has been replaced by and extended to the action of the ring on an abelian group in a module.

In an Alexander quandle we have the Laurent ring $\mathbb{Z}[t, t^{-1}]$ acting on a set X. We formally define an Alexander quandle as follows.

Definition 2.2.20 (Alexander quandle). Let X be a module over the Laurent ring $\mathbb{Z}[t, t^{-1}]$. Then for $x, y \in X$,

$$x \triangleright y = tx + (1 - t)y$$

defines a quandle operation on X. The quandle $(X, \triangleright)$ is an *Alexander quandle.*

Remark 2.2.21. In an Alexander quandle t acts on the group. The action is as a group automorphism, $t : X \to X$. An alternative definition of an Alexander quandle used by, for example, Bae and Choi [4] is that an Alexander quandle is an abelian group, X, with a quandle operation

$a \triangleright b = ta + (1-t)b$ where t is a group automorphism of the abelian group, X. Here 1 represents the identity automorphism and $(1-t)y = 1y - ty$.

Distributivity in the module, $t \cdot (x+y) = t \cdot x + t \cdot y$ informs us that t acts as a homomorphism in the group. Moreover, since $1 \cdot x = x$ and $t \cdot (s \cdot x) = (ts) \cdot x$ we have that for $s = t^{-1}$, $t \cdot (s \cdot x) = s \cdot (t \cdot x) = x$ and therefore the homomorphism is an automorphism.

We can show that an Alexander quandle is a quandle by checking the quandle axioms.

Theorem 2.2.22 (Alexander quandle). *An Alexander quandle is a quandle.*

Proof. Let X be an Alexander quandle and we check each quandle axiom in turn.

- Q1 — for all $x \in X$, $x \triangleright x = tx + (1-t)x = tx + x - tx = x$;
- Q2 — for all $y, z \in X$, we solve $x \triangleright y = tx + (1-t)y = z$ by working in X to obtain $tx = z - (1-t)y$ and then by acting on tx by t^{-1} to obtain the unique solution $x = t^{-1}z + (1-t^{-1})y$. The solution is unique because t and therefore t^{-1} is a bijection;
- Q3 — for all $x, y, z \in X$, we work with the left hand side and right hand side of the distributivity axiom $(x \triangleright y) \triangleright z) = (x \triangleright z) \triangleright (y \triangleright z)$

separately to obtain:

$$\begin{aligned}
\text{LHS:} \qquad (x \triangleright y) \triangleright z &= \big(tx + (1-t)y\big) \triangleright z \\
&= t^2x + t(1-t)y + (1-t)z; \\
\text{RHS:} \quad (x \triangleright z) \triangleright (y \triangleright z) &= \big(tx + (1-t)z\big) \triangleright \big(ty + (1-t)z\big) \\
&= t^2x + t(1-t)z + (1-t)\big(ty + (1-t)z\big) \\
&= t^2x + t(1-t)y + (1-t)z \\
&= (x \triangleright y) \triangleright z.
\end{aligned}$$

Since the left hand side equals the right hand side we have distributivity as required.

Since all of the quandle axioms are satisfied, $(X, \triangleright)$ is a quandle. □

Corollary 2.2.23 (Alexander inverse quandle operation). *Let* $(X, \triangleright)$ *be an Alexander quandle with* $t \neq 0$ *and quandle operation*

$$x \triangleright y = tx + (1-t)y$$

then

1. *The inverse quandle operation is*

$$x \triangleleft y = t^{-1} + (1-t^{-1})y.$$

2. *The quandle* $(X, \triangleleft)$ *is an Alexander quandle.*

Proof. Part 1 was proved in Theorem 2.2.22 in establishing that for all $y, z \in X$, $x \triangleright y = z$ had the unique solution $x = t^{-1}z + (1 - t^{-1})y$.

We can check that this is the inverse by performing the calculation

$$\begin{aligned}(x \triangleright y) \triangleleft y &= \big(tx + (1-t)y\big) \triangleleft y \\ &= t^{-1}\big(tx + (1-t)y\big) + (1 - t^{-1})y \\ &= x + (t^{-1} - 1)y + (1 - t^{-1})y \\ &= x.\end{aligned}$$

Part 2 we can see immediately from the form of the inverse operation. The inverse quandle operation in an Alexander quandle is itself an Alexander quandle operation with the action of t replaced by the action of t^{-1}. If t is an automorphism then t^{-1} is an authomorphism. Therefore whenever $(X, \triangleright)$ is an Alexander quandle, $(X, \triangleleft)$ is an Alexander quandle.

□

Remark 2.2.24.

The distributive identity $(a + b) \triangleright (c + d) = (a \triangleright c) + (b \triangleright d)$ is frequently useful in Alexander quandles.[2]Therefore we show it is true in the following lemma.

---

[2] This is the simplistic rule that many high school and undergraduate students mistakenly try to use when multiplying out brackets:

$$(a + b)(c + d) \neq ac + bd.$$

Equality holds in this quandle. There are no mixed terms.

Lemma 2.2.25 (A useful identity). *Let A be an Alexander quandle then for all $a, b, c, d \in A$,*

$$(a+b) \triangleright (c+d) = (a \triangleright c) + (b \triangleright d). \tag{2.2.5}$$

Proof. Let A be an Alexander quandle with $a, b, c, d \in A$. Then

$$\begin{aligned}(a+b) \triangleright (c+d) &= t(a+b) + (1-t)(c+d) \\ &= \big(ta + (1-t)c\big) + \big(tb + (1-t)d\big) \\ &= (a \triangleright c) + (b \triangleright d).\end{aligned}$$

$\square$

Since the inverse quandle operation in an Alexander quandle is an Alexander quandle operation with t replaced by t^{-1} Lemma 2.2.25 applies to the analogous calculation with the inverse operation.

Corollary 2.2.26. *Let A be an Alexander quandle then for all $a, b, c, d \in A$,*

$$(a+b) \triangleleft (c+d) = (a \triangleleft c) + (b \triangleleft d). \tag{2.2.6}$$

Remark 2.2.27. Note the parentheses on the right hand sides of equations (2.2.5) and (2.2.6) are not necessary providing we adopt the order of operations convention that the quandle operations $\triangleright$ and $\triangleleft$ take precedence over addition. We adopt that convention.

Later, in Chapter 5, we will look at averaging quandles on $\mathbb{Q}$ in which the quandle operation is the arithmetic mean. The averaging quandle is an example of an Alexander quandle.

Example 2.2.28 (Averaging quandle). Working in the set of rational numbers, $\mathbb{Q}$, with the binary operation defined by

$$x \triangleright y = \frac{x+y}{2}$$

the arithmetic mean of x and y, $(\mathbb{Q}, \triangleright)$ is a quandle. We can see this is of the form of an Alexander quandle by writing the quandle operation $x \triangleright y = \frac{x+y}{2}$ as $x \triangleright y = \frac{1}{2}x + (1 - \frac{1}{2})y = tx + (1-t)y$ with $t = \frac{1}{2} \in \mathbb{Q}$ and therefore $t^{-1} = 2 \in \mathbb{Q}$.

That the averaging quandle is a quandle follows from Theorem 2.2.22 where we showed that the more general Alexander quandle as defined in Definition 2.2.20 was a quandle. Nevertheless, for illustrative purposes we will explicitly show that the quandle axioms are satisfied in this special case.

- Q1 For all $x \in \mathbb{Q}$ we have

$$x \triangleright x = \frac{x+x}{2} = x;$$

- Q2 For all $y, z \in \mathbb{Q}$ the equation

$$x \triangleright y = \frac{x+y}{2} = z$$

has the unique solution

$$x = 2z - y;$$

- Q3 For all $x, y, z \in \mathbb{Q}$ we have

  $$(x \triangleright y) \triangleright z = \frac{x}{4} + \frac{y}{4} + \frac{z}{2},$$

  and

  $$(x \triangleright z) \triangleright (y \triangleright z) = \frac{x}{4} + \frac{y}{4} + \frac{z}{2} = (x \triangleright y) \triangleright z.$$

In $\mathbb{Q}$, the averaging quandle can be generalised to weighted average quandles, in which the quandle operation is $x \triangleright y = tx+(1-t)y$ for some weight, $t \in \mathbb{Q}$.

Example 2.2.29 (Weighted average quandle). Let $X = \mathbb{Q}$ and define the binary operation, $\triangleright$, by

$$x \triangleright y = tx + (1 - t)y,$$

for some $t \in \mathbb{Q} \setminus \{0\}$. Then $(\mathbb{Q}, \triangleright)$ is a quandle. Showing that the weighted average operation defines a quandle on $\mathbb{Q}$ follows the demonstration that an Alexander quandle satisfies the quandle axioms in Theorem 2.2.22 and so will not be repeated here. The inverse operation in a weighted average quandle is

$$x \triangleleft y = t^{-1}x + (1 - t^{-1})y.$$

This is a special case of the inverse in an Alexander quandle and it can be demonstrated by the calculation in Corollary 2.2.23. Note that the inverse operation is a weighted average quandle operation with t replaced by t^{-1}.

The averaging quandle is a special case of the weighted average quandle with a weight of $t = \frac{1}{2}$. The averaging and weighted average quandles are examples of Alexander quandles.

Remark 2.2.30. The weighted average quandle example can be traced back to Burstin and Mayer [9] who give a weighted average example in $\mathbb{C}$. They state that composition of two complex numbers a and b given by

$$a \cdot b = \alpha a + \beta b,$$

where $\alpha + \beta = 1$ is a distributive group. Recall, as discussed in Section 1.2, that for a distributive group Burstin and Mayer required invertibility both on the left and right, that is, for all $b, c \in \mathbb{C}$, both

$$\alpha x + \beta b = c \text{ and } \alpha b + \beta y = c$$

have unique solutions $x, y \in \mathbb{C}$, and self-distributivity on the left and right, that is, for all $a, b, c \in \mathbb{C}$,

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

and

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

but they did not explicitly require idempotence. This example, as we have seen, does satisfy the idempotence axiom and so is a quandle. Indeed, Burstin and Mayer note that in a distributive groupoid for all a, $a = a \cdot a$, so idempotence is guaranteed, as we noted in Section 1.2. That is a consequence of having both right self-distributivity and right invertibility (or left self-distributivity and left invertibility — and Burstin and Mayer have both properties on both the left and right).

We can see this by considering for all a in a distributive groupoid:

$$\begin{aligned} x &= (a \cdot a) \cdot a \\ &= (a \cdot a) \cdot (a \cdot a) && \text{by right self-distributivity.} \end{aligned}$$

Now we can deduce from right invertibility that $a = a \cdot a$ which establishes idempotence. The reasoning is identical if we use left self-distributivity and left invertibility but this reasoning fails in a rack where there is right self-distributivity and left invertibility. Hence, in racks we do not necessarily have idempotence.

Burstin and Mayer used idempotence to establish that a non-trivial distributive groupoid could not have a unit. For if there was a unit, e, such that for all a, $e \cdot a = a$ then since $a \cdot a = a$ we would have from invertibility that $e = a$ which can't be true for all a in a non-trivial distributive groupoid.

Another similar example to averaging and weighted average quandles is introduced by Burstin and Mayer using the geometric mean rather than the arithmetic mean. This time on $\mathbb{R}^+ = \{x \in \mathbb{R} : x > 0\}$ they define a binary operation for $a, b \in \mathbb{R}^+$ as

$$a \cdot b = \sqrt{ab}$$

and note that it is left and right invertible and left and right self-distributive. It is easy to see that $a \cdot a = \sqrt{a^2} = a$ and therefore this distributive group is idempotent and therefore a quandle.

They further extend this example in a manner similar to a weighted average in the context of multiplication by defining a binary operation

$$a \cdot b = a^\alpha b^\beta$$

with $\alpha + \beta = 1$. Again it is easily seen that this is idempotent as well as left and right invertible and left and right self-distributive and so $(\mathbb{R}^+, \cdot)$ is a quandle.

Burstin and Mayer's generalised geometric mean example is isomorphic to their weighted average example restricted to $\mathbb{R}^+$ by the isomorphism $\phi : \mathbb{R}^+ \to \mathbb{R}^+$ defined by $\phi(x) = \ln(x)$. Then $\phi(a \cdot b) = \phi(a^\alpha b^\beta) = \alpha \ln a + \beta \ln b$, which is the weighted average of $\ln a$ and $\ln b$.

Another special case of an Alexander quandle is the Takasaki kei. The Takasaki kei is historically significant. It was investigated by Takasaki in 1943 [29] and was one of the first examples of quandles to be investigated. The Takasaki kei is a weighted average quandle on $\mathbb{Z}$ with a weight $t = -1$. The Takasaki kei has the special property that $t^{-1} = t = -1$ which in turn means that the inverse quandle operation is identical to the quandle operation.

Example 2.2.31 (Takasaki kei). Let $K = \mathbb{Z}$. Then $x \triangleright y = 2y - x$ defines a quandle operation. Again, although not necessary since we have shown more generally that any Alexander quandle is a quandle we will explicitly check the quandle axioms for the Takasaki kei.

- Q1 — For all $x \in K$,

  $$x \triangleright x = 2x - x = x;$$

- Q2 — For all $y, z \in K$,

  $$x \triangleright y = 2y - x = z$$

  has the unique solution

  $$x = 2y - z = z \triangleright y;$$

- Q3 — For all $x, y, z \in K$,

  $$(x \triangleright y) \triangleright z = 2z - 2y + x,$$

and

$$\begin{aligned}(x \triangleright z) \triangleright (y \triangleright z) &= (2z - x) \triangleright (2z - y) \\ &= 4z - 2y - 2z + x \\ &= 2z - 2y + x \\ &= (x \triangleright y) \triangleright z.\end{aligned}$$

Remark 2.2.32. In fact, more generally, a **kei**, pronounced "kay", was defined by Takasaki [29] as a set with a binary operation that satisfies the three axioms:

1. Idempotence, $aa = a$;
2. Involution, $(ab)b = a$;
3. Self-distributivity $(ab)c = (ac)(bc)$,

where a, b, c are in the set.

Remark 2.2.33 (Involutory property). The involution property in the Takasaki kei is a special case of invertibility. Involution is the property that a second repeated action by the same element returns the element that was being acted upon, $(x \triangleright y) \triangleright y = x$. That is, the quandle operation is its own inverse operation. A quandle with a quandle operation that is its own inverse is known as involutary. Which leads to the following definition.

Definition 2.2.34 (Involutory quandle or kei). A quandle that satisfies the condition

$$(x \triangleright y) \triangleright y = x$$

is called an *involutary quandle* or for historical reasons as we saw in Section 1.2 a *kei*.

Remark 2.2.35 (Cyclic quandle). If we replace $\mathbb{Z}$ by $\mathbb{Z}_n$ in the Takasaki kei of Example 2.2.31 and perform the quandle operation modulo n, so that

$$x \triangleright y = (2y - x) \mod n,$$

the resultant quandle is called the *cyclic quandle of order n*. This quandle can be thought of as representing the reflections in D_n under conjugation and so is also sometimes called the *dihedral quandle*.

Remark 2.2.36. The structure of the Takasaki kei would apply to any Abelian group $(A, +)$ with the binary operation defined by $x \triangleright y = 2y - x = y + y - x$ applied to it, in which case $(A, \triangleright)$ is a quandle. Checking the axioms follows the reasoning in Example 2.2.31 and so is not repeated here.

Remark 2.2.37. The concept of involution can be generalised to quandles, Q, that have the property where for some $n \in \mathbb{N}$ we have $x \triangleright^n y = x$, for every $x, y \in Q$, where $\triangleright^n$ has the same meaning that we gave to it in Example 2.2.11. It is convenient here to think of the quandle operation as the symmetry function S_y. So we are considering quandles with the property that for all $x \in Q$, $xS_y^n = x$ for some $n \in \mathbb{N}$ with $n > 1$. Therefore the inverse operation in those quandles will be $(S_y)^{n-1}$ since $x = x(S_y)^n = (xS_y)(S_y)^{n-1} = (x \triangleright y) \triangleleft y$. In particular, for any finite quandle, Q, since S_y is necessarily a bijection of finite order there always exists $n \in \mathbb{N}$ such that $x(S_y)^n = x$ for all $x, y \in Q$. Note that if for all $x \in Q$, $xS_y^1 = x$, that is $n = 1$ satisfies the previous equation, then we have the trivial quandle which is uninterestingly involutory since $x \triangleright y \triangleright y = x \triangleright y = x$.

An Alexander quandle requires the Laurent ring $\mathbb{Z}[t, t^{-1}]$. A similar structure can be formed more generally from any ring R and R-module G, and the familiar binary operation $x \triangleright y = tx + (1 - t)y$, where we choose a particular $t \in R$. However, if the action of t on the group G is not invertible then we will not satisfy the invertibility axiom and therefore we will not have a quandle. Instead we will be left with a spindle since the operation will be both idempotent and self-distributive.

Example 2.2.38 (**Alexander spindle [12]**)**.** Let R be a ring with $t \in R$ and G an R-Module then the binary operation defined on G by

$$a \triangleright b = ta + (1 - t)b$$

gives $(G, \triangleright)$ the structure of a spindle. We will call such a spindle an *Alexander spindle*. Showing idempotence and self-distributivity follows exactly the proof shown for an Alexander quandle in Theorem 2.2.22.

Dehornoy [12] claims that an Alexander spindle is a quandle if and only if t is invertible. It is true that if t is invertible then we have precisely the situation in an Alexander quandle where we have shown that the invertibility axiom holds. However, it is sufficient for t to act invertibly and it is not necessary for t to be invertible for the spindle to be a quandle. We show this in the next example.

Example 2.2.39 (Alexander splindle in which t acts invertibly). In Example 2.2.38, let $R = \mathbb{Z}$, $G = \mathbb{Q}$ and choose $t = 2$ with R acting on G by multiplication. Then noting that $t^{-1} = 2^{-1}$ does not exist in $\mathbb{Z}$, we have $a \triangleright b = 2a - b$. This is the quandle operation for the weighted average quandle with weight $t = 2$ and therefore satisfies the invertibility axiom. For all, $a, b \in \mathbb{Q}$, the equation $x \triangleright a = b$ has the unique solution $x = \frac{a+b}{2} \in \mathbb{Q}$. Therefore $(G, \triangleright)$ is a quandle.

Lemma 2.2.40. *Let R be a ring and choose $t \in R$ and let $(G, \triangleright)$ be an Alexander spindle so that for all $a, b \in G$ we have $\triangleright$ defined by $a \triangleright b = ta + (1 - t)b$. Then $(G, \triangleright)$ is a quandle if and only if t acts invertibly on G.*

Proof. Define $f : G \to G$ by $f(x) = tx$ the action of t on G. We need to show that G is a quandle if and only if f is a bijection.

If $(G, \triangleright)$ is a quandle then choose any $b \in G$. Since $x \triangleright a = b$ has a unique solution for all $a, b \in G$ we can choose $a = 0$ and we get from the definition of the quandle operation that $tx = b$ has a unique solution for all $b \in G$. Thus f is a bijection.

If f is a bijection then f^{-1} exists. Therefore since the equation $x \triangleright a = tx + (1 - t)a = b$ is equivalent to $xt = b - (1 - t)a = c$ which will have the unique solution $x = f^{-1}(c)$. Therefore we have established invertibility.

In an Alexander spindle both idempotence and right self-distributivity are guaranteed. Therefore $(G, \triangleright)$, is a quandle. $\square$

2.3 Racks and Quandle Preliminaries

In this section we present some further detail and elementary results relating to racks and quandles.

2.3.1 Symmetries

In a rack $(R, \triangleright)$, for fixed $y \in R$ we can think of $x \triangleright y$ as a function, S_y, that sends x to $x \triangleright y$ for all $x \in R$. We refer to each of these functions, S_y, as the *symmetry at y*. For consistency with $x \triangleright y$, we write xS_y, rather than the more familiar function notation, $S_y(x)$ as we foreshadowed in Remark 2.1.5, to indicate the result of the symmetry at y acting on x from the right, that is, $xS_y = x \triangleright y$. Since, by axiom Q2, for all $z \in R$ there exists a unique $x \in R$ such that $x \triangleright y = xS_y = z$, S_y is one-to-one and onto, that is S_y is a permutation of the elements of R, which is the motivation for calling these functions "the symmetry at y". Therefore there necessarily exists an inverse function, S_y^{-1}. The collection of these S_y^{-1}, for all $y \in R$, define the second binary operation, $\triangleleft$, in axiom Q2a.

Definition 2.3.1 (Joyce [16]). The function S_y is called the *symmetry* at y. For a rack, R, $S_y \in S_R$, the symmetric group on R, because it is a bijection. Further we will see in Section 3.3 that $S_y \in \operatorname{Aut}(R)$, the automorphism group of R.

Joyce's work was in terms of racks but it can easily be extended to quandles whenever we have idempotence. The quandle axioms can be rewritten in terms of these symmetries. For a quandle, Q, with symmetric group, S_Q:

1. **Idempotence.** For all $y \in Q$, y is a fixed point of the symmetry S_y, that is for all $y \in Q$, $yS_y = y$.

2. **Invertibility.** For all $y \in Q$ the symmetry at y, S_y is a bijection.

   That is S_y^{-1} exists and is a bijection and therefore the unique solution of $xS_y = z$ is $x = zS_y^{-1}$. For all $y, z \in Q$, the equation $xS_y = z$ has a unique solution. In other words, $xS_yS_y^{-1} = x$.

3. **Distributivity.** For all $y, z \in Q$ we have the following identity for the composition of symmetries:

   $$S_yS_z = S_zS_{yS_z}. \tag{2.3.1}$$

   This can be seen from the definitions of the functions S_y as shown below:

   $$\begin{aligned}(xS_y)S_z &= (x \triangleright y) \triangleright z \\ &= (x \triangleright z) \triangleright (y \triangleright z) \\ &= (xS_z) \triangleright (yS_z) \\ &= (xS_z)S_{yS_z}.\end{aligned}$$

Now since on both the left and the right we are operating on x by a composition of symmetries, we can equation the two compositions of symmetries to get equation (2.3.1). This is explored more below in Section 2.3.2.

2.3.2 The rack identity

Recall a rack satisfies the second and third quandle axioms. In a rack, the self-distributivity axiom can be thought of in multiple ways. It is sometimes referred to as the *rack identity.*

Fenn and Rourke [14] give three equivalent forms of the rack identity. The first form is as we have presented in the rack (or quandle) axioms. The second form is obtained from the first by substituting $w = x \triangleright z$ and rewriting that equation using the inverse rack operation as $x = w \triangleleft z$ in Axiom Q3 to obtain

$$((w \triangleleft z) \triangleright y) \triangleright z = w \triangleright (y \triangleright z).$$

Then by simply replacing the symbol w by x we can rewrite this as :

$$((x \triangleleft z) \triangleright y) \triangleright z = x \triangleright (y \triangleright z) \text{ — Axiom Q3 second form.}$$

This is true for all x, y, z in the rack.

The third form they obtain from the second by considering the rack operation, $x \triangleright y$, and the inverse operation, $x \triangleleft y$, as operators that operate on the element x by y. They use the exponential notation y^z to mean $y \triangleright z$ and $y^{\bar{z}}$

to mean $y \triangleleft z$ together with the understanding that $x^{yz} = (x \triangleright y) \triangleright z$ and $x^{y^z} = x \triangleright (y \triangleright z)$. Using this notation the second form of Axiom Q3 would be written:

$$x^{\overline{z}yz} = x^{y^z}, \tag{2.3.2}$$

for all x, y, z in the rack.

Here the equality in equation (2.3.2) means that the operators, $\overline{z}yz$ and y^z, are equivalent since we have equality when both operators are operating on an arbitrary element x. So the third form of Axiom Q3 is the operator equivalence of:

$$\overline{z}yz \equiv y^z \text{ — Axiom Q3 third form.}$$

In terms of symmetries the third form of the rack identity can be written:

$$S_z^{-1} S_y S_z = S_{yS_z}$$

where the operation on the left hand side, combining the symmetries, is function composition (from left to right). This is equivalent to equation (2.3.1) presented in Section 2.3.1 where the inverse operation had been shifted to the right hand side of the equation. Also note that the subscript on the right hand side, yS_z, is equivalent to y^z using exponential notation and $y \triangleright z$ using the standard binary operation notation.

2.3.3 The dual rack

Recall that the invertibility Axiom Q2 is equivalent to the existence of a second binary operation, $\triangleleft$, which satisfies Axiom Q2a. We show that whenever $(R, \triangleright)$ is a rack then $(R, \triangleleft)$ is a rack. This result seems to be known. Joyce [16] states without proof a distributivity axiom for the inverse operation together with similar results for two mixed operation distributivity identities, which we will prove in Section 2.3.4, that are analogous to the distributivity axiom on the primary operation. Nelson and Wong [22] note that the inverse operation is a bijection, thus between them Joyce and Nelson and Wong state the invertibility and self-distributivity axioms. Thus together their claim is that $(R, \triangleleft)$ is a rack. Nelson and Wong are actually working with quandles and explicitly claim that $(Q, \triangleleft)$ is a quandle. Moreover they call this quandle the *dual quandle* of $(Q, \triangleright)$. We will adopt that terminology of a *dual* rack or quandle in which the set is fixed but in which we are viewing the inverse rack operation as the primary rack operation and vice versa. Lopes and Roseman [18] prove that the dual rack is a rack for a finite rack. They also adopt the *dual rack* terminology for the rack $(R, \triangleleft)$ obtained from $(R, \triangleright)$ by using the inverse rack operation. There is no necessity to restrict the proof to finite racks and quandles and their proof can easily be extended to infinite racks and quandles. Although it is almost certainly well-known we provide a proof that the dual of a rack or a quandle is respectively a rack or a quandle.

Proposition 2.3.2. *Let* $(R, \triangleright)$ *be a rack. Then* $(R, \triangleleft)$ *is a rack. In addition, if* $(R, \triangleright)$ *is a quandle then* $(R, \triangleleft)$ *is a quandle.*

This proposition asserts, more explicitly in terms of both rack operations, that if $(R, \triangleright, \triangleleft)$ is a rack then so is $(R, \triangleleft, \triangleright)$. Obviously, these two racks have a strong relationship with each other since they each have the same set and the same two operations albeit playing different roles. We will adopt the terminology of Nelson and Wong referred to above and refer to the two racks as *dual racks.*

Definition 2.3.3 (Dual rack)**.** For any rack, $(R, \triangleright, \triangleleft)$, on the set R with primary rack operation, $\triangleright$, and inverse rack operation, $\triangleleft$, the rack $(R, \triangleleft, \triangleright)$ is called as the *dual rack* of $(R, \triangleright, \triangleleft)$. When the rack, R, is a quandle then the dual rack is also a quandle and we call it the *dual quandle.* The inverse operation, $\triangleleft$, can be referred to as the *dual operation* compared to the primary operation, $\triangleright$, or we may refer to the two operations, $\triangleright$ and $\triangleleft$ as *dual operations.*

This relationship is symmetric. That is, $(R, \triangleright, \triangleleft)$ has the dual rack $(R, \triangleleft, \triangleright)$ which in turn has the dual rack $(R, \triangleright, \triangleleft)$. Therefore the two racks, $(R, \triangleright, \triangleleft)$ and $(R, \triangleleft, \triangleright)$ are known as *dual* racks and if in addition idempotence holds then they are *dual* quandles.

Proof of Proposition 2.3.2. We need to check the two rack axioms.

1. Firstly, we check invertibility. Since R is a rack, for all $y, z \in R$ there exists a unique $x \in R$ such that $z = x \triangleright y$. This is equivalent to the symmetry, $S_y : R \to R$ with $xS_y = z$, being one-to-one and onto — a bijection. Therefore the inverse function $S_y^{-1} : R \to R$ with $zS_y^{-1} = x$

exists and is a bijection and as we noted previously in the preamble to this section, the collection of these inverse functions define the inverse rack operation. That is, for all $x, y \in R$ there exists a unique $z \in R$ such that $x = z \triangleleft y$.

2. Secondly, we check distributivity. We have from the third quandle Axiom Q3 for all $x, y, z \in R$

$$(x \triangleright y) \triangleright z = (x \triangleright z) \triangleright (y \triangleright z),$$

and we wish to show for all $x, y, z \in R$

$$(x \triangleleft y) \triangleleft z = (x \triangleleft z) \triangleleft (y \triangleleft z).$$

That is, the rack axioms imply right self-distributivity of the inverse quandle operation. We show the right self-distributivity of the inverse quandle operation by making a series of substitutions, which are well defined because of the uniqueness Axiom Q2 in R.

Given any $\xi, \gamma, \zeta \in R$ we let

$z = \zeta \in R$,

$y = \gamma \triangleleft z$, the unique element in R such that $\gamma = y \triangleright z$,

$u = \xi \triangleleft z$, the unique element in R such that $\xi = u \triangleright z$,

$x = u \triangleleft y$, the unique element in R such that $u = x \triangleright y$.

Note $\xi = u \triangleright z = (x \triangleright y) \triangleright z$. Therefore,

$$\begin{aligned}
\xi \triangleleft \zeta &= \big((x \triangleright y) \triangleright z\big) \triangleleft z = x \triangleright y \\
\gamma \triangleleft \zeta &= (y \triangleright z) \triangleleft z = y.
\end{aligned}$$

Therefore,

$$(\xi \triangleleft \zeta) \triangleleft (\gamma \triangleleft \zeta) = (x \triangleright y) \triangleleft y = x.$$

On the other hand,

$$\begin{aligned}
(\xi \triangleleft \gamma) \triangleleft \zeta &= \Big(\big((x \triangleright y) \triangleright z\big) \triangleleft (y \triangleright z)\Big) \triangleleft z \\
&= \Big(\big((x \triangleright z) \triangleright (y \triangleright z)\big) \triangleleft (y \triangleright z)\Big) \ \triangleleft z \\
&= (x \triangleright z) \triangleleft z \\
&= x.
\end{aligned}$$

Therefore we have,

$$(\xi \triangleleft \gamma) \triangleleft \zeta = x = (\xi \triangleleft \zeta) \triangleleft (\gamma \triangleleft \zeta),$$

which shows that the inverse quandle operation is right self-distributive for ξ, γ and ζ. However, since ξ, γ and ζ were any elements of R right self-distributivity applies to all elements of R. Therefore we have, for all $x, y, z \in R$

$$(x \triangleright y) \triangleright z = (x \triangleright z) \triangleright (y \triangleright z).$$

Therefore, since the rack axioms are satisfied, $(R, \triangleleft)$ is a rack.

If $(R, \triangleright)$ is a quandle then for all $x \in R$ we have idempotence, that is, $x = x \triangleright x$. By operating on both sides of the idempotence equation on the right by x with the inverse rack operation we have

$$x \triangleleft x = (x \triangleright x) \triangleleft x = x$$

and so we have idempotence in $(R, \triangleleft)$ and therefore $(R, \triangleleft)$ is a quandle. □

Remark 2.3.4. Since the operations, $\triangleright$ and $\triangleleft$, have symmetrical roles in a quandle or rack, both $(Q, \triangleright, \triangleleft)$ and $(Q, \triangleleft, \triangleright)$ are quandles and similarly both $(R, \triangleright, \triangleleft)$ and $(R, \triangleleft, \triangleright)$ are racks.

2.3.4 Distributivity laws

By definition of a rack the right distributivity axioms hold for both the rack operation and the inverse operation. As a consequence, we will show that similar right distributivity laws hold for the two expressions with mixed rack operations. As noted previously, this is a result stated but not proved by Joyce [16].

Lemma 2.3.5. *In any rack, R, with binary operations $\triangleright$ and $\triangleleft$, the distributivity laws*

$$(x \triangleright y) \triangleleft z = (x \triangleleft z) \triangleright (y \triangleleft z), \tag{2.3.3}$$

$$(x \triangleleft y) \triangleright z = (x \triangleright z) \triangleleft (y \triangleright z), \tag{2.3.4}$$

hold for all $x, y, z \in R$.

Proof. Let $x, y, z \in R$. Acting on the left hand side of equation (2.3.3) by z with the primary rack operation we get:

$$((x \triangleright y) \triangleleft z) \triangleright z = x \triangleright y.$$

Similarly, acting on the right hand side by z and applying the distributivity axiom in $(R, \triangleright)$, we get:

$$\begin{aligned}\Big((x \triangleleft z) \triangleright (y \triangleleft z)\Big) \triangleright z &= \Big((x \triangleleft z) \triangleright z\Big) \triangleright \Big((y \triangleleft z) \triangleright z\Big)\\ &= x \triangleright y.\end{aligned}$$

Since the results of these two calculations are equal we can apply the uniqueness axiom to deduce that:

$$(x \triangleright y) \triangleleft z = (x \triangleleft z) \triangleright (y \triangleleft z)$$

as required.

By a similar argument, or by applying the above result to the rack $(R, \triangleleft, \triangleright)$ — that is, swapping the roles of $\triangleright$ and $\triangleleft$ — we can deduce:

$$(x \triangleleft y) \triangleright z = (x \triangleright z) \triangleleft (y \triangleright z).$$

□

In addition, recall in Lemma 2.2.13 we showed that distributivity holds when there are repeated operations by the same elements. That is,

$$(x \triangleright^m y) \triangleright^n z = (x \triangleright^n z) \triangleright^m (y \triangleright^n z).$$

A similar law involving both the rack operation and the inverse rack operation can be shown to be true. That is, both

$$(x \triangleright^m y) \triangleleft^n z = (x \triangleleft^n z) \triangleright^m (y \triangleleft^n z)$$

and

$$(x \triangleleft^m y) \triangleright^n z = (x \triangleright^n z) \triangleleft^m (y \triangleright^n z)$$

hold. In both cases $x \triangleright^k y$ is understood to mean k repeated actions by the rack operation of y on x and similarly $x \triangleleft^k y$ is understood to mean k repeated actions by the inverse rack operation of y on x as defined in Definition 2.2.9.

Lemma 2.3.6. *In any rack, R, with binary operations $\triangleright$ and $\triangleleft$, the distributivity laws:*

$$(x \triangleright^m y) \triangleleft^n z = (x \triangleleft^n z) \triangleright^m (y \triangleleft^n z), \tag{2.3.5}$$

$$(x \triangleleft^m y) \triangleright^n z = (x \triangleright^n z) \triangleleft^n (y \triangleright^m z), \tag{2.3.6}$$

hold for all $x, y, z \in R$ and for all $m, n \in \mathbb{N}$.

Proof. We prove this lemma with a similar argument to the proof of Lemma 2.2.13 by two inductions first over m and then over n. Before beginning we note that proving either of equations (2.3.5) or (2.3.6) implies the other holds by for example, applying equation (2.3.5) to the rack $(R, \triangleleft, \triangleright)$ where the roles of the rack operations have been swapped. So we proceed to prove equation (2.3.5) by induction.

First we will prove that the simplified equation

$$(x \triangleright^m y) \triangleleft z = (x \triangleleft z) \triangleright^m (x \triangleleft z)$$

holds for all $m \in \mathbb{N}$. Note that Lemma 2.3.5 provides the base case for our induction, that is, we have in equation (2.3.3) that $(x \triangleright y) \triangleleft z = (x \triangleleft z) \triangleright (y \triangleleft z)$.

Assume that $(x \triangleright^k y) \triangleleft z = (x \triangleleft z) \triangleright^k (y \triangleleft z)$ for some $k \in \mathbb{N}$ and consider

$$\begin{aligned}
(x \triangleright^{k+1} y) \triangleleft z &= \Big((x \triangleright^k y) \triangleright y\Big) \triangleleft z && \text{by definition}\\
&= \Big((x \triangleright^k y) \triangleleft z\Big) \triangleright (y \triangleleft z) && \text{applying equation (2.3.3)}\\
&= \Big((x \triangleleft z) \triangleright^k (y \triangleleft z)\Big) \triangleright (y \triangleleft z) && \text{inductive assumption}\\
&= \Big((x \triangleleft z) \triangleright^{k+1} (y \triangleleft z)\Big) && \text{by definition.}
\end{aligned}$$

Therefore $(x \triangleright^m y) \triangleleft z = (x \triangleleft z) \triangleright^m (y \triangleleft z)$ for all $m \in \mathbb{N}$.

We now use this result as the base case to prove equation (2.3.5) by induction over n. So we have $(x \triangleright^m y) \triangleleft z = (x \triangleleft z) \triangleright^m (y \triangleleft z)$ and assume $(x \triangleright^m y) \triangleleft^k z = (x \triangleleft^k z) \triangleright^m (y \triangleleft^k z)$ is true for some $k \in \mathbb{N}$. We examine

$(x \triangleright^m y) \triangleleft^{k+1} z$:

$$
\begin{aligned}
(x \triangleright^m y) \triangleleft^{k+1} z &= \Big((x \triangleright^m y) \triangleleft^k z\Big) \triangleleft z && \text{by definition} \\
&= \Big((x \triangleleft^k z) \triangleright^m (y \triangleleft^k z)\Big) \triangleleft z && \text{inductive assumption} \\
&= \Big((x \triangleleft^k z) \triangleleft z\Big) \triangleright^m \Big((y \triangleleft^k z) \triangleleft z\Big) && \text{applying the base case} \\
&= (x \triangleleft^{k+1} z) \triangleright^m (y \triangleleft^{k+1} z) && \text{by definition.}
\end{aligned}
$$

Therefore $(x \triangleright^m y) \triangleleft^n z = (x \triangleleft^n z) \triangleright^m (y \triangleleft^n z)$ for all $m, n \in \mathbb{N}$. □

These distributivity rules can be combined into one rule for all $x, y, z \in R$ and for all $m, n \in \mathbb{Z}$ where it is understood that for $k < 0$, the operator $\triangleright^k$ is equivalent to the operator $\triangleleft^{-k}$ and for $k = 0$ the operator $\triangleright^0$ means there is no action so that $x \triangleright^0 y = x$. We formally adopt that as a definition of $\triangleright^k$. This extends Definition 2.2.9, which defined repeated applications of the quandle operation but was restricted to non-negative powers, so that any integer power of a quandle operation is defined.

Definition 2.3.7 (**Quandle operation power).** Given a rack $(R, \triangleright)$, for all $x, y \in R$ and for all $n \in \mathbb{Z}$ we define $x \triangleright^n y$ to mean:

1. For $n > 0$, n repeated actions of y by the rack operation on x, as in Definition 2.2.9,
2. For $n < 0$, $|n|$ repeated actions of y by the inverse rack operation on x as in Definition 2.2.9 applied to the inverse rack operation, and

3. For $k = 0$, no action of y on x, that is, $x \triangleright^0 y = x$.

We now can consolidate Lemmas 2.2.13 and 2.3.5 into one statement that for all $m, n \in \mathbb{Z}$,

$$(x \triangleright^m y) \triangleright^n z = (x \triangleright^n z) \triangleright^m (y \triangleright^m z).$$

The proof replicates the proofs in those lemmas therefore we state the following consolidated distributivity rule without proof as a corollary of the earlier results.

Corollary 2.3.8 (Consolidated distributivity rule). *In any rack,* $(R, \triangleright)$*, for all* $x, y, z \in R$ *and for all* $m, n \in \mathbb{Z}$ *we have distributivity over* $\triangleright^m$ *and* $\triangleright^n$ *as follows:*

$$(x \triangleright^m y) \triangleright^n z = (x \triangleright^n z) \triangleright^m (y \triangleright^n z). \tag{2.3.7}$$

2.3.5 Subracks and subquandles

Some subsets of a rack or a quandle are racks or quandles in their own right. Therefore it is useful to introduce the concept of subrack and subquandle.

Subrack and subquandle definitions and examples

In this section we give definitions of subracks and subquandles. First we define the restriction of a binary operation defined on a set to a subset of that set.

Definition 2.3.9 (Restriction of a binary operation). Given a set S

together with a binary operation $\triangleright$ and a subset $P \subseteq S$, then we define $\triangleright|_{P\times P}$ to mean the restriction of the binary operation $\triangleright$ to $P \times P$.

We now define the terms subrack and subquandle.

Definition 2.3.10 (Subrack). A subset P of a rack $(R, \triangleright)$ is a *subrack* if and only if $(P, \triangleright|_{P\times P})$ is a rack. In addition, if R is a quandle and $(P, \triangleright|_{P\times P})$ is a subrack then since idempotence will be preserved in the subrack, $(P, \triangleright|_{P\times P})$ is a *subquandle* of R.

Remark 2.3.11. We could similarly and formally define the concepts of *subspindle* and *subshelf* as subsets that together with the shelf operation restricted to the subset defines a spindle or shelf respectively.

We now give some examples of subracks and subquandles. The first two examples are rather trivial in nature with the second being more useful than the first. The first example is valid only if we allow racks and quandles to be empty sets and there is no reason not to.

Example 2.3.12 (Empty set). The empty set, $\emptyset$, is a subrack or a subquandle since the rack and quandle axioms hold vacuously.

Singletons in a quandle define a subquandle.

Example 2.3.13 (Singleton quandle). For any element, x, in any quandle, Q, the singleton $\{x\}$ is a subquandle. The quandle axioms are easily checked. This is not true in general in a rack since $x \triangleright x$ is not necessarily even in $\{x\}$.

That is, in a rack, a singleton set is not necessarily even closed under the restricted rack operation.

Example 2.3.14 (Subquandle of a Takasaki kei). Let $(K, \triangleright)$ be the Takasaki kei defined in Example 2.2.31. The subset of even integers, $E = \{x \in \mathbb{Z} : x = 2n, n \in \mathbb{Z}\} \subseteq K$, is a subquandle of the Takasaki kei. Axioms Q1 and Q3 follow immediately in the subset E since they apply in $(K, \triangleright)$ and by noting that if $x, y \in E$ then $x \triangleright y = 2y - x \in E$. Axiom Q2 is established since $x \triangleright y = z$ has the unique solution $x = y \triangleright z$ since the Takasaki kei is involutory and since we have $y, z \in E$ then necessarily $x \in E$.

Similarly, the subset of odd integers $O = \{x \in \mathbb{Z} : x = 2n+1, n \in \mathbb{Z} \subseteq K$ can be shown to be a subquandle of the Takasaki kei since $x \triangleright y = 2y - x \in O$ whenever $x, y \in O$.

By definition every rack, R, has at least two subracks, $\emptyset$ and R itself.[3] As for subsets where we have a definition of a proper subset, it is useful to define a proper subrack of R as not being R itself.

Definition 2.3.15 (Proper subrack or subquandle). A subrack, P, of a rack, R, is a *proper subrack* of a rack of R, if and only if $P \neq R$. Similarly, a subquandle, P, of a quandle, Q, is a *proper subquandle* of a quandle of Q, if and only if $P \neq Q$.

---

[3] It will turn out convenient to consider that $\emptyset$ is a subrack when, in Section 2.3.6, we look at Q-complemented subquandles, in which the complement of a subquandle is a subquandle. In particular, Lemma 2.3.34 states that the intersection of two Q-complemented quandles is Q-complemented and that will not be true if the intersection is the empty set and the empty set was not considered to be a subquandle.

Subrack and subquandle tests

We need only work with racks since any result for a rack will trivially extend to a quandle. This is because in a quandle we have idempotence, that is, $x \triangleright x = x$, and it is easily seen that idempotence is preserved for any subset of a quandle. Therefore, since every quandle is a rack a subtest for a subrack will automatically extend to any subset of a quandle and we effectively get idempotence in the subquandle for free.

To test that a subset, P, of a rack, R, is a subrack it turns out that it is sufficient to test the subset, $P \subseteq R$, is closed under the rack operations. Moreover, for a finite subset we will see that it is sufficient to check for closure under only one of the rack operations. There is some confusion in the literature as to whether it is necessary to check closure under both operations. For example Nelson and Wong [22] state a lemma in which it is claimed it is sufficient to check closure under only one operation.

They argue that if we write $a \triangleright b = f_b(a)$ then f_b is a bijection and so is the restriction to a subset $X \subseteq Q$, $f_b|_X$ and therefore invertibility is satsified. Implicitly this relies on $f_b^{-1}|_X$ doing the work to solve $x \triangleright a = b$. This works for a finite set as a function $f : X \to X$ that is one-to-one implies the function is onto. However, when the set has infinite cardinality a function, $f : X \to X$ that is one-to-one no longer implies that the function is onto the set. Therefore there may be some equations $x \triangleright a = b$ for which there is no solution.

Thus, testing one operation is indeed not sufficient in general. A subrack needs to be closed under both the rack operation and the inverse operation. The counterexample presented in Example 2.3.20 shows a subset that is closed under only the rack operation is not necessarily a subquandle. Elsewhere, for example in Anderson et al [1] it is correctly stated that the subquandle needs to be finite for closure under only one operation to be sufficient. They do not state or prove a condition for infinite (sub)quandles. For completeness, we give a proof here that closure under both rack operations is necessary and sufficient for a subset to be a subrack — this proof and the following proof for finite racks are almost certainly well-known. After which, in Lemma 2.3.17, we will show that for a finite rack closure under one operation is sufficient for a subset to be a subrack. That is in a finite rack closure of one operation in a subset necessarily implies closure under the other rack operation.

Lemma 2.3.16 (Subrack test). *Let R be a rack. A subset, $P \subseteq R$, is a subrack if and only if P is closed under $\triangleright$ and $\triangleleft$.*

In addition, when the rack is a quandle, the subrack will be a subquandle.

Proof. If P is a subrack then when $\triangleright$ and $\triangleleft$ are restricted to P, P is necessarily closed since $\triangleright$ and $\triangleleft$ are binary operations on P.

If P is closed under the binary operations, $\triangleright$ and $\triangleleft$, then we need to check the two rack axioms.

The distributivity axiom is automatically true in P, since it is true in R. From Axiom Q3 we have, for all $x, y, z \in R$, $(x \triangleright y) \triangleright z = (x \triangleright z) \triangleright (y \triangleright z)$, therefore, in particular, for all $x, y, z \in P \subseteq R$, $(x \triangleright y) \triangleright z = (x \triangleright z) \triangleright (y \triangleright z)$. Moreover since P is closed under $\triangleright$, $(x \triangleright y) \triangleright z \in P$.

For uniqueness we have from Axiom Q2 in R, for all $y, z \in P \subseteq R$, there exists a unique $x \in R$ such that $x \triangleright y = z$. Since P is closed under $\triangleleft$, $x = z \triangleleft y \in P$. Therefore, for all $y, z \in P$, there exists a unique $x \in P$ such that $x \triangleright y = z$.

Therefore P is a subrack of R.

As noted above if the rack is a quandle so that we have idempotence then the subrack is a subquandle. We get this effectively for free as follows: From Axiom Q1 we have, for all $x \in R$, $x \triangleright x = x$, therefore, in particular, for all $x \in P \subseteq R$, $x \triangleright x = x \in P$. $\square$

When the subset $P \subseteq R$ is finite we can simplify testing that P is a subrack further. In this case, it is sufficient to show closure under either one of the binary operations. This is because, in a finite quandle the uniqueness in Axiom Q2 guarantees that the symmetry S_y is onto for all $y \in P$ and therefore P will be closed under the inverse operation.

More generally, in a finite set a function from that set to itself is onto if and only if it is one-to-one, which in turn implies that the inverse function is one-to-one and onto. This is not true in an infinite set, for example, in $\mathbb{Z}$, $n \mapsto 2n$ is one-to-one but it is not onto and $n \mapsto \lfloor \frac{n}{2} \rfloor$ is onto but it is not one-to-one.

Lemma 2.3.17 (Finite subrack). *Let R be a rack. A finite subset, $P \subseteq R$, is a subrack if and only if P is closed under $\triangleright|_{P\times P}$, the rack operation restricted to elements in the subset, R.*

In addition, when the rack is a quandle, the subrack will be a subquandle.

Proof. As in Lemma 2.3.16, if P is a finite subrack then when $\triangleright$ is restricted to P, P is necessarily closed since $\triangleright$ is a binary operation on P.

Let P be a finite subset of R and let P be closed under the operation $\triangleright$.

From Axiom Q2 in R we have for all $y, z \in R$ there exists a unique $x \in R$ such that $z = x \triangleright y$. In particular, this is true for all $y, z \in P$. We need to show that when $y, z \in P$ then $x \in P$.

Since P is closed under $\triangleright$, for $y \in P$ we have that for all $x \in P$, $x \triangleright y = xS_y|_P \in P$, where $S_y|_P$ is the restriction of the symmetry at y, S_y, in R to P,

$$S_y|_P : P \to P, \quad xS_y|_P = x \triangleright y.$$

Since S_y is a bijection therefore $S_y|_P$ is one-to-one, and since P is finite and closed under $\triangleright$ therefore $S_y|_P$ is onto. Therefore $S_y|_P$ is a bijection. Therefore for all $z \in P$ there exists a unique $\xi \in P$ such that $\xi S_y = z$. Since there exists a unique $x \in R$ satisfying $x \triangleright y = z$ and $xS_y = z$ and $\xi S_y = z$ then since $\xi \in P \subseteq R$ we have $x = \xi \in P$.

Therefore P is a subrack of R.

Precisely as before in Lemma 2.3.16, we get idempotence for free if the rack is a quandle. So in a finite quandle any subset closed under one quandle operation is a subquandle. □

Remark 2.3.18. Alternatively, having established that $S_y|_P$ is a bijection from P to P we immediately have that $S_y^{-1}|_P$ exists and is a bijection from P to P. Since $S_y^{-1}|_P$ defines the inverse operation $\lhd|_{P\times P}$ we have that P is closed under $\rhd|_{P\times P}$ implies closure under $\lhd|_{P\times P}$. Therefore by Lemma 2.3.16 we have that P is a subrack .

Remark 2.3.19. Since Quandle Axiom Q2 implies the existence of an inverse operation $\lhd$, therefore, if $(P, \rhd)$ is a subquandle of $(Q, \rhd)$ then the dual subquandle $(P, \lhd)$ will also be a subquandle of the dual quandle $(Q, \lhd)$. Similarly, if $(P, \rhd)$ is a subrack of $(R, \rhd)$ then the dual subrack $(P, \lhd)$ will also be a subrack of the dual rack $(R, \lhd)$.

Kamada [17] gives some examples of subsets of quandles that are closed under the quandle operation but that are not subquandles. A simpler example has been given in an anonymous blog post [2]. We slightly modify that example and present it here.

Example 2.3.20 (A subquandle non-example). Let $Q = \mathbb{R}$ with operation $x \rhd y = \frac{x+y}{2}$. This is the averaging quandle example that we showed was a quandle in Example 2.2.28 except that in that example we used the rational numbers rather than the real numbers here. Nevertheless the proof that this example is a quandle is effectively the same as in the previous example and so will not be repeated here. However, in this quandle the subset of positive real numbers, $\mathbb{R}^+$, is closed under $\triangleright$ — for all $x, y \in \mathbb{R}^+$, $\frac{x+y}{2} \in \mathbb{R}^+$ — but it is not true that for all $y, z \in \mathbb{R}^+$, $x = 2z - y$ has a solution $x > 0$. It is easy to see that $x > 0$ only if $y < 2z$. Therefore the invertibility axiom is not satisfied in $(\mathbb{R}^+, \triangleright)$. There is a unique solution $x \in \mathbb{R}$ but it is not necessarily in $\mathbb{R}^+$. For example, $x \triangleright 3 = \frac{x+3}{2} = 1$ has the solution $x = -1 \notin \mathbb{R}^+$.

The subset in this example fails to be a subquandle because while the bijective functions $S_y : \mathbb{R} \to \mathbb{R}$ defined by the quandle operation when restricted to the positive real numbers define a function that is $S_y|_{\mathbb{R}^+} : \mathbb{R}^+ \to \mathbb{R}^+$, as required, and these restricted functions are one-to-one, since S_y is one-to-one, they are not onto $\mathbb{R}^+$. For given $y \in \mathbb{R}^+$, the function $S_y : \mathbb{R}^+ \to \mathbb{R}^+$, where $xS_y = x \triangleright y$, is onto the subset $\left(\frac{y}{2}, \infty\right) \subseteq \mathbb{R}^+$, since $y \in \mathbb{R}^+$. So taking $z \in (0, \frac{y}{2}) \subseteq \mathbb{R}^+$ necessarily leads to an equation $x \triangleright y = z$ without a solution in $\mathbb{R}^+$.

By contrast, for a finite subset, P, of a rack, R, $P \subseteq R$, and restricted symmetries at $y \in P$, $S_y|_P : P \to P$, $S_y|_P$ being one-to-one implies that $S_y|_P$ is also onto and so is a bijection.

2.3.6 Orbits

The concept of orbit is well known from group theory and can be extended to racks and quandles. We prove a number of useful lemmas and corollaries on orbits. The Lemmas 2.3.22, 2.3.28 and 2.3.33 and their corollaries are likely to be well known but we have not found them explicitly stated in the literature, so we provide our proofs of those results here.

Definition 2.3.21 (Orbit). Let R be a rack and let $a \in R$. We define the *orbit* of a to be the set of all elements $b \in R$, that can be written as:

$$b = (\cdots((a \triangleright^{k_1} x_1) \triangleright^{k_2} x_2) \cdots) \triangleright^{k_n} x_n,$$

where $x_1, x_2, \ldots, x_n \in R$ and $k_1, k_2, \ldots, k_n \in \{1, -1\}$, with $\triangleright^1 = \triangleright$ and $\triangleright^{-1} = \triangleleft$.

We will write $O(a)$ to represent the orbit of a.

For a quandle, Q, we can show that the orbits of the elements of Q are equivalence classes of an equivalence relation. This is not true in general for racks because we require reflexivity which in the case of quandles comes from the idempotence axiom but is not necessarily true in a rack.

Lemma 2.3.22. *On a quandle, Q, define $a \sim b$ if and only if $a \in O(b)$. Then $\sim$ is an equivalence relation.*

Proof. Let Q be a quandle and let $a \sim b$ if and only if $a \in O(b)$. The relation, $\sim$, is:

1. **Reflexive** — For $a \in Q$, $a \in O(a)$ since $a \triangleright a = a$.
2. **Symmetric** — For $a, b \in Q$, $a \in O(b)$ implies $b \in O(a)$.

   Let $a \in O(b)$. Then $a = (\cdots((b \triangleright^{k_1} x_1) \triangleright^{k_2} x_2) \cdots) \triangleright^{k_n} x_n$ which implies that $b = (\cdots((a \triangleright^{-k_n} x_n) \triangleright^{-k_{n-1}} x_{n-1}) \cdots) \triangleright^{-k_1} x_1 \in O(a)$.

3. **Transitive** — For $a, b, c \in Q$, $a \in O(b)$ and $b \in O(c)$ implies $a \in O(c)$.

   Let $a \in O(b)$. Then

   $$a = (\cdots((b \triangleright^{k_1} x_1) \triangleright^{k_2} x_2) \cdots) \triangleright^{k_n} x_n.$$

   Similarly, let $b \in O(c)$. Then

   $$b = (\cdots((c \triangleright^{l_1} y_1) \triangleright^{l_2} y_2) \cdots) \triangleright^{l_m} y_m.$$

   Therefore

   $$\begin{aligned} a &= [\cdots[[((\cdots((c \triangleright^{l_1} y_1) \triangleright^{l_2} y_2) \cdots) \triangleright^{l_m} y_m) \triangleright^{k_1} x_1] \triangleright^{k_2} x_2] \cdots] \triangleright^{k_n} x_n \\ &\in O(c). \end{aligned}$$

Therefore $\sim$ is an equivalence relation. $\square$

Remark 2.3.23. The equivalence class of a, $[a]$, is the orbit of a, $O(a)$. Since the equivalence classes of an equivalence relation partition a set, the orbits of the elements of Q partition Q. That is, $Q = \bigcup_{a \in Q} O(a)$, with $O(a) = O(b)$ or $O(a) \cap O(b) = \emptyset$, for all $a, b \in Q$.

We will call a rack connected if it has only one orbit. This follows an equivalent definition by Nelson and Wong [22] of a connected quandle.

Definition 2.3.24 (Connected). Let R be a rack. If for all $x, y \in R$, $x \in O(y)$, then we say that the rack R is *connected*.

Nelson and Wong [22] introduce the concept of a subquandle, $P \subseteq Q$, being *Q-complemented* if and only if $Q \setminus P$ is also a subquandle.

Definition 2.3.25 (**Q-complemented, Nelson and Wong [22]**)**.** Let Q be a quandle and let $P \subseteq Q$ be a subquandle. We say that P is *complemented in Q* or *Q-complemented* if $Q \setminus P$ is a subquandle of Q. A quandle, Q, is *complementary* if it has a proper non-empty Q-complemented subquandle.

Remark 2.3.26. Every quandle, Q, is Q-complemented in itself since the empty set, $\emptyset$, is a subquandle, with the quandle axioms being vacuously satisfied. Therefore the condition on the Q-complemented subquandle to be proper is necessary otherwise every quandle would be complementary.

Remark 2.3.27. It is easily seen that it is not true in general that every subquandle, $P \subseteq Q$, is Q-complemented. For example, any singleton $\{x\} \subseteq Q$ is a subquandle but $Q \setminus \{x\}$ is typically not a subquandle. In particular, $Q \setminus \{x\}$ may not be closed as it may be possible to find $y, z \in Q \setminus \{x\}$ such that $y \triangleright z = x$.

Indeed, only the trivial quandle has the property that every singleton is Q-complemented. If, for all $y, z \in Q \setminus \{x\}$, we have $y \triangleright z \neq x$ then since, by Axiom Q2, every equation of the form $w \triangleright z = x$ has a solution, necessarily $x \triangleright z = x$ for all $z \in Q$. If this property is true for all singletons $\{x\} \subseteq Q$ then Q must be the trivial quandle.

We now show that the orbits of a quandle, Q, are Q-complemented subquandles. First we show that the orbits of a quandle are subquandles. This result relies on the fact that the orbits are invariant sets. That is, $O(a)S_b \subseteq O(a)$ and $O(a)S_b^{-1} \subseteq O(a)$ for all $b \in Q$, where for any $b \in Q$ we define

$$O(a)S_b = \{xS_b : x \in O(a)\},$$

which in terms of the quandle operation is equivalent to

$$O(a) \triangleright b = \{x \triangleright b : x \in O(a)\},$$

and

$$O(a)S_b^{-1} = \{xS_b^{-1} : x \in O(a)\},$$

which in terms of the quandle operation is equivalent to

$$O(a) \triangleleft b = \{x \triangleleft b : x \in O(a)\}.$$

In fact, the stronger result that $O(a)S_b = O(a)$ and $O(a)S_b^{-1} = O(a)$ can be shown to be true.

Lemma 2.3.28. *Let Q be a quandle with $a \in Q$. Then*

$$O(a)S_b = O(a) \text{ and } O(a)S_b^{-1} = O(a)$$

for all $b \in Q$.

Proof. First we will show that $O(a)S_b \subseteq O(a)$ and $O(a)S_b^{-1} \subseteq O(a)$.

Let $b \in Q$ and $c \in O(a)$. Then $c \triangleright b$ is a general element in $O(a)S_b$. We need to show that $c \triangleright b$ is in $O(a)$.

We have $c = (\cdots((a \triangleright^{k_1} x_1) \triangleright^{k_2} x_2)\cdots) \triangleright^{k_n} x_n$ for some $x_1, x_2, \ldots, x_n \in Q$ and $k_1, k_2, \ldots, k_n \in \{1, -1\}$. Now

$$c \triangleright b = ((\cdots((a \triangleright^{k_1} x_1) \triangleright^{k_2} x_2)\cdots) \triangleright^{k_n} x_n) \triangleright b \in O(a),$$

by the definition of an orbit. Therefore $O(a)S_b \subseteq O(a)$.

Similarly, we can show that

$$c \triangleleft b = ((\cdots((a \triangleright^{k_1} x_1) \triangleright^{k_2} x_2)\cdots) \triangleright^{k_n} x_n) \triangleleft b \in O(a),$$

and therefore $O(a)S_b^{-1} \subseteq O(a)$.

Now we show that $O(a) \subseteq O(a)S_b$ and $O(a) \subseteq O(a)S_b^{-1}$. We choose some $y \in O(a)$ and consider the equation $y = z \triangleright b$, which by the quandle Axiom Q2 we know has a unique solution $z \in Q$. We can solve this equation to get $z = y \triangleleft b$ and we can apply the result in the first part of the proof of this lemma that when $y \in O(a)$ and $b \in Q$ we have $z = y \triangleleft b \in O(a)$. Therefore $y = z \triangleright b \in O(a)S_b$ and $O(a) \subseteq O(a)S_b$.

Similarly, by considering the equation $y = z' \triangleleft b$ we see that $z' = y \triangleright b \in O(a)$ and therefore $y = z' \triangleleft b \in O(a)S_b^{-1}$ and $O(a) \subseteq O(a)S_b^{-1}$.

Therefore, both

$$O(a)S_b = O(a),$$

and

$$O(a)S_b^{-1} = O(a).$$

$\square$

Since both $O(a)S_b = O(a)$ and $O(a)S_b^{-1} = O(a)$ for all $b \in Q$ it is certainly true for all $b' \in O(a)$. We can use that fact to show that any particular orbit is closed under both of the binary operations. Closure under both binary operations is precisely the condition that we need to establish that a subset is a subquandle.

Corollary 2.3.29 (Every orbit is a subquandle). *Let Q be a quandle and let $a \in Q$. Then the orbit of a, $O(a)$, is a subquandle of Q.*

Proof. An immediate consequence of Lemma 2.3.28 is that for each $b \in Q$ the symmetry S_b at b when restricted to the orbit of $a \in Q$ is onto $O(a)$. That is $S_b|_{O(a)} : O(a) \to O(a)$ for all $b \in Q$. If we restrict b so that $b \in O(a)$ the symmetry at b restricted to $O(a)$ will still be onto $O(a)$. That necessarily means that $O(a)$ is closed under the restricted operation $\triangleright|_{O(a)}$.

Similarly, $O(a)$ is closed under the restricted inverse operation, $\triangleleft|_{O(a)}$, since $S_b^{-1}|_{O(a)}$ is also onto $O(a)$. Closure under both binary operations from Lemma 2.3.16 implies that $O(a)$ is a subquandle as required. $\square$

Moreover, the result in Corollary 2.3.29 can be extended to the union of orbits.

Corollary 2.3.30. *Let Q be a quandle. Let $A \subseteq Q$. Then the union of orbits, $\bigcup\limits_{a\in A} O(a)$, is a subquandle.*

Proof. Choose $b, c \in \bigcup\limits_{a\in A} O(a)$ with $b \in O(a_1)$ and $c \in O(a_2)$ for some $a_1, a_2 \in A$. Then

$$b \triangleright c = bS_c \in O(a_1) \subseteq \bigcup_{a\in A} O(a)$$

and similarly,

$$b \triangleleft c = bS_c^{-1} \in O(a_1) \subseteq \bigcup_{a\in A} O(a).$$

Therefore the union of orbits, $\bigcup\limits_{a\in A} O(a)$, is closed under both binary operations restricted to $\bigcup\limits_{a\in A} O(a)$ and we have that the union of orbits is a subquandle. $\square$

Corollary 2.3.31. *Let Q be a quandle and let $a \in Q$. Then the orbit of a, $O(a)$, is a Q-complemented subquandle of Q.*

Proof. We show this by simply noting that $Q \setminus O(a)$ is a union of orbits of elements of Q and applying Corollary 2.3.30. That is,

$$Q \setminus O(a) = \bigcup_{b\notin O(a)} O(b).$$

Therefore $Q \setminus O(a)$ is a Q-complemented subquandle of Q. $\square$

We can show that any union of orbits is a Q-complemented subquandle by a similar argument.

Corollary 2.3.32. *Let Q be a quandle. Let $A \subseteq Q$. Then the union of orbits, $\mathcal{A} = \bigcup_{a \in A} O(a)$, is a Q-complemented subquandle of Q.*

Proof. Since $Q \setminus \mathcal{A} = \bigcup_{b \notin \mathcal{A}} O(b)$ is a union of orbits it is a subquandle and therefore $\mathcal{A} = \bigcup_{a \in A} O(a)$ is Q-complemented. □

To use the orbits of a quandle as fundamental building blocks of the quandle we need to establish that they have no Q-complemented proper subquandles.

Lemma 2.3.33. *Let Q be a quandle and let $a \in Q$. Then the orbit of a, $O(a)$, has no Q-complemented proper subquandle.*

Proof. Suppose $R(a)$ is a Q-complemented proper subquandle of $O(a)$.

Without loss of generality, we can assume $a \in R(a)$. As if not, then since $R(a)$ is non-empty there must exist $b \in R(a) \subsetneq O(a)$, but then we have $O(a) = O(b)$. Therefore by renaming $R(a)$ as $R(b)$ we have $b \in Q$ and $O(b)$ satisfying the conditions of the lemma.

Since $R(a)$ is Q-complemented we have $Q \setminus R(a)$ is a subquandle and therefore closed under $\triangleright$ and $\triangleleft$. That is, for all $x, y \in Q \setminus R(a)$,

$$x \triangleright y = xS_y \in Q \setminus R(a),$$

and

$$x \triangleleft y = xS_y^{-1} \in Q \setminus R(a).$$

Let $b \in R(a)$. Let $y \in Q$. Consider $b \triangleright y = bS_y$. We claim that $bS_y \in R(a)$. There are two cases:

1. If $y \in R(a)$, then $bS_y \in R(a)$ since $R(a)$ is a subquandle.
2. If $y \in Q \setminus R(a)$, that is $y \notin R(a)$, then assume that $z = bS_y \notin R(a)$. Then $b = bS_yS_y^{-1} = zS_y^{-1} \in Q \setminus R(a)$ since $z \in Q \setminus R(a)$ and $Q \setminus R(a)$ is a subquandle. However, that contradicts that we chose $b \in R(a)$. Therefore $z = bS_y \in R(a)$.

Therefore for all $y \in Q$, $bS_y \in R(a)$. Similarly, we can argue that for all $b \in R(a)$ and for all $y \in Q$, $b \triangleleft y \in R(a)$.

Therefore, for all $b \in R(a)$ and for all $x_1, x_2, \ldots, x_n \in Q$,

$$(\cdots((b \triangleright^{k_1} x_1) \triangleright^{k_2} x_2) \cdots) \triangleright^{k_n} x_n \in R(a).$$

In particular this is true for $b = a$:

$$(\cdots((a \triangleright^{k_1} x_1) \triangleright^{k_2} x_2) \cdots) \triangleright^{k_n} x_n \in R(a),$$

but this is the definition of the orbit of a. Therefore $O(a) \subseteq R(a) \subsetneq O(a)$ which is a contradiction since $R(a)$ is a proper subset of $O(a)$ and therefore $O(a)$ has no Q-complemented proper subset. $\square$

Finally, in this chapter we visit a lemma of Nelson and Wong. Nelson and Wong's proof of their Lemma 2 [22] that the intersection of two sub-quandles is a subquandle and moreover if the subquandles are Q-complemented then so is the intersection is not quite correct. In the proof, they rely on a previously stated result in Lemma 1 of their paper that closure under the quandle operation implies that a subset is a subquandle — that check is sufficient in some cases, for example, when the quandle is finite. Consequently, in their proof they only check for closure under the quandle operation and omit checks of closure under the inverse quandle operation as we have shown to be required in general in Lemma 2.3.16. Therefore their proof only covers the cases where closure under one operation implies closure under the inverse operation, for example finite quandles. The proof is very easily extended to any quandle by simply checking for closure under the inverse quandle operation in both the intersection, for the first part of the lemma, and in the Q-complement of the intersection in the second part of the lemma. For completeness, we present that result here and add the checks on the closure of the inverse operation to the proof.

Lemma 2.3.34. *Let Q be a quandle and let X and Y be subquandles of Q. Then the intersection $X \cap Y$ is a subquandle of Q. Moreover if X and Y are Q-complemented then $X \cap Y$ is Q-complemented.*

Proof. Suppose Q is a quandle with $X \subseteq Q$ and $Y \subseteq Q$ as subquandles. Let $\xi, \eta \in X \cap Y$. Then $\xi, \eta \in X$ and $\xi, \eta \in Y$. We have $\xi \triangleright \eta \in X$, $\xi \triangleleft \eta \in X$, $\xi \triangleright \eta \in Y$, and $\xi \triangleleft \eta \in Y$, therefore $\xi \triangleright \eta \in X \cap Y$ and $\xi \triangleleft \eta \in X \cap Y$. Therefore $X \cap Y$ is closed under $\triangleright$ and $\triangleleft$ and therefore by Lemma 2.3.16, $X \cap Y$ is a subquandle of Q.

Suppose X and Y are Q-complemented and consider $Q \setminus (X \cap Y) = (Q \setminus X) \cup$

$(Q \setminus Y)$. Let $x, y \in Q \setminus (X \cap Y)$. There are four cases to consider depending on the location of x and y:

1. When $x, y \in Q \setminus X$, since $Q \setminus X$ is a subquandle

   $$x \triangleright y \in Q \setminus X \subseteq Q \setminus (X \cap Y)$$

   and similarly

   $$x \triangleleft y \in Q \setminus X \subseteq Q \setminus (X \cap Y).$$

2. When $x, y \in Q \setminus Y$ a similar argument to Case 1 above shows that $x \triangleright y \in Q \setminus (X \cap Y)$ and $x \triangleleft y \in Q \setminus (X \cap Y)$.

3. When $x \in Q \setminus X$ and $y \notin Q \setminus X$, therefore $y \in X$, consider $x \triangleright y = z$.

   Suppose $z \in X$. Therefore $z \triangleleft y = x$, but $z \triangleleft y \in X$ since X is closed under $\triangleleft$. This contradicts $x \in Q \setminus X$. Therefore

   $$z \in Q \setminus X \subseteq Q \setminus (X \cap Y).$$

   Similarly, considering $x \triangleleft y = z'$ leads to the conclusion that

   $$z' \in Q \setminus X \subseteq Q \setminus (X \cap Y).$$

4. When $x \in Q \setminus Y$ and $y \notin Q \setminus Y$ a similar argument to Case 3 above shows that $x \triangleright y \in Q \setminus (X \cap Y)$ and $x \triangleleft y \in Q \setminus (X \cap Y)$.

Therefore in all cases $Q \setminus (X \cap Y)$ is closed under $\triangleright$ and $\triangleleft$ and therefore is a subquandle. Therefore $(X \cap Y)$ is Q-complemented. $\square$

Chapter 3

Congruences, Quotients, and Homomorphisms

In this chapter we will traverse the concepts of congruences, quotients, and homomorphisms as they apply to racks and quandles. For our purposes, congruences are equivalence relations applied to racks and quandles that preserve one or both rack operations. From a congruence we can build a coarser structure known as a quotient from which properties of the rack or quandle can be deduced.

Homomorphisms, isomorphisms, and automorphisms are well known concepts from abstract algebra. We will conclude the chapter by providing isomorphism theorems for racks and quandles.

3.1 Congruences

A congruence is a familiar concept more generally in abstract algebra. A congruence is an equivalence relation on a set with an operation that respects the operation. As a consequence, the operation is well defined on the equivalence classes formed from the equivalence relation. In the context of racks and quandles we will be interested in sets with two binary operations. A congruence can be defined more generally on sets with any number of operations with any arity. Therefore we will begin with a meta-definition of a congruence that can be applied to any algebraic structure with an operation of any arity. As we will need to use the concept of a congruence in racks and quandles with two operations, we will then extend the definition to algebraic structures with multiple operations. From there we will apply that definition to quandles, racks, shelves, and spindles.

3.1.1 Meta-definition of congruence

A congruence is an equivalence relation that respects an operation on a set. The racks and quandles we are interested in have two operations. The key issue that we will be investigating is under what conditions do equivalence relations respect one but not the other operation. So it is helpful to have both a weak definition of a congruence for whenever any set operation is respected and stronger and more specific definitions that describe precisely which operations are respected. We will formally make a generic definition of a congruence before making specific definitions that are related to the operations and structure in a set.

Definition 3.1.1 (Congruence). Let $\sim$ be an equivalence relation on a set S and $\phi = \phi(x_1, \ldots, x_n)$ be a n-ary operation on S. We say that $\sim$ is a *ϕ-congruence* when $a_i \sim b_i$ for $i = 1, \ldots, n$ implies $\phi(a_1, \ldots, a_n) \sim \phi(b_1, \ldots, b_n)$.

We will call the conditional statement that if, for all $i \in \{1, 2, \ldots, n\}$, $a_i \sim b_i$ then $\phi(a_1, a_2, \ldots, a_n) \sim \phi(b_1, b_2, \ldots, b_n)$ the *ϕ-congruence condition.*

If S has multiple operations ϕ_i, for $i = 1, 2, \cdots, k$ then we write *ϕ_i-congruence* when we want to emphasise which operations are respected by a particular equivalence relation. We use the standalone term *congruence* loosely to mean that there is at least one i for which we have a ϕ_i-congruence. Where the context is clear we may use congruence to refer to a particular congruence. For example: If a ϕ-congruence is under discussion we may refer to the congruence condition and it will be understood that we mean the ϕ-congruence condition.

Where we have a set with multiple operations, making a claim that an equivalence relation is a ϕ_i-congruence will have no implication about whether or not we have a ϕ_j-congruence for some $i \neq j$.

Remark 3.1.2. While the Definition 3.1.1 is in terms of a n-ary operation, in the context of racks and quandles, in practice, we will be working with two binary operations. The definition of a congruence is in terms of functions, where for a binary operation we would have: $\phi_i = \phi_i(x, y)$. These functions are just the rack operations. That is we will have two functions $\phi_1(x, y) = x \triangleright y$ and $\phi_2(x, y) = x \triangleleft y$. For a binary operation $\phi(x, y) = x * y$ we will use the terms ϕ-congruence and $*$-congruence interchangeably to refer to the congruence that respects the operation $\phi(x, y) = x*y$. In the specific context of racks we will define the terms $\triangleright$-congruence and $\triangleleft$-congruence in Definition 3.1.5 below.

Also, in racks and quandles, where there are two binary operations, we will typically be interested in whether or not the equivalence relation respects one or both binary operations.

An example of a congruence would be the non-negative integers modulo n, where n is some positive integer greater than one.

Example 3.1.3. Let $(N, +, \times)$ be the set of non-negative integers with the standard operations of addition and multiplication, and choose $n \in \mathbb{N}$ as some fixed integer with $n > 1$. We define the equivalence relation $\sim$ such that $a \sim b$ if and only if $a \equiv b \bmod n$. We claim this equivalence relation defines both a $+$-congruence and a $\times$-congruence on $\mathbb{N}$.

If we choose $a \sim b$ then $a \equiv b \bmod n$ so

$$a = m_1 n + k \equiv k \text{ mod } n \text{ and } b = m_2 n + k \equiv k \text{ mod } n.$$

Similarly, if we choose $c \sim d$ then

$$c = m_3 n + l \equiv l \text{ mod } n \text{ and } d = m_4 n + l \equiv l \text{ mod } n.$$

Now

$$\begin{aligned} a + c &= m_1 n + k + m_3 n + l \\ &= (m_1 + m_3)n + (k + l) \end{aligned}$$

and

$$\begin{aligned} b + d &= m_2 n + k + m_4 n + l \\ &= (m_2 + m_4)n + (k + l). \end{aligned}$$

We can see that $a+c \sim b+d$ since both are equal to $(k+l) \bmod n$. Therefore equivalence modulo n is a $+$-congruence on the set of non-negative integers.

As before let $a \sim b$ and $c \sim d$ and consider $a \times c$ and $b \times d$. We see, using the same definitions as above, that

$$\begin{aligned} a \times c &= (m_1 n + k)(m_3 n + l) \\ &= (m_1 m_3)n^2 + (k m_3 + l m_1)n + kl \\ &\equiv kl \bmod n \end{aligned}$$

and

$$\begin{aligned} b \times d &= (m_2 n + k)(m_4 n + l) \\ &= (m_2 m_4)n^2 + (k m_4 + l m_2)n + kl \\ &\equiv kl \bmod n. \end{aligned}$$

So $a \times c \sim b \times d$ and we have a $\times$-congruence. Therefore we have both a $\times$-congruence and a $+$-congruence on $(\mathbb{N}, +, \times)$.

We give an example of a congruence on a set with two binary operations where only one of the two operations on the set is respected. An equivalent example can be constructed on either the set of real or rational numbers with the operations of addition and multiplication.

Example 3.1.4. Let $S = \mathbb{Q}$, the set of rational numbers, with the operations addition, $+$, and multiplication, $\times$ and let $\sim$ be an equivalence relation with $a \sim b$ if and only if the fractional part of a is equal to the fractional part of b. That is we can write every $x \in \mathbb{Q}$ as $x = n_x + f_x$ with $n_x \in \mathbb{Z}$ and $0 \leq f_x < 1$. So $a \sim b$ if and only if $f_a = f_b$, which is equivalent to $a \sim b$ if and only if $a - b \in \mathbb{Z}$.

This congruence respects addition but does not respect multiplication. As a result, we have a $+$-congruence but not a $\times$-congruence.

For any $a, b, c, d \in \mathbb{Q}$ with $a \sim b$ and $c \sim d$ we have

$$\begin{aligned} a + c &= n_a + f_a + n_c + f_c \\ &= (n_a + n_c) + (f_a + f_c) \end{aligned}$$

and the fractional part of $a + c$ will be determined by the fractional part of $f_a + f_c$. Similarly,

$$b + d = n_b + f_b + n_d + f_d$$

$$= (n_b + n_d) + (f_a + f_c)$$

since the fractional parts of a and b are the same and the fractional parts of c and d are the same, and therefore the fractional part of $b + d$ will be determined by the fractional part of $f_a + f_c$. Therefore $a + c \sim b + d$.

However, we do not have equivalence with multiplication, where we have

$$\begin{aligned} a \times c &= (n_a + f_a) \times (n_c + f_c) \\ &= n_a \times n_c + n_a \times f_c + n_c \times f_a + f_a \times f_c. \end{aligned}$$

Therefore the fractional part is determined by the fractional part of $n_a \times f_c + n_c \times f_a + f_a \times f_c$, which is dependent on a and c. However, the equivalent calculation with b and d gives

$$\begin{aligned} b \times d &= (n_b + f_a) \times (n_d + f_c) \\ &= n_b \times n_d + n_b \times f_c + n_d \times f_a + f_a \times f_c. \end{aligned}$$

Therefore the fractional part is determined by the fractional part of $n_b \times f_c + n_d \times f_a + f_a \times f_c$, which is dependent on a, b, c, and d and will not necessarily be equal to the fraction part of $a \times c$. For example: $2 \sim 3$ and trivially $\frac{1}{2} \sim \frac{1}{2}$ but $2 \times \frac{1}{2} = 1 \not\sim 1 + \frac{1}{2} = \frac{3}{2} = 3 \times \frac{1}{2}$.

3.1.2 Congruences in racks and quandles

We, of course in this study, are primarily interested in congruences as they apply to racks and quandles. In a rack, a congruence as defined in Definition 3.1.1 can respect one or both rack operations. We will introduce the term rack congruence for when both operations are respected and consistently with Definition 3.1.1 we will introduce the terms $\triangleright$-congruence and $\triangleleft$-congruence to describe when one (and possibly) both operations are respected. Later in Definition 3.2.12 we will make analogous definitions to rack congruence for quandle congruences, and also for shelf congruence and spindle congruence which only have one operation.

The terms $\triangleright$-congruence and $\triangleleft$-congruence are defined by reference to the meta-definition in Definition 3.1.1. However, since we will be working almost exclusively with racks and quandles we will formally define those terms in the context of a rack.

Definition 3.1.5 ($\triangleright$-congruence and $\triangleleft$-congruence). Given a rack, R, and an equivalence relation, $\sim$, on R then $\sim$ is a:

1. $\triangleright$-*congruence* if and only if whenever $a \sim b$ and $c \sim d$ then

$$(a \triangleright c) \sim (b \triangleright d);$$

2. $\triangleleft$-*congruence* if and only if whenever $a \sim b$ and $c \sim d$ then

$$(a \triangleleft c) \sim (b \triangleleft d).$$

When both operations are respected we have a rack congruence.

Definition 3.1.6 (rack congruence). Given a rack, R, and an equivalence relation, $\sim$, on R then $\sim$ is a *rack congruence* if it is both a $\triangleright$-congruence and a $\triangleleft$-congruence. That is if and only if for all $a, b, c, d \in R$ whenever $a \sim b$ and $c \sim d$ then $(a \triangleright c) \sim (b \triangleright d)$ and $(a \triangleleft c) \sim (b \triangleleft d)$. The conditional statements:

1. If $a \sim b$ and $c \sim d$ then $(a \triangleright c) \sim (b \triangleright d)$;
2. If $a \sim b$ and $c \sim d$ then $(a \triangleleft c) \sim (b \triangleleft d)$,

we will call *rack congruence conditions* or where the context is clear simply *congruence conditions*.

Remark 3.1.7. We explicitly refer to the congruence as a rack congruence to indicate that both of the rack operations are respected. Elsewhere, for example in Budden [6] what we are calling a rack congruence is simply referred to as a congruence. We need to make a distinction between when one or both operations are respected as we will be investigating the existence of congruences that respect only one of the rack operations. These will be called half congruences in Definition 3.2.14 and will be investigated in Chapter 4.

In a rack or a quandle it is possible to have congruences that respect one or both operations. Later in Definition 3.2.12 we will extend this definition to quandles, shelves, and spindles by introducing the analogous terms quandle congruence, shelf congruence, and spindle congruence to describe a congruence that respects both operations.

Example 3.1.8. Let K be the Takasaki kei as defined in Example 2.2.31 and let $\sim$ be an equivalence relation defined by $a \sim b$ whenever $a - b \equiv 0 \bmod n$, for some fixed $n \in \mathbb{Z}$ with $n > 1$. This equivalence relation defines a congruence on the Takasaki kei. In the case of a Takasaki kei a congruence with respect to the quandle operation will automatically be a congruence with respect to the inverse quandle operation since the Takasaki kei is involutory and those two operations are identical.

Let $a = m_a n + k$ and $b = m_b n + k$ so that $a \sim b$ and $c = m_c n + l$ and $d = m_d n + l$ so that $c \sim d$, where $m_a, m_b, m_c, m_d \in \mathbb{Z}$ and $0 \leq k < n$ and $0 \leq l < n$. Then $a \triangleright c = 2c - a \equiv (2l - k) \bmod n$ and $b \triangleright d = 2d - b \equiv (2l - k) \bmod n$ so $a \triangleright c \sim b \triangleright d$. So the equivalence relation defines a $\triangleright$-congruence on the Takasaki kei, K. In this case the existence of a $\triangleright$-congruence automatically implies we also have a $\triangleleft$-congruence.

Alongside a congruence is the related concept of a congruence class. A congruence class is a set of elements that are related by the underlying equivalence relation that defines the congruence. We will give a formal definition in the context of a rack.

Definition 3.1.9 (Congruence classes). Given a rack, R and an equivalence relation $\sim$ that determines a congruence, then the *congruence class* of an element $x \in R$, denoted by $[x]$, is the set defined by $[x] = \{a \in R \mid a \sim x\}$.

Remark 3.1.10. The congruence classes are determined by the equivalence relation. If the equivalence relation is not a congruence then the classes are known as *equivalence classes*. At times, we will be working with more than one equivalence relation. Where necessary, for the removal of ambiguity we will decorate the congruence classes (or equivalence classes) with a subscript to indicate the equivalence relation that determines the congruence classes. That is, $[x]_\sim$ will mean the congruence class of the element x determined by the equivalence relation $\sim$. However, typically in context, the equivalence relation will be unambiguously known and we will write $[x]$ to mean $[x]_\sim$.

A congruence class (or an equivalence class) can be named for any of the elements that are included in the congruence class. That is, if $a, b \in [x]$ then $[x] = [a] = [b]$ all represent the same congruence class.

Example 3.1.11. The congruence classes in Example 3.1.8 on the Takasaki kei are the sets $[k] = \{mn + k : m \in \mathbb{Z}\}$, for $0 \leq k < n$ where $n \in \mathbb{Z}$ is fixed from the previous example. For example, if $n = 2$ then the congruence classes are the even integers, $[0] = \{2m : m \in \mathbb{Z}\}$, and the odd integers, $[1] = \{2m + 1 : m \in \mathbb{Z}\}$.

3.2 Quotients

Congruences allow us to construct a related algebraic structure in which we work with the congruence classes rather than the elements of the rack we began with. This structure is called a quotient.

Definition 3.2.1 (Quotient). Given a rack, $(R, \triangleright)$, and a $\triangleright$-congruence, $\sim$, then the *quotient*, $(R/{\sim}, \triangleright)$, is the set of all congruence classes of $\sim$, together with the operation, $\triangleright$, defined on congruence classes in the natural way. That is, for $[x], [y] \in R/{\sim}$, $[x] \triangleright [y] = [x \triangleright y]$. We will see in Lemma 3.2.6 that this operation is well defined by the congruence condition.

Remark 3.2.2. Note that, consistent with our definitions, we can form a quotient based on a congruence that respects one or both rack operations. The definition is in terms of one operation. If the congruence respects both operations then we will have one set of congruence classes and in the quotient we will have both operations defined as $[x] \triangleright [y] = [x \triangleright y]$ and $[x] \triangleleft [y] = [x \triangleleft y]$.

The following example looks at the quotient that is formed on the congruence classes in Example 3.1.11 which is on the Takasaki kei.

Example 3.2.3. We will write the quotient that is formed from Examples 3.1.8 and 3.1.11 as $(K/{\sim}, \triangleright)$, where $K/{\sim}$ represents the set of congruence classes in the quotient and $\triangleright$ is the operation on those congruence classes derived from the identically named operation in $(K, \triangleright)$ as described in Definition 3.2.1. The set $K/{\sim}$ is the set of sets of integers that are equivalent to the integers $0, 1, \ldots, n-1$ respectively for some fixed n. That is

$$K/{\sim} = \{[0], [1], \ldots, [n-1]\},$$

where for $k \in \{0, 1, \ldots, n-1\}$, $[k] = \{mn + k : m \in \mathbb{Z}\}$, $0 \leq k < n-1$. The claim is that the operation defined by $[x] \triangleright [y] = [x \triangleright y]$ is well defined. This follows immediately as a consequence of the definition of a congruence and as noted will be shown in general in Lemma 3.2.6.

In this example, since the Takasaki kei is involutory, the rack operation identical to the inverse rack operation. In general that will not be the case. Therefore we will extend the definition of a quotient to the case where the equivalence relation respects both rack operations and therefore we have both a $\triangleright$-congruence and a $\triangleleft$-congruence. We will prematurely call this a quotient rack and later in Theorem 3.2.7 we will show that indeed a quotient formed based on a congruence that respects both rack operations is a rack.

Definition 3.2.4 (Quotient rack). Given a rack, $(R, \triangleright, \triangleleft)$, and a congruence, $\sim$, that is both a $\triangleright$-congruence and a $\triangleleft$-congruence, then the *quotient*, $R/{\sim}$, is the set of all congruence classes of $\sim$, together with the rack operation, $\triangleright$, defined on congruence classes in the natural way. That is, for $[x], [y] \in R/{\sim}$, $[x] \triangleright [y] = [x \triangleright y]$ and $[x] \triangleleft [y] = [x \triangleleft y]$. We will see that this operation is well defined by the congruence condition.

Remark 3.2.5. As speculated, the hope is that a quotient defined in this manner turns out to be a rack and indeed it does as we shall prove. Fenn and Rourke [14] and Ryder [27, 28] define a congruence by the congruence condition only on the rack operation and not the inverse rack operation. This turns out to be sufficient to define a quotient rack whenever the rack is finite and in some cases when the rack is infinite but is not true in general. In Section 4.1 we give some counterexamples where the congruence condition holds only for the rack operation and not for the inverse rack operation. In consequence, in the examples, the resultant quotient, $R/{\sim}$, is not in fact a rack.

We show that the rack operations defined on equivalence classes are well defined.

Lemma 3.2.6. *Let R be a rack and let $\sim$ be a congruence on R. Then*

1. *If $\sim$ is a $\triangleright$-congruence then $[x] \triangleright [y] = [x \triangleright y]$ is a well-defined binary operation.*
2. *If $\sim$ is a $\triangleleft$-congruence then $[x] \triangleleft [y] = [x \triangleleft y]$ is a well-defined binary operation.*

Proof. This is a straightforward consequence of the definition of a congruence.

For all $a \in [x]$, $a \sim x$ and similarly for all $b \in [y]$, $b \sim y$ therefore

1. In a $\triangleright$-congruence: since $(a \triangleright b) \sim (x \triangleright y)$, we have

$$[a] \triangleright [b] = [a \triangleright b] = [x \triangleright y] = [x] \triangleright [y].$$

2. Similarly, in a $\triangleleft$-congruence: since $(a \triangleleft b) \sim (x \triangleleft y)$, we have

$$[a] \triangleleft [b] = [a \triangleleft b] = [x \triangleleft y] = [x] \triangleleft [y].$$

Therefore the binary operations on equivalence classes are well defined. □

We will now show that a quotient defined in this way based on a rack congruence, so that both rack operations are respected, does form a rack. This is likely to be a known result but we present a proof.

Theorem 3.2.7. *Let $(R, \triangleright, \triangleleft)$ be a rack and let $\sim$ be a rack congruence on R. Then $(R/{\sim}, \triangleright, \triangleleft)$ is a rack, where the operations $\triangleright$ and $\triangleleft$ are the well-defined operations on the equivalence classes of $\sim$.*

Proof. We need to check Axioms Q2 and Q3 hold in $R/{\sim}$. In fact, it is easier to check the equivalent Axiom Q2a rather than checking Axiom Q2 directly. Both Axioms Q2a and Q3 hold in $R/{\sim}$ as an immediate consequence of them holding in R.

Checking Axiom Q2a we have for all $x, y \in R$,

$$\begin{aligned} ([x] \triangleright [y]) \triangleleft [y] &= [x \triangleright y] \triangleleft [y] \\ &= [(x \triangleright y) \triangleleft y] \\ &= [x]. \end{aligned}$$

Checking Axiom Q3 we have for all $x, y, z \in R$,

$$\begin{aligned} ([x] \triangleright [y]) \triangleright [z] &= [x \triangleright y] \triangleright [z] \\ &= [(x \triangleright y) \triangleright z] \\ &= [(x \triangleright z) \triangleright (y \triangleright z)] \\ &= [x \triangleright z] \triangleright [y \triangleright z] \\ &= ([x] \triangleright [z]) \triangleright ([y] \triangleright [z]) . \end{aligned}$$

Therefore $(R/{\sim}, \triangleright, \triangleleft)$ is a rack. $\square$

The proof of invertibility and self-distributivity are independent. That means that the second part of the proof dealing with self-distributivity applies to any shelf.

Corollary 3.2.8. *Let* $(S, \triangleright)$ *be a shelf and let* $\sim$ *be a* $\triangleright$*-congruence on* S*. Then* $(S/{\sim}, \triangleright)$ *is a shelf, where the operation* $\triangleright$ *is the well-defined operation on the equivalence classes of* $\sim$*.*

Proof. The corollary was proved in the second part of the proof of Theorem 3.2.7. $\square$

We can prove a similar theorem holds in a quandle simply by applying Theorem 3.2.7 and in addition checking that Quandle Axiom Q1 is satisfied.

Theorem 3.2.9. *Let* $(Q, \triangleright, \triangleleft)$ *be a quandle and let* $\sim$ *be both a* $\triangleright$*-congruence and a* $\triangleleft$*-congruence on* Q*. Then* $(Q/{\sim}, \triangleright, \triangleleft)$ *is a quandle, where the operations* $\triangleright$ *and* $\triangleleft$ *are the well-defined operations on the equivalence classes of* $\sim$*.*

Proof. Axioms Q2 and Q3 hold by Theorem 3.2.7, therefore we only need to prove that Axiom Q1 holds in $Q/{\sim}$. As for the rack axioms, this axiom holds as an immediate consequence of it holding in Q.

For all $x \in Q$,

$$\begin{aligned}[x] \triangleright [x] &= [x \triangleright x] \\ &= [x].\end{aligned}$$

Therefore $(Q/{\sim}, \triangleright, \triangleleft)$ is a quandle. $\square$

By combining the part of the proof of Theorem 3.2.9 which deals with idempotence and the part of the proof of Theorem 3.2.7 which deals with self-distributivity, we can deduce a similar result on spindles.

Corollary 3.2.10. *Let $(S, \triangleright)$ be a spindle and let $\sim$ be a $\triangleright$-congruence on S. Then $(S/{\sim}, \triangleright)$ is a spindle, where the operation $\triangleright$ is the well-defined operation on the equivalence classes of $\sim$.*

Proof. The proof is a combination of the proof of idempotence in Theorem 3.2.9 and Corollary 3.2.8. $\square$

Remark 3.2.11. As we saw in Definition 3.1.6 where a congruence respects both rack operations we defined the congruence as a rack congruence. We now make an analogous definition for a quandle congruence. We will also give definitions of a shelf congruence and a spindle congruence to apply to those structures. Since every rack is a shelf and every quandle is a spindle, we will also use the terms shelf congruence and spindle congruence when an equivalence relation only respects one of the operations in a rack or a quandle respectively. We use the following formal definitions for those terms. For clarity, we repeat the definition of a rack congruence here.

Definition 3.2.12 (quandle congruence, rack congruence, spindle congruence, and shelf congruence). Given a quandle, rack, shelf, or spindle if an equivalence relation preserves one or more of the axiomatic properties of the given structure we will refer to the equivalence relation in terms of the preserved axiomatic properties. That is:

1. A *quandle congruence* is a congruence on a quandle, $(Q, \triangleright)$, which is both a $\triangleright$-congruence and a $\triangleleft$-congruence.
2. A *rack congruence* is a congruence on a rack, $(R, \triangleright)$, which is both a $\triangleright$-congruence and a $\triangleleft$-congruence.
3. A *spindle congruence* is a congruence on a spindle, $(S, \triangleright)$, which is a $\triangleright$-congruence.
4. A *shelf congruence* is a congruence on a shelf, $(S, \triangleright)$, which is a $\triangleright$-congruence.

Remark 3.2.13. For the removal of doubt our intention is for these terms to be inclusive in the following sense: since every quandle can be viewed as a rack or a shelf or a spindle with additional properties, the terms rack congruence, shelf congruence, and spindle congruence do not preclude the possibility of the structure being a quandle congruence. Similarly a shelf congruence may be a rack congruence or a spindle congruence if invertibility or idempotence are present respectively.

Similarly, the terms $\triangleright$-congruence and $\triangleleft$-congruence are inclusive in the sense that describing a congruence as a $\triangleright$-congruence does not preclude us also having a $\triangleleft$-congruence and vice versa. However sometimes in a rack we will wish to identify that the congruence condition holds only for one rack operation and we have a congruence with respect to that rack operation but we do not have a rack operation with respect to the other rack operation, whether it is the primary rack operation or the inverse operation. For that purpose we will introduce the term half congruence. In the next chapter we will show the existence of half congruences.

Definition 3.2.14. In a rack, R, a *half congruence* is either a $\triangleright$-congruence that is not a $\triangleleft$-congruence or a $\triangleleft$-congruence that is not a $\triangleright$-congruence.

Remark 3.2.15. A half congruence in a rack is a shelf congruence and in a quandle is a spindle congruence. The resultant quotients will be a shelf or a spindle respectively.

3.3 Homomorphisms

The concepts of homomorphism, isomorphism and automorphism can be applied to racks. Since there are effectively two rack operations it naturally seems there are two conditions that need to be satisfied for a function to be a homomorphism. However it turns out that it is sufficient to impose the homomorphism condition on only one of the rack operations, and the condition on the other operation can be deduced from that.

Definition 3.3.1. Let $(R, \triangleright)$ and $(R_*, \triangleright_*)$ be racks. A function, $\psi : R \to R_*$ is a *homomorphism* if for all $x, y \in R$,

$$\psi(x \triangleright y) = \psi(x) \triangleright_* \psi(y),$$

where the operation on the left, $\triangleright$, is in the rack R and the operation on the right, $\triangleright_*$, is in the rack R_*.

In the usual way, a *homomorphism* that is a bijection is an *isomorphism.*

The next example is a homomorphism from the Takasaki kei to the cyclic quandle of Remark 2.2.35.

Example 3.3.2. Let $K = \mathbb{Z}$ be the Takasaki kei of Example 2.2.31. Then $\phi : \mathbb{Z} \to \mathbb{Z}_n$ with $\phi(k) = [k]$, where for some $n \in \mathbb{Z}$ with $n > 1$, $[k] = \{x \in K : x - k \equiv 0 \bmod n\}$ is a homomorphism. Where we take the quandle operation in $\mathbb{Z}_n$ to be $[x] \triangleright_n [y] = [2y - x]$ which is the equivalence class of elements of K that are congruent to $2y - x$ modulo n.

We can see this is a homomorphism by choosing $x = a_x n + k_x$ and $y = a_y n + k_y$. Then we see:

$$\begin{aligned}
\phi(x \triangleright y) &= \phi(2y - x) \\
&= \phi((2y_a - a_x)n + 2k_y - k_x) \\
&\equiv (2k_y - k_x) \bmod n \\
&\equiv \big(2(a_y n - k_y) - (a_x n - k_x)\big) \bmod n \\
&= \phi(x) \triangleright_n \phi(y),
\end{aligned}$$

as required.

We will now show, in Lemma 3.3.3, that for a homomorphism the condition on one of the rack operations implies a similar condition on the other operation. Again, this lemma is likely to be well known but as far as we are aware not explicitly stated in the literature. It is possible that it has been overlooked in some work because checks on, for example, closure are only required on one operation when the rack is finite. We will need Lemma 3.3.3 in order to prove that the image of a homomorphism is a subrack in Lemma 3.3.4.

Lemma 3.3.3. *Let* $(R, \triangleright)$ *and* $(R_*, \triangleright_*)$ *be racks and let* $\psi : R \to R_*$ *be a homomorphism. Then*

$$\psi(x \triangleleft y) = \psi(x) \triangleleft_* \psi(y). \tag{3.3.1}$$

Proof. From the right hand side of equation (3.3.1) we have

$$\begin{aligned} \psi(x) \triangleleft_* \psi(y) &= \psi\left((x \triangleleft y) \triangleright y\right) \triangleleft_* \psi(y) \\ &= \left(\psi(x \triangleleft y) \triangleright_* \psi(y)\right) \triangleleft_* \psi(y) \\ &= \psi(x \triangleleft y), \end{aligned}$$

which is the left hand side of equation (3.3.1), as required. □

Homomorphisms preserve a rack or quandle structure. That is, the homomorphic image of a rack or quandle is a rack or quandle, respectively.

Lemma 3.3.4. *Let R and R_* be racks. Let $\phi : R \to R_*$ be a homomorphism. Then* $\mathrm{Im}(R) = \phi(R)$ *is a subrack of R_*. In addition, if idempotence holds in R then* $\mathrm{Im}(R) = \phi(R)$ *is a subquandle of R_*.*

Proof. Let $\phi(x)$, $\phi(y) \in \phi(R)$. Then $\phi(x) \rhd_* \phi(y) = \phi(x \rhd y) \in \phi(R)$. Similarly, $\phi(x) \lhd_* \phi(y) = \phi(x \lhd y) \in \phi(R)$. Therefore $\phi(R)$ is closed under $\rhd_*$ and $\lhd_*$. Therefore $\phi(R)$ is a subrack of R_*.

If idempotence holds in R then $\phi(x) \rhd_* \phi(x) = \phi(x \rhd x) = \phi(x) \in \phi(R)$. Therefore we have idempotence in $\phi(R)$. □

Lemma 3.3.4 can be applied to a subrack or subquandle.

Corollary 3.3.5. *Let R and R_* be racks. Let $\phi : R \to R_*$ be a homomorphism. Let $S \subseteq R$ be a subrack of R. Then $S_* = \phi(S)$ is a subrack of R_*.*

Similarly, if we have a subrack $S \subseteq R$ then if we have idempotence in S so that S is a quandle then we have $S_* = \phi(S)$ is a subquandle of R_*.

Proof. Applying Lemma 3.3.4 to the racks or quandles S and R_* with the homomorphism, ϕ, restricted to S we have that $\phi(S)$ is a subrack and if S is a quandle then $\phi(S)$ is a quandle. □

Remark 3.3.6. Alternatively, since ϕ is by definition into R_* we clearly have $\mathrm{Im}(\phi) \subseteq R_*$. Therefore to establish that $\mathrm{Im}(\phi)$ is a rack we need to check the rack axioms in $\mathrm{Im}(\phi)$.

1. **Invertibility:** We appeal to the invertibility axiom in both R and R_* to establish invertibility in $\mathrm{Im}(R)$. Let $\phi(y), \phi(z) \in \mathrm{Im}(\phi) \subseteq R_*$, with $y, z \in R$. Then since R_* is a rack there exists a unique $\xi \in R_*$ such that

   $$\xi \triangleright_* \phi(y) = \phi(z).$$

   Also, since R is a rack there exists a unique $x \in R$ such that

   $$x \triangleright y = z.$$

   This implies

   $$\phi(x \triangleright y) = \phi(x) \triangleright_* \phi(y) = \phi(z).$$

   Since $\xi \in R_*$ is the unique element in R_* with this property then

   $$\xi = \phi(x) \in \mathrm{Im}(\phi).$$

2. **Distributivity:** Let $\phi(x), \phi(y), \phi(z) \in \mathrm{Im}(R)$, with $x, y, z \in R$. Then since $(x \triangleright y) \triangleright z = (x \triangleright z) \triangleright (y \triangleright z)$ in R,

   $$\begin{aligned} & \phi\Big((x \triangleright y) \triangleright z\Big) = \phi\Big((x \triangleright z) \triangleright (y \triangleright z)\Big) \\ \Rightarrow \quad & \phi(x \triangleright y) \triangleright_* \phi(z) = \phi(x \triangleright z) \triangleright_* \phi(y \triangleright z) \\ \Rightarrow \quad & \Big(\phi(x) \triangleright_* \phi(y)\Big) \triangleright_* \phi(z) = \Big(\phi(x) \triangleright_* \phi(z)\Big) \triangleright_* \Big(\phi(y) \triangleright_* \phi(z)\Big) \end{aligned}$$

3. **Idempotence:** Moreover if R is a quandle then let $\phi(x) \in \mathrm{Im}(\phi)$, with

$x \in R$. Then

$$\phi(x) \triangleright_* \phi(x) = \phi(x \triangleright x) = \phi(x).$$

Therefore $\phi(R) = \mathrm{Im}(\phi)$ is a rack. Moreover if R is a quandle then $\phi(R) = \mathrm{Im}(\phi)$ is a quandle.

Similarly, we can define isomorphisms and automorphisms of racks.

Definition 3.3.7. An *isomorphism* is a homomorphism that is one-to-one and onto.

Definition 3.3.8. An *automorphism* is an isomorphism where $R = R_*$.

The symmetries, S_y, define an automorphism on a rack. This is well known and we provide a proof.

Lemma 3.3.9. *Let R be a rack, let $y \in R$ and let the symmetry at y be S_y. Then S_y defines an automorphism on R.*

Proof. For all $x \in R$, $xS_y = x \triangleright y \in R$, therefore S_y is into R.

Suppose $xS_y = x'S_y$. Then $x \triangleright y = x' \triangleright y$ which implies $x = x'$ by the invertibility axiom. Therefore S_y is one-to-one.

Suppose $z \in R$. Then by the invertibility axiom there exists $x \in R$ such that $x \triangleright y = xS_y = z$. Therefore S_y is onto R.

We need $(x \triangleright z)S_y = xS_y \triangleright zS_y$, but this is simply the third Quandle Axiom

Q3 as:

$$(x \triangleright z)S_y = (x \triangleright z) \triangleright y = (x \triangleright y) \triangleright (z \triangleright y) = xS_y \triangleright zS_z.$$

Therefore S_y is an automorphism of R. $\square$

There are three automorphism groups of interest for a rack, R — see Joyce [16] for a discussion of these groups.

1. The full automorphism group, $\mathrm{Aut}(R)$, which is the group of all automorphisms of R. All symmetries $S_y \in \mathrm{Aut}(R)$.

2. The inner automorphism group, $\mathrm{Inn}(R)$, which is the group generated by all symmetries, S_y, of R.

3. The transvection group, $\mathrm{Trans}(R)$, which is the group generated by all automorphisms of the form $S_x S_y^{-1}$ for some $x, y \in R$.

Lemma 3.3.10. *Let R_1 and R_2 be racks and let $\phi : R_1 \to R_2$ be a homomorphism. If $S_2 \subseteq R_2$ a subrack of R_2 then $S_1 = \phi^{-1}(S_2) \subseteq R_1$ is a subrack of R_1.*

Proof. We have by definition

$$S_1 = \phi^{-1}(S_2) = \{x \in R_1 : \phi(x) \in S_2\}.$$

Let $x, y \in S_1$ then $\phi(x), \phi(y) \in S_2$ and consider $x \triangleright y = z \in R_1$. Since the subrack, S_2, is closed under $\triangleright$ we have $\phi(x) \triangleright \phi(y) = \phi(x \triangleright y) = \phi(z) \in S_2$

and therefore necessarily $z \in S_1$. Similarly, consider $x \triangleleft y = z' \in R_1$. Since the subrack, S_2 is also closed under $\triangleleft$ we have $\phi(x) \triangleleft \phi(y) = \phi(x \triangleleft y) = \phi(z') \in S_2$ and therefore necessarily $z' \in S_1$.

Therefore, since S_1 is closed under both rack operations, S_1 is a sub-rack of R_1. □

3.4 Isomorphism Theorems in Racks and Quandles

We show that there is an isomorphism theorem on racks and quandles analogous to the First Isomorphism Theorem in group theory. The First Isomorphism Theorem includes a statement that the kernel of a homomorphism is a normal subgroup in the group. There is no analogy of this part of the First Isomorphism Theorem since there is no analogy of an identity element in a rack or quandle and therefore no analogy to the kernel of a homomorphism. However there is an analogy in that defining $a \sim b$ if and only if $\phi(a) = \phi(b)$ for a homomorphism ϕ defines an equivalence relation in both cases. In the group case this gives the cosets of the kernel.

3.4.1 An isomorphism theorem

We will use these theorems to establish isomorphism theorems in racks and quandles. First we note that a homomorphism can always be used to define an equivalence relation.

Lemma 3.4.1. *If* $\phi : X \to X^*$ *is a homomorphism and* $x, y \in X$ *then the relation* $\sim$ *where* $x \sim y$ *if and only if* $\phi(x) = \phi(y)$ *is an equivalence relation.*

It is easily seen that this relation is reflexive, symmetric, and transitive so the proof is omitted.

Theorem 3.4.2. *Let* $(R, \triangleright)$ *and* $(R_*, \ \triangleright_* \ )$ *be racks, let* $\phi : R \to R_*$ *be a homomorphism, and let* $\sim$ *be the equivalence relation on* R*, defined by, for all* $x, y \in R$*,* $x \sim y$ *if and only if* $\phi(x) = \phi(y)$*. Then*

1. *The image of* ϕ*,* $\operatorname{Im}(\phi) = \phi(R)$*, is a subrack of* R_**;*

2. *The equivalence relation is a rack congruence;*

3. *The function* $\psi([x]) = \phi(x)$ *is an isomorphism from* $R/{\sim}$ *to* $\phi(R)$*.*

Moreover if R *is a quandle then the image of* ϕ*,* $\operatorname{Im}(\phi) = \phi(R)$*, is a subquandle of* R_**.*

Proof. We need to establish three things to prove the theorem:

1. That $\operatorname{Im}(\phi) = \phi(R)$ is a rack and therefore a subrack of R_*;

2. That the quotient $R/{\sim}$ is a rack;

3. That $\psi\left([x]\right) = \phi(x)$ is an isomorphism from $R/{\sim}$ to $\operatorname{Im}(\phi)$.

In addition, in items 1, 2, and 3 above, we need to show that the corresponding result is true when the rack is a quandle. That is, we will need to show that Quandle Axiom Q1 (idempotence) holds when R is a quandle.

1. That the image of R is a subrack of R_* follows from ϕ being a homomorphism by Lemma 3.3.4.

2. We need to check that $R/{\sim}$ is a rack, and is a quandle whenever R is a quandle. We do this by showing that $\sim$ is a congruence and appealing to Theorems 3.2.7 and 3.2.9.

   For all $x, y, z, w \in R$ whenever $x \sim y$ and $z \sim w$ we have:

   $$\begin{aligned} \phi(x \triangleright z) &= \phi(x) \triangleright_* \phi(z) \\ &= \phi(y) \triangleright_* \phi(w) \\ &= \phi(y \triangleright w). \end{aligned}$$

   This implies that $(x \triangleright z) \sim (y \triangleright w)$.

   Similarly,

   $$\begin{aligned} \phi(x \triangleleft z) &= \phi(x) \triangleleft_* \phi(z) \\ &= \phi(y) \triangleleft_* \phi(w) \\ &= \phi(y \triangleleft w). \end{aligned}$$

   Which in turn implies that $(x \triangleleft z) \sim (y \triangleleft w)$.

   Therefore $\sim$ is a congruence. Since the rack operations are well defined on the congruence classes, $R/{\sim}$ is a rack by Theorem 3.2.7 and whenever R is a quandle, $R/{\sim}$ is a quandle by Theorem 3.2.9.

3. We show that $\psi : R/{\sim} \to \phi(R) \subseteq R_*$ where $\psi([x]) = \phi(x)$ is an isomorphism. The map $\psi : R \to \mathrm{Im}(R)$ is:

   (a) Well defined since for any $\xi \in [x]$, $\psi([\xi]) = \phi(\xi) = \phi(x) = \psi([x])$, by definition of $[x]$.

   (b) A homomorphism since $\psi\left([x] \triangleright [y]\right) = \psi([x \triangleright y]) = \phi(x \triangleright y) = \phi(x) \triangleright_* \phi(y) = \psi([x]) \triangleright_* \psi([y])$.

   (c) one-to-one. Let $[x], [y] \in R/{\sim}$ and assume $\psi([x]) = \psi([y])$. By definition of ψ this implies $\phi(x) = \phi(y)$ which in turn, by definition of the equivalence relation, implies $x \sim y$ which implies $y \in [x]$ (and $x \in [y]$) and therefore $[x] = [y]$.

   (d) Is onto by definition of $\phi(R) = \mathrm{Im}(\phi)$.

   Therefore ψ is an isomorphism from $R/{\sim}$ to $\phi(R)$ as required.

This establishes the theorem. □

We return to the example of the Takasaki kei.

Example 3.4.3. Let $K = \mathbb{Z}$ be the Takasaki kei. Choose $n > 1$ and let $\phi : K \to \mathbb{Z}_n$ be the homomorphism defined by $\phi(x) = [x]$. Let $\sim$ be the equivalence relation where for $a, b \in K$, $a \sim b$ if and only if $\phi(a) = \phi(b)$ which is equivalent to $a \equiv b \bmod n$. Then:

1. Trivially, $\mathrm{Im}(\phi) = \phi(K) = \mathbb{Z}_n$ is a subrack (subquandle) of itself.

2. If we choose $x_1, x_2, y_1, y_2 \in K$ such that $x_1 \sim x_2$ and $y_1 \sim y_2$ then we can write $x_i = a_i n + k_x$ and $y_i = b_i n + k_y$ for some $a_i, b_i, k_x, k_y \in \mathbb{Z}$ and $i \in \{1, 2\}$. Now we can see that

$$\begin{aligned} x_1 \triangleright y_1 &= 2y_1 - x_1 \\ &= (2b_1 - a_1)n + 2k_y - k_x \\ &\sim (2b_2 - a_2)n + 2k_y - k_x \\ &= 2y_2 - x_2 \\ &= x_2 \triangleright y_2, \end{aligned}$$

   and similarly $x_1 \triangleleft y_1 \sim x_2 \triangleleft y_2$. Therefore $\sim$ is a rack congruence on K. This in turn means that $K/\sim$ is a quotient rack (quandle).

3. The congruence classes of $\sim$ are the n sets $[x] = \{a : (x - a) \bmod n \equiv 0, a \in \mathbb{Z}\}$. The map $\psi : K/\sim \to \mathbb{Z}_n$ defined by $\psi([x]) \mapsto [x]$ is clearly a bijection from the n congruence classes of $\sim$ onto the n elements of $\mathbb{Z}_n$ and so is an isomorphism from $K/\sim$ to $\phi(K) = \mathbb{Z}_n$.

Chapter 4

Existence of Half Congruences

We defined congruences and the associated terms: $\triangleright$-congruence; $\triangleleft$-congruence; quandle congruence; rack congruence; spindle congruence; and shelf congruence, in Section 3.1. We also defined the term half congruence. We will now look in more detail at properties of congruences in racks and quandles. Of particular interest will be the property that a congruence on one rack operation does not imply that we have a congruence on the other rack operation. That is, the existence of half congruences. There has been some confusion about this property in the literature, with some authors claiming erroneously that a quotient rack can be formed when we have a congruence on only one rack operation.

In some cases, a congruence on one rack operation does imply that the quotient is a rack. In particular, that is always true when the rack is finite and it is also true at times for infinite racks. However, as we will see, at times invertibility in the quotient breaks down. Since the symmetries at each point are bijections then necessarily the inverse of the symmetries at each point is a bijection. For a function from a finite set to itself, a bijection is a surjection and conversely a surjection is a bijection. The key property is that a one-to-one function is onto and vice versa. In contrast, for an infinite set, a one-to-one function need not be onto and an onto function need not be one-to-one.[1]

We begin by looking in more detail at the issues in an infinite rack.

4.1 Congruences in racks

As noted previously in Remark 3.2.5, Fenn and Rourke [14] and Ryder [28] define a congruence on a rack. Their definition depends on only the primary rack operation. They state, without proof, such a congruence, which we have called a $\triangleright$-congruence, defines a quotient which is a rack. That is, they state that if $\sim$ is an $\triangleright$-congruence on R, then $R/{\sim}$ is a rack. It turns out that their definition of a congruence, in some cases, is not sufficient to define a 'quotient rack'. That is, the quotient so defined is not necessarily a rack. In order to define a 'quotient rack' the stronger condition based on both rack operations is required.

We have already defined the terms "congruence" in Definition 3.1.1 and "quo-

---

[1] This is a familiar but curious property of infinity. For example, the map $f : \mathbb{Z} \to \mathbb{Z}$ defined by $n \mapsto 2n$ is one-to-one but not onto $\mathbb{Z}$. Conversely $g : \mathbb{Z} \to \mathbb{Z}$ defined by $n \mapsto \lfloor \frac{n}{2} \rfloor$ is onto $\mathbb{Z}$ but it is not one to one.

For a great read on infinity I recommend Wallace, D.F., 2010. *Everything and more: a compact history of infinity.* WW Norton & Company.

tient" in Definition 3.2.1. We also defined particular types of congruence depending on what operations were respected by the underlying equivalence relation. Recall from Theorems 3.2.7 and 3.2.9 and their corollaries that a rack congruence preserved the rack structure in the quotient; a quandle congruence preserved the quandle structure in the quotient; a spindle congruence preserved the spindle structure in the quotient; and a shelf congruence preserved the shelf structure in the quotient. We also defined the terms $\triangleright$-congruence and $\triangleleft$-congruence to mean that a congruence condition was satisfied for the operations $\triangleright$ and $\triangleleft$ respectively. In terms of those definitions, we claim that it is possible to have half congruences, $\triangleright$-congruences that are not $\triangleleft$-congruences and vice-versa. In this chapter we prove that by showing the existence of half congruences by way of example.

What happens in the quotient when we have a $\triangleright$-congruence that is not a $\triangleleft$-congruence (or equivalently a $\triangleleft$-congruence that is not a $\triangleright$-congruence) is that invertibility fails. That is, the operation, $\triangleright$, is well defined on the quotient but we have elements in the quotient, $[x_1]$, $[x_2]$, $[y]$, and $[z]$ with $[x_1] \neq [x_2]$ where both

$$[x_1] \triangleright [y] = [z] \text{ and } [x_2] \triangleright [y] = [z]$$

hold and so in general we cannot satisfy Axiom Q2 as there is no unique element, $[x]$, for all $[y]$, $[z]$ in the quotient, that solves the equation $[x] \triangleright [y] = [z]$.

In such a quotient, we do preserve both idempotence, when we start from a quandle, and distributivity, whether we are working from a quandle or a rack, but not invertibility so that the resulting quotient is a shelf or a spindle. That is, while we started in a rack or a quandle the quotient formed is a shelf or a spindle.

Remark 4.1.1. We have seen in Theorem 3.2.7 that when we have a rack congruence that the quotient is a rack and in Corollary 3.2.8 that when we have a shelf congruence that the quotient is a shelf. A rack congruence is both a $\triangleright$-congruence and a $\triangleleft$-congruence. A shelf congruence in a rack, is a $\triangleright$-congruence that is not necessarily a $\triangleleft$-congruence or vice versa. When a congruence only respects one operation in a rack we have called the congruence a half congruence. A question that naturally arises is do half congruences exist?

That question is related to the question of whether or not the quotient formed from a $\triangleright$-congruence (or a $\triangleleft$-congruence) is a rack. The answer is in the affirmative whenever the congruence is a rack congruence. Therefore if we have a congruence in a rack but the quotient is not a rack then necessarily the congruence is a half congruence.

Theorem 4.1.2. *Let R be a rack and $\sim$ be a congruence on R. Then $\sim$ is a half congruence if and only if $R/\sim$ is not a rack.*

Proof. If $R/\sim$ is not a rack then $\sim$ is a half congruence follows from Theorem 3.2.7. The contrapositive of that theorem gives us that if the quotient is not a rack then we do not have a rack congruence. However, since this theorem states that $\sim$ is a congruence, the congruence therefore must be a half congruence.

On the other hand if we have a half congruence then we can assume, without loss of generality, that we have a $\triangleright$-congruence. If not then work with the dual rack, where the roles of the rack operations are interchanged. If $\sim$ is a half congruence then there exists $a \sim b$ and $c \sim d$ with $a \triangleright c \sim b \triangleright d$ but $a \triangleleft c \not\sim b \triangleleft d$. Consider the equation $[x] \triangleright [c] = [a]$ which has the solution $[x] = [a \triangleleft c]$. Since $a \sim b$ and $c \sim d$ this equation is identical to $[x] \triangleright [d] = [b]$ which has the solution $[x] = [b \triangleleft d]$. However because $a \triangleleft c \not\sim b \triangleleft d$, $[a \triangleleft c] \neq [b \triangleleft d]$ and therefore there is not a unique solution to this equation and therefore the quotient is not a rack. $\square$

Remark 4.1.3. The contrapositive of this theorem, in both directions, is also useful. That is, if R is a rack and $\sim$ a congruence on R then $R/{\sim}$ is a rack if and only if $\sim$ is a rack congruence. We have already seen one direction of the contrapositive in Theorem 3.2.7: if $\sim$ is a rack congruence (a congruence that is not a half congruence) then $R/{\sim}$ is a rack.

As noted previously and illustrated in the proof of the previous theorem, the issue that arises in the quotient when we have a half congruence, is that the uniqueness axiom, Axiom Q2, is not satisfied in general. We have uniqueness in the rack, R, so that for all $y, z \in R$ there exists $x \in R$ such that $x \triangleright y = z$. Therefore $[x \triangleright y] = [z]$ and by the definition of the congruence $[x \triangleright y] = [x] \triangleright [y] = [z]$. In order to show that $R/{\sim}$ is a rack we require $[x]$ to be the unique solution of this equation. Suppose however $[x'] \triangleright [y] = [z]$.

Therefore $[x' \triangleright y] = [z]$ and we have both $x' \triangleright y \in [z]$ and $x \triangleright y \in [z]$ hence $(x' \triangleright y) \sim (x \triangleright y)$. However, the definition of the congruence allows no cancellation law and thus no means to deduce from that statement that $x' \sim x$ so that it is not necessarily true that $[x'] = [x]$.

For all $[y], [z] \in R/{\sim}$, the equation $[x] \triangleright [y] = [z]$ has a solution since in the rack, R, $x \triangleright y = z$ has solution x which is unique. Therefore for all $x_i \in [x]$ and for all $y_i \in [y]$ we have $x_i \triangleright y_i \sim x \triangleright y = z$. So $[x]$ is a solution of the equation $[x] \triangleright [y] = [z]$. However uniqueness is not guaranteed since there maybe some $x' \notin [x]$ with $x' \triangleright y \sim z$.

4.2 A sufficient condition for a $\triangleright$-congruence to be a rack congruence

Nevertheless, there are some cases in which a congruence condition on only one rack operation is sufficient to ensure that the resulting quotient is a rack. Before producing examples where the invertibility breaks down in the quotient, we will introduce a sufficient condition in Theorem 4.2.3 under which the congruence condition on one operation is sufficient to ensure that we get a quotient rack.

Example 4.2.1. Trivial Quandle. In a trivial quandle, $x \triangleright y = x$ for all $x, y \in R$. Therefore $x' \triangleright y \sim x \triangleright y$ implies $x' \sim x$ and therefore $[x'] = [x]$.

Example 4.2.2. Involutory Rack. In an involutory rack, $(x \triangleright y) \triangleright y = x$ for all $x, y \in R$. Since we have $(x' \triangleright y) \sim (x \triangleright y)$ and trivially $y \sim y$ therefore

$x' = (x' \triangleright y) \triangleright y \sim (x \triangleright y) \triangleright y = x$. Therefore $[x'] = [x]$.

The previous involutory rack example can be generalised to a rack that has the property that $(\cdots(x \triangleright y) \triangleright y)\cdots \triangleright y) = x$, for some finite repeated action of y.

Theorem 4.2.3. *Let $\sim$ be a $\triangleright$-congruence on a rack R. Assume that for each $y \in R$ there is $n \in \mathbb{N}$ such that:*

$$x \triangleright^n y = x$$

for all $x \in R$. Then

1. *The $\triangleright$-congruence, $\sim$ is a rack congruence and the quotient $R/\sim$ is a rack;*
2. *If R is a quandle, then $\sim$ is a quandle congruence and the quotient $R/\sim$ is a quandle.*

Remark 4.2.4. In Example 4.2.1 for all y we have $n = 1$. In Example 4.2.2 for all y we have $n = 2$.

We now prove Theorem 4.2.3.

Proof. In a rack R suppose $\sim$ is a $\triangleright$-congruence. Choose any $y, z \in R$ and suppose x is the unique solution of $x \triangleright y = z$. Therefore in the quotient $[x] \triangleright [y] = [x \triangleright y] = [z]$. So the equation $[x] \triangleright [y] = [z]$ has a solution and we need to show that the solution is unique. Suppose we have $x' \in R$

with $[x'] \triangleright [y] = [z]$. Therefore we have both $x \triangleright y \in [z]$ and $x' \triangleright y \in [z]$ and $x \triangleright y \sim x' \triangleright y$. By repeated action by y on the right we then get for all $k \in \mathbb{N}$, $x' \triangleright^k y \sim x \triangleright^k y$. In particular, there exists $n\mathbb{N}$ such that $x = x \triangleright^n y \sim x' \triangleright^n y = x'$ and therefore $x' \in [x]$ and $[x'] = [x]$. Therefore we have invertibility in the quotient.

We get self-distributivity in the quotient from Corollary 3.2.8 — a shelf with a congruence necessarily means that the quotient is a shelf. Since we have invertibility and self-distributivity in the quotient the quotient is a rack.

From the contrapositive to Theorem 4.1.2 we have from existence of a quotient rack that $\sim$ is a rack congruence.

Finally, if R is a quandle then from Corollary 3.2.10 we know the quotient is a spindle. A spindle that is a rack is a quandle. Also since we have a rack congruence on a quandle we necessarily have a quandle congruence. □

This property is always present in a finite rack since the rack operation is essentially a permutation which necessarily has finite order. Therefore we have as a corollary that in any finite rack any congruence is a rack congruence and the quotient is a rack.

Corollary 4.2.5. *Let R be a finite rack and $\sim$ be a $\triangleright$-congruence then $\sim$ is a rack congruence and the quotient $R/{\sim}$ is a rack.*

If R is a quandle then $\sim$ is a quandle congruence and the quotient $R/{\sim}$ is a quandle.

Proof. Since for $x, y \in R$, $x \triangleright y = xS_y$, where S_y is the symmetry at y and is a permutation of the elements of R by brute force we have $S_y^{|R|!} = \mathrm{Id}_R$, where $|R|!$ is the number of elements in the symmetric group on $|R|$ symbols. Therefore $xS_y^{|R|!} = x$ and the conditions in Theorem 4.2.3 are satisfied.

Therefore in every finite rack a $\triangleright$-congruence is a rack congruence and the quotient is a rack. Similarly, in every finite quandle a $\triangleright$-congruence is a quandle congruence and the quotient is a quotient. □

4.3 Half congruence examples

In general, in infinite racks, we need a stronger congruence condition to ensure that $R/{\sim}$ is a rack. The stronger condition is that the congruence respects both the rack operation and the inverse rack operation. To illustrate this, we give some counterexamples of the proposition that a $\triangleright$-congruence allows us to construct a quotient rack. That is we have a congruence condition on one rack operation but the quotient is not a rack or equivalently, these are examples where we have a $\triangleright$-congruence but not a $\triangleleft$-congruence and consequently the resulting quotient is not a rack. Succinctly, they are examples of half congruences.

4.3.1 Half congruence in a rack on $\mathbb{Z} \times \mathbb{Z}$

In the first example of a half congruence, we define equivalence classes on ordered pairs of integers based on the first integer in the pair. Viewing the rack operation as a symmetry at each element of $\mathbb{Z} \times \mathbb{Z}$ we will see that the symmetries can map members of two distinct equivalence classes into one equivalence class. Then, as a result, in the quotient we lose invertibility because for each equivalence class we cannot return to a single unique equivalence class.

Essentially, while in the rack, the rack operation at y, which we can think of as the symmetry S_y on the ordered pairs in $\mathbb{Z} \times \mathbb{Z}$, is one-to-one as is needed, in the quotient the induced map becomes two to one and therefore is no longer a bijection. Thus invertibility is necessarily lost.

The picture is that in the rack every member of two distinct congruence classes, say $[x_1]$ and $[x_2]$, are mapped by the symmetry at y to one congruence class, say $[z]$. Then when we work in the quotient and try to solve the equation $[x] \triangleright [y] = [z]$ we have no information to determine whether we have come from $[x_1]$ or $[x_2]$. There is no way to determine a unique solution.

Example 4.3.1 (half congruence example). Let $R = \mathbb{Z} \times \mathbb{Z}$ and define a binary operation on R by

$$(i,j) \triangleright (m,n) = f(i,j) = \begin{cases} \left(\frac{i}{2}, 2j\right), & i \equiv 0 \mod 2 \\ \left(\frac{i+1}{2}, 2j+1\right), & i \equiv 1 \mod 2. \end{cases}$$

Note the binary operation is dependent only on the first element, (i,j). That is, $(i,j) \triangleright (m,n) = f(i,j)$. We showed in Example 2.2.2 that such an operation always defines a rack provided f is a bijection.

We show that f is a bijection by constructing an inverse function $g = f^{-1}$.

For all, $(x, y) \in \mathbb{R} \times \mathbb{R}$ define,

$$g(x,y) = \begin{cases} \left(2x, \frac{y}{2}\right) & y \equiv 0 \mod 2 \\ \left(2x-1, \frac{y-1}{2}\right) & y \equiv 1 \mod 2. \end{cases}$$

We can see that $f \circ g = g \circ f$ is the identity function so f is a bijection with inverse $f^{-1} = g$ and $(R, \triangleright)$ is a rack. The inverse operation is:

$$(i,j) \triangleleft (m,n) = g(i,j) = \begin{cases} \left(2i, \frac{j}{2}\right), & j \equiv 0 \mod 2 \\ \left(2i-1, \frac{j-1}{2}\right), & j \equiv 1 \mod 2. \end{cases}$$

On this rack we can define an equivalence relation, $\sim$, by $(i, j) \sim (m, n)$ if and only if $i = m$. It is easily confirmed that $\sim$ is an equivalence relation:

1. **Reflexive.** For all $(i, j) \in R$, $(i, j) \sim (i, j)$ since $i = i$.
2. **Symmetric.** For all $(i, j), (m, n) \in R$, if $(i, j) \sim (m, n)$ then $(m, n) \sim (i, j)$ since equality is symmetric.
3. **Transitive.** For all $(i, j), (m, n), (p, q) \in R$, if $(i, j) \sim (m, n)$ and $(m, n) \sim (p, q)$ then $i = m = p$ and therefore $(i, j) \sim (p, q)$.

Moreover, since for all $(i, j), (m, n), (p, q), (r, s) \in R$, if $(i, j) \sim (m, n)$ and $(p, q) \sim (r, s)$ then

$$(i,j) \triangleright (p,q) = \begin{cases} \left(\frac{i}{2}, 2j\right) & i \equiv 0 \mod 2 \\ \left(\frac{i+1}{2}, 2j+1\right) & i \equiv 1 \mod 2 \end{cases}$$

$$\begin{aligned} &\sim \begin{cases} \left(\frac{m}{2}, 2n\right) & m \equiv 0 \mod 2 \\ \left(\frac{m+1}{2}, 2n+1\right) & m \equiv 1 \mod 2 \end{cases} \\ &= (m,n) \triangleright (r,s). \end{aligned}$$

That is, $\sim$ has the congruence property with respect to the binary operation, $\triangleright$. However, in the quotient $\mathbb{Z} \times \mathbb{Z}/\sim$, for all $[(m,n)], [(p,q)] \in R/\sim$ the equation

$$[(x,y)] \triangleright [(m,n)] = [(p,q)] \tag{4.3.1}$$

has solutions but they are not unique.

Suppose, without loss of generality, that $q = 2r$. Then $(p, 2r) \in [(p,q)]$ and

$$[(x,y)] = [(2p, r)]$$

is a solution of equation (4.3.1). However, we also have $(p, 2r+1) \in [(p,q)]$ so

$$[(x,y)] = [(2p-1, r)]$$

is also a solution of equation (4.3.1). Since $[(2p,r)] \neq [(2p-1,r)]$ the solution to equation (4.3.1) is not unique in the quotient $R/\sim$ and so $R/\sim$ is not a rack.

The rack operation, $(x,y) \triangleright (w,z) = f(x,y)$, maps all of the elements from two distinct equivalence classes into one equivalence class. When we try to invert this operation we cannot therefore return to one distinct equivalence class.

We can also see that the equivalence relation does not respect the inverse rack operation. If we take the two elements $(p, 2r)$ and $(p, 2r+1)$ then we can see that $(p, 2r) \sim (p, 2r+1)$. However,

$$(p, 2r) \triangleleft (a, b) = (2p, r) \not\sim (2p-1, r) = (p, 2r+1) \triangleleft (a, b)$$

and therefore $\sim$ does not respect the inverse rack operation. Therefore we have established that $\sim$ is a half congruence.

4.3.2 Bi-infinite Cantor sequence example

In the second half congruence example we work with bi-infinite Cantor sequences. The rack operation is to shift the sequence one place to the left so that the inverse operation is to shift the sequence one place to the right. The equivalence relation is based on one half of the sequence being identical. The left shift means that we lose information about one element from that half sequence in the equivalence class. Again, so while the symmetry functions in the rack are one-to-one, in the quotient, the symmetry functions become two to one and so do not have a bijection and therefore invertibility is lost. So the quotient cannot be a rack and the equivalence relation will be a half congruence and not a rack congruence.

First, we define what we mean here by a Cantor sequence.

Definition 4.3.2 (Cantor sequence)**.** A *Cantor sequence* is a countably infinite sequence (c_i). Typically, the Cantor sequence is defined for $i \in \mathbb{N}$ or $i \in \mathbb{Z}$. A Cantor sequence is *bi-infinite* if it extends indefinitely in both the positive and negative directions, that is when it is defined for all $i \in \mathbb{Z}$. So in a bi-infinite Cantor sequence we have the following form $(\cdots, c_{-2}, c_{-1}, c_0, c_1, c_2, \cdots)$. We will describe a Cantor sequence as *binary* if and only if each $c_i \in \{0, 1\}$.

Now we can present an example of a half congruence using Cantor sequences.

Example 4.3.3 (Bi-Infinite Cantor Sequences Rack Example). We define a rack on bi-infinite Cantor sequences of binary digits. That is, our rack is

$$C = \{a = (a_i) \mid a_i \in \{0, 1\}, i \in \mathbb{Z}\}.$$

We define the rack operation by $a \triangleright b = l(a)$ where $l(a)$ is the left shift operator defined for all $i \in \mathbb{Z}$ by $(l(a))_i = a_{i+1}$, so that each term in the sequence is shifted one place to the left by the rack operation. Note that the inverse rack operation will be the right shift operator, r, which is defined for all $i \in \mathbb{Z}$ by, $(r(a))_i = a_{i-1}$. Therefore, $a \triangleleft b = l^{-1}(a) = r(a)$.

As in the previous example we can establish that $(C, \triangleright)$ is a rack by noting that the left shift operator, l, is a bijection and depends only on a thus $a \triangleright b = f(a)$ which is the condition noted in Example 2.2.2 that such a function defines a rack.

Here it is also very easy to check the rack axioms directly.

1. Invertibility: For all $a, b \in C$,

$$(a \triangleright b) \triangleleft b = l(a) \triangleleft b = r(l(a)) = a;$$

2. Distributivity: For all $a, b, c \in C$,

$$(a \triangleright b) \triangleright c = l(a) \triangleright c = l(l(a)) = l(a \triangleright c) = (a \triangleright c) \triangleright (b \triangleright c).$$

Therefore $(C, \triangleright)$ is a rack.

We introduce an equivalence, $\sim$, on C, where for all $a, b \in C$, $a \sim b$ if and only if $a_i = b_i$ for all $i \in \mathbb{N}$. This relationship clearly partitions C and thus is an equivalence relation.

We see that the rack operation is well defined on equivalence classes of $\sim$. For all $x, y \in C$, for all $a, b \in [x]$ and $c, d \in [y]$,

$$a \triangleright c = l(a) \sim l(x) \sim l(b) = b \triangleright d,$$

so

$$[x] \triangleright [y] = [l(x)].$$

However, as we shall see, the equation $[x] \triangleright [y] = [z]$ does not have a unique solution $[x]$. We can always find two sequences, a and b in $[z]$ with $a = z$ and $b_i = a_i$ except when $i = 0$, so that $b_0 = 0$ when $z_0 = 1$ and $b_0 = 1$ when $z_0 = 0$. Now when we apply the inverse operation (the right shift operator) we obtain two sequences, $r(a)$ and $r(b)$ with $r(a)_1 \neq r(b)_1$ and therefore $r(a)$ and $r(b)$ are not in the same equivalence class. Consequently,

$$[r(a)] \neq [r(b)]$$

and the solution is not unique. Therefore the quotient $C/{\sim}$ is not a rack and $\sim$ is a half congruence and not a rack congruence.

We can see that $\sim$ is not a $\triangleleft$-congruence directly by taking two sequences $a, b \in C$ with $a \sim b$ but $a_0 = 0$ and $b_0 = 1$. Now for any $c \in C$ we have $a \triangleleft c = r(a) \not\sim r(b) = b \triangleleft c$ since $r(a)_1 = 0 \neq 1 = r(b)_1$.

4.3.3 Bi-infinite Cantor sequence quandle example

We need to work a little harder to extend this sort of example to a quandle. It is not a quandle as described as the idempotence axiom does not apply, in general $a \triangleright a = l(a) \neq a$. This can be fixed by the introduction of a second equivalence relation and a modification to the rack operation based on this second equivalence relation.

Example 4.3.4 (Bi-infinite Cantor sequence quandle example). As in Example 4.3.3, let $C = \{a = (a_i) \mid a_i \in \{0, 1\}, i \in \mathbb{Z}\}$ and let $\sim$ be an equivalence relation with for all $a, b \in C$, $a \sim b$ if and only if $a_i = b_i$ for all $i \in \mathbb{N}$.

We introduce a second equivalence relation $\approx$ on C, where for all $a, b \in C$, $a \approx b$ if and only if there exists $s, t \in \mathbb{Z}$ such that $l^s(a) \sim l^t(b)$. That is, we can apply some (usually different) number of left (or right, since s and t can be negative) shifts to a and b so that the resultant sequences are equivalent by the first equivalence relation, $\sim$.

Effectively, this means whenever $a \approx b$ that for all $i \in \mathbb{N}$ we have $a_{i+s} = b_{i+t}$

for some $s, t \in \mathbb{Z}$. As a consequence, whenever $a \approx b$ and $b \sim c$ we have $a \approx c$. We state this as a lemma as it will be used below.

Lemma 4.3.5. *Let* $C = \{a = (a_i) \mid a_i \in \{0, 1\}, i \in \mathbb{Z}\}$ *and let* $\sim$ *and* $\approx$ *be equivalence relations with for all* $a, b \in C$, $a \sim b$ *if and only if* $a_i = b_i$ *for all* $i \in \mathbb{N}$ *and* $a \approx b$ *if and only if there exists* $s, t \in \mathbb{Z}$ *such that* $l^s(a) \sim l^t(b)$. *Then if* $a \approx b$ *and* $b \sim c$ *we have that* $a \approx c$.

Proof. Assume $a \approx b$ and $b \sim c$ for some $a, b, c \in C$ and that $l^s(a) = l^t(b)$ for some $s, t \in \mathbb{Z}$.

If $t > 0$ we have immediately from $b \sim c$ that $a_{i+s} = b_{i+t} = c_{i+t}$ and so $a \approx c$. If $t \leq 0$ then we know $b_{i+t} = c_{i+t}$ whenever $i > t$ so $a_{i+s} = c_{i+t}$ for $i > t$ which by putting $j = i + t$ is equivalent to $a_{j-t+s} = c_j$ for $j > 0$. That is $l^{s-t}(a) \sim l^0(c)$ and therefore $a \approx c$. □

Now we define a quandle operation on C that is contingent on this second equivalence relation:

$$a \triangleright b = \begin{cases} a, & a \approx b \\ l(a), & a \not\approx b. \end{cases}$$

Note that the inverse operation will be:

$$a \triangleleft b = \begin{cases} a, & a \approx b \\ r(a), & a \not\approx b. \end{cases}$$

In this example, unlike the previous example, the quandle operation $a \triangleright b$

depends on both a and b so is not a function $f = f(a)$ and so we check the quandle axioms to establish that we have defined a quandle:

1. Idempotence: For all $a \in C$, $a \triangleright a = a$ since $a \approx a$;
2. Invertibility: For all $a, b \in C$,

$$\begin{aligned}
(a \triangleright b) \triangleleft b &= \begin{cases} a \triangleleft b, & a \approx b \\ l(a) \triangleleft b, & a \not\approx b \end{cases} \\
&= \begin{cases} a, & a \approx b \\ r(l(a)), & a \not\approx b \end{cases} \\
&= a;
\end{aligned}$$

3. Distributivity: For all $a, b, c \in C$,

$$(a \triangleright b) \triangleright c = \begin{cases} a, & a \approx b, a \approx c \\ l(a), & a \approx b, a \not\approx c \\ l(a), & a \not\approx b, a \approx c \\ l^2(a), & a \not\approx b, a \not\approx c, \end{cases}$$

and

$$\begin{aligned}(a \triangleright c) \triangleright (b \triangleright c) &= \begin{cases} a, & a \approx c, a \approx b \\ l(a) & a \not\approx c, a \approx b \\ l(a) & a \approx c, a \not\approx b \\ l^2(a) & a \not\approx c, a \not\approx b \end{cases} \\ &= (a \triangleright b) \triangleright c.\end{aligned}$$

Note, we use the fact that for all $a, b \in C$, $a \approx b$ if and only if $a \approx l(b)$.

The quandle operation is well defined on the equivalence classes of $\sim$. For all $x, y \in C$, for all $a, b \in [x]$ and $c, d \in [y]$,

$$a \triangleright c = \begin{cases} a, & a \approx c \\ l(a), & a \not\approx c. \end{cases} \tag{4.3.2}$$

Since $a \sim b$ and $c \sim d$, whenever $a \approx c$ in equation (4.3.2) we have from Lemma 4.3.5 that $a \approx d$ and then from that, $b \approx d$. We can then establish, as shown below in equation (4.3.3), that $a \triangleright c \sim b \triangleright d$ since the conditions $a \approx c$ and $b \approx d$ are either simultaneously true or simultaneously false. Since

$a \sim b$ we also have $l(a) \sim l(b)$ and therefore:

$$\begin{aligned} a \triangleright c &= \begin{cases} a, & a \approx c \\ l(a), & a \not\approx c \end{cases} \\ &\sim \begin{cases} b, & b \approx d \\ l(b), & b \not\approx d \end{cases} \\ &= b \triangleright d. \end{aligned} \tag{4.3.3}$$

However, as above in Example 4.3.3, the equation $[x] \triangleright [y] = [z]$, where the equivalence classes are with respect to the equivalence relation, $\sim$, does not necessarily have a unique solution $[x]$.

To see this, choose $y \not\approx z$ so that $z \triangleleft y = r(z)$. We can find two sequences, a and b in $[z]$ with, for example, $a = z$ and $b_i = a_i$ except when $i = 0$ where $b_0 = 0$ if $a_0 = z_0 = 1$ or $b_0 = 1$ if $a_0 = z_0 = 0$. When we apply the inverse operation (which is the right shift operator since $y \not\approx z$) to a and b we get two sequences, $r(a)$ and $r(b)$ with $r(a) \not\sim r(b)$ since $r(a)_1 \neq r(b)_1$ and so $r(a)$ and $r(b)$ are not in the same equivalence class. Therefore $[r(a)] \neq [r(b)]$ and the quotient, $C/\sim$ is not a quandle and $\sim$ is a half congruence and not a quandle congruence.

Remark 4.3.6. Obviously the theme in this example is not restricted to binary sequences and can be extended to any bi-infinite sequences as the binary nature of the infinite sequences does not play a role. In particular there is a similarity between these bi-infinite sequences of binary digits and the real numbers.

4.3.4 Real number example

If a real number, r is represented in binary form and the binary point removed then r can be thought of as a bi-infinite sequence of binary digits r_i, where say the binary point comes to the right of r_0. It is easy to see, that the non-negative real numbers are a proper subset of $C = \{a = (a_i) \mid a_i \in \{0, 1\}, i \in \mathbb{Z}\}$. There are two types of elements of C that need to be excluded to uniquely represent the non-negative real numbers:

1. For $a \in C$ to represent a real number we need $a_i = 0$ for all $i < s$ for some $s \in \mathbb{Z}$.

2. We need to eliminate the binary equivalent of infinite repeating decimals. We do this by excluding infinite repeating ones to the right. That is, for $a \in C$ to represent a real number for all $t \in \mathbb{Z}$ we need $a_i = 0$ for some $i > t$.

This theme can be extended to the following example with real numbers and a decimal shift.

Example 4.3.7 (Real numbers with a decimal shift). Define an equivalence relation $\sim$ on the real numbers, $\mathbb{R}$ as for all $x, y \in \mathbb{R}$, $x \sim y$ if and only if the fractional part of x,

$$\operatorname{frac}(x) = \begin{cases} x - \lfloor x \rfloor, & x \geq 0 \\ x - \lceil x \rceil, & x < 0 \end{cases},$$

is equal to the fractional part of y, $\operatorname{frac}(y)$. As in Example 4.3.4, we define a second equivalence relation, $\approx$, so that $x \approx y$ if and only if there exists $s, t \in \mathbb{Z}$ such that $10^s x \sim 10^t y$. Now again following the previous example, we define a quandle operation:

$$x \rhd y = \begin{cases} x, & x \approx y \\ 10x, & x \not\approx y \end{cases}.$$

The inverse quandle operation will be:

$$x \lhd y = \begin{cases} x, & x \approx y \\ x/10, & x \not\approx y \end{cases}.$$

Note that multiplying and dividing by 10 are effectively right and left shifts of the decimal point in the decimal representation of real numbers.

We can see that $(\mathbb{R}, \rhd)$ is a quandle by checking the quandle axioms:

1. Idempotence: For all $x \in \mathbb{R}$, $x \rhd x = x$ since $x \approx x$;

2. Invertibility: For all $x, y \in \mathbb{R}$,

$$\begin{aligned}(x \triangleright y) \triangleleft y &= \begin{cases} x \triangleleft y, & x \approx y \\ (10x) \triangleleft y, & x \not\approx y \end{cases} \\ &= \begin{cases} x, & x \approx y \\ x & x \not\approx y \end{cases} \\ &= x;\end{aligned}$$

3. Distributivity: For all $x, y, z \in \mathbb{R}$,

$$(x \triangleright y) \triangleright z = \begin{cases} x, & x \approx y, x \approx z \\ 10x, & x \approx y, x \not\approx z \\ 10x, & x \not\approx y, x \approx z \\ 100x, & x \not\approx y, x \not\approx z, \end{cases}$$

and

$$\begin{aligned}(x \triangleright z) \triangleright (y \triangleright z) &= \begin{cases} x, & x \approx z, x \approx y \\ 10x, & x \approx z, x \not\approx y \\ 10x, & x \not\approx z, x \approx y \\ 100x, & x \not\approx z, x \not\approx y \end{cases} \\ &= (x \triangleright y) \triangleright z.\end{aligned}$$

However the equation $[x] \triangleright [y] = [z]$, where the equivalence classes are with respect to the equivalence relation, $\sim$, does not necessarily have a unique solution, $[x]$. For example, for $x, y > 0$, if $x \not\approx y$ and $x + 0.1 \not\approx y$ then since $x \not\sim (x+0.1)$, $(x+0.1) \notin [x]$ but $(x \triangleright y) = 10x \sim (10x+1) = (x+0.1) \triangleright y$ so $(x+0.1) \triangleright y \in [x \triangleright y]$. That is both $[x] \triangleright [y]$ and $[x+0.1] \triangleright [y]$ are in $[x \triangleright y]$.

4.3.5 A finitely presented countable example

Examples 4.3.3, 4.3.4, and 4.3.7 featured racks and quandles that were uncountably infinite. Example 4.3.1 was on a countably infinite set. We present here another countable example that has the feature that it can be finitely presented.

Example 4.3.8 (**Countable quandle example**)**.** Let

$$Q = \{a^k : k \in \mathbb{Z}\} \bigcup \{b^j : j \in \mathbb{Z}\} \bigcup \{c\}$$

where $\{a, b, c\}$ is a set of symbols.

Define a binary operation, $\triangleright$, on Q by

$$x \triangleright y = \begin{cases} x, & x = c \text{ or } y = \alpha^k, k \in \mathbb{Z} \\ \alpha^{k+1}, & x = \alpha^k \text{ and } y = c. \end{cases}$$

Where $\alpha \in \{a, b\}$.

It is easy to show that $(Q, \triangleright)$ is a quandle. There are several cases to check but their number can be reduced by writing α^k to mean either a^k or b^k since the action of a^k and b^k is the same on every element in Q. Similarly, β^k and γ^k will also be used to represent elements of Q of the form a^k or b^k.

1. **Idempotence** — there are two cases. In both cases idempotence follows by definition of the binary operation, $\rhd$.
    (a) $\alpha^k \rhd \alpha^k = \alpha^k$ since we have $y = \alpha^k$;
    (b) $c \rhd c = c$ since we have $x = c$.
2. **Invertibility** — there are four cases. Each case has a unique solution as follows:
    (a) $x \rhd \alpha^k = \beta^j$ has the unique solution $x = \beta^j$,
    (b) $x \rhd \alpha^k = c$ has the unique solution $x = c$,
    (c) $x \rhd c = \alpha^k$ has the unique solution $x = \alpha^{k-1}$,
    (d) $x \rhd c = c$ has the unique solution $x = c$.
3. **Distributivity** — there are eight cases to check as follows:
    (a) $(\alpha^k \rhd \beta^j) \rhd \gamma^l = \alpha^k \rhd \gamma^l = \alpha^k$ and

    $(\alpha^k \rhd \gamma^l) \rhd (\beta^j \rhd \gamma^l) = \alpha^k \rhd \beta^j = \alpha^k$,

    (b) $(\alpha^k \rhd \beta^j) \rhd c = \alpha^k \rhd c = \alpha^{k+1}$ and

    $(\alpha^k \rhd c) \rhd (\beta^j \rhd c) = \alpha^{k+1} \rhd \beta^{j+1} = \alpha^{k+1}$,

(c) $(\alpha^k \triangleright c) \triangleright \gamma^l = \alpha^{k+1} \triangleright \gamma^l = \alpha^{k+1}$ and

$(\alpha^k \triangleright \gamma^l) \triangleright (c \triangleright \gamma^l) = \alpha^k \triangleright c = \alpha^{k+1}$,

(d) $(c \triangleright \beta^j) \triangleright \gamma^l = c \triangleright \gamma^l = c$ and

$(c \triangleright \gamma^l) \triangleright (\beta^j \triangleright \gamma^l) = c \triangleright \beta^j = c$,

(e) $(\alpha^k \triangleright c) \triangleright c = \alpha^{k+1} \triangleright c = \alpha^{k+2}$ and

$(\alpha^k \triangleright c) \triangleright (c \triangleright c) = \alpha^{k+1} \triangleright c = \alpha^{k+2}$,

(f) $(c \triangleright \beta^j) \triangleright c = c \triangleright c = c$ and

$(c \triangleright c) \triangleright (\beta^j \triangleright c) = c \triangleright \beta^{j+1} = c$,

(g) $(c \triangleright c) \triangleright \gamma^l = c \triangleright \gamma^l = c$ and

$(c \triangleright \gamma^l) \triangleright (c \triangleright \gamma^l) = c \triangleright c = c$,

(h) $(c \triangleright c) \triangleright c = c \triangleright c = c$ and

$(c \triangleright c) \triangleright (c \triangleright c) = c \triangleright c = c$.

Therefore $(Q, \triangleright)$ is a quandle.

Remark 4.3.9. From the calculations to establish the invertibility axiom holds, we can construct the inverse quandle operation. The inverse quandle operation is given by:

$$x \triangleleft y = \begin{cases} x, & x = c \text{ or } y = \alpha^k, k \in \mathbb{Z} \\ \alpha^{k-1}, & x = \alpha^k \text{ and } y = c. \end{cases}$$

On this quandle we can define an equivalence relation, $\sim$, where for all $x, y \in Q$, $x \sim y$ if and only if either $x = y$ or $x = \alpha^i$ and $y = \beta^i$ for some $i > 0$ with $\alpha, \beta \in \{a, b\}$. That is, the congruence classes either consist of two elements of Q, namely $[a^i] = [b^i] = \{a^i, b^i\}$ for each $i > 0$ or in every other case, the congruence classes is a singleton, either $[c] = \{c\}$, $[a^i] = \{a^i\}$ or $[b^i] = \{b^i\}$, where $i \leq 0$.

There are a number of cases but it is easy to check that this is a congruence. We need whenever $x \sim y$ and $s \sim t$ to have $x \triangleright s \sim y \triangleright t$. If x and s are in congruence classes of cardinality one then $x = y$ and $s = t$ and therefore trivially $x \triangleright s \sim y \triangleright t$. That takes care of $c \triangleright c$, $c \triangleright \alpha^i$, $\alpha^i \triangleright c$, and $\alpha^i \triangleright \beta^j$ for $i, j \leq 0$.

We now need to consider the cases where we have elements from equivalence classes of cardinality two in one or both operands. We will use the generic elements $\alpha, \beta, \gamma, \delta \in \{a, b\}$.

1. If $x = \alpha^j \sim \beta^j = y$ and $s = \gamma^k \sim \delta^k = t$ then $\alpha^j \triangleright \gamma^k = \alpha^j \sim \beta^j = \beta^j \triangleright \delta^k$ for $j, k > 0$.

2. If $x = y = \gamma^k$ and $s = \alpha^j \sim \beta^j = t$ with $j > 0$ and $k \leq 0$ then $x \triangleright \alpha^j = \gamma^k \sim \gamma^k = y \triangleright \alpha^j$.

3. If $x = \alpha^j \sim \beta^j = y$ and $s = t = \gamma^k$ with $j > 0$ and $k \leq 0$ then $\alpha^j \triangleright s = \alpha^j \sim \beta^j = \beta^j \triangleright t$.

4. If $x = y = c$ and $s = \alpha^j \sim \beta^j = t$ with $j > 0$ then $c \triangleright \alpha^j = c \sim c = c \triangleright \beta^j$.

5. If $x = \alpha^j \sim \beta^j = y$ and $s = t = c$ with $j > 0$ then $\alpha^j \triangleright c = \alpha^{j+1} \sim \beta^{j+1} = \beta^j \triangleright c$.

Thus $\sim$ is a $\triangleright$-congruence.

However, for this $\triangleright$-congruence, the quotient $Q/{\sim}$ is not a quandle. The uniqueness axiom breaks down for one equation:

$$[x] \triangleright [c] = [a^1].$$

This equation has two solutions, namely $[x] = [a^0]$ and $[x] = [b^0]$ since $[a^1] = \{a^1, b^1\}$ and both $a^0 \triangleright c = a^1 \in [a^1]$ and $b^0 \triangleright c = b^1 \in [a^1]$ and $a_0 \neq b_0$.

Equivalently, based on what we have just seen, in Q we have $a^0 \triangleright c = a^1$ and $b^0 \triangleright c = b^1$ from which we have $a^1 \triangleleft c = a^0$ and $b^1 \triangleleft c = b^0$. However, since we have $a^1 \sim b^1$ and trivially $c \sim c$ the congruence condition is not satisfied on the inverse quandle operation because

$$a^1 \triangleleft c = a^0 \not\sim b^0 = b^1 \triangleleft c.$$

This illustrates that we do not have a $\triangleleft$-congruence and therefore that since $\sim$ is a $\triangleright$-congruence it must be a half congruence.

Although the quandle from Example 4.3.8 is countably infinite, interestingly it can be finitely presented as

$$\langle a, b, c : a \triangleright b = a, b \triangleright a = b, c \triangleright a = c, c \triangleright b = c \rangle.$$

To show this we will use the following generic understandings:

1. Both of the generic symbols α and β can represent either a or b. That is $\alpha, \beta \in \{a, b\}$.
2. We define $a^1 = a$ and $b^1 = b$ and similarly $\alpha^1 = \alpha$ and $\beta^1 = \beta$.
3. We define α^k inductively by $\alpha^k = \alpha^1 \triangleright^{k-1} c$ for $k > 0$.
4. For $k < 0$, we define $\alpha^k = \alpha^1 \triangleright^{k-1} c = \alpha^1 \triangleleft^{-k+1} c$.
5. We define $\alpha^0 = \alpha \triangleright^{-1} c = \alpha \triangleleft c$.

We need to establish that the presentation implies:

1. For all $j \in \mathbb{Z}$,
$$c \triangleright \alpha^j = c; \tag{4.3.4}$$
2. For all $k, j \in \mathbb{Z}$,
$$\alpha^k \triangleright \beta^j = \alpha^k; \tag{4.3.5}$$
3. The only words that can be generated are of the form a^k, b^k, c. That is, the quandle defined by the presentation, $\{a^j, b^k, c : j, k \in \mathbb{Z}\}$, is closed under the quandle operation and the inverse quandle operation.

We can establish the first two results by induction. However we have to take care of both positive and negative indices. In the second case we will first establish that $\alpha^k \triangleright \beta = \alpha^k$ by induction on k before establishing $\alpha^k \triangleright \beta^j = \alpha^k$ by induction on j.

Immediate consequences for the inverse quandle operation from establishing equations 4.3.4 and 4.3.5 will be that we have established that both:

$$c \triangleleft \alpha^j = c \tag{4.3.6}$$

and

$$\alpha^k \triangleleft \beta^j = \alpha^k \tag{4.3.7}$$

hold.

1. The first result is straightforward as an immediate consequence of distributivity. For negative indices we need to use the distributivity across both binary operations.

   For some $j > 0$, assume $c \triangleright \alpha^j = c$. Then

$$\begin{aligned} & & c \triangleright \alpha^j &= c \\ &\Rightarrow & (c \triangleright \alpha^j) \triangleright c &= c \triangleright c \\ &\Rightarrow & (c \triangleright c) \triangleright (\alpha^j \triangleright c) &= c \\ &\Rightarrow & c \triangleright \alpha^{j+1} &= c. \end{aligned}$$

Since $c \triangleright \alpha = c \triangleright \alpha^1 = c$ we have established $c \triangleright \alpha^j = c$ for all $j > 0$.

Similarly, for some $j \geq -1$, assume $c \triangleright \alpha^{-j} = c$. Then

$$\begin{aligned} & & c \triangleright \alpha^{-j} &= c \\ &\Rightarrow & (c \triangleright \alpha^{-j}) \triangleleft c &= c \triangleleft c \\ &\Rightarrow & (c \triangleleft c) \triangleright (\alpha^{-j} \triangleleft c) &= c \\ &\Rightarrow & c \triangleright \alpha^{-(j+1)} &= c. \end{aligned}$$

Since $c \triangleright \alpha = c \triangleright \alpha^{-(-1)} = c$ we have established $c \triangleright \alpha^{-j} = c$ for all $j \geq -1$.

Therefore $c \triangleright \alpha^j = c$ for all $j \in \mathbb{Z}$. As a result, as noted, by the definition of the inverse quandle operation we also have $c \triangleleft \alpha^j = c$.

2. As foreshadowed the second result is established in two parts. The first part $\alpha^k \triangleright \beta = \alpha^k$ is again an immediate consequence of distributivity. The second part $\alpha^k \triangleright \beta^j$ is obtained by applying distributivity twice and using the result established above that $c \triangleright \alpha^j = c$.

   (a) For some $k > 0$, assume $\alpha^k \triangleright \beta = \alpha^k$. Then

$$\begin{aligned} \alpha^{k+1} \triangleright \beta &= (\alpha^k \triangleright c) \triangleright \beta \\ &= (\alpha^k \triangleright \beta) \triangleright (c \triangleright \beta) \\ &= \alpha^k \triangleright c \\ &= \alpha^{k+1}. \end{aligned}$$

Since $\alpha^1 \triangleright \beta = \alpha \triangleright \beta = \alpha$ we have established $\alpha^k \triangleright \beta = \alpha^k$ for all $k > 0$.

Similarly, for some $k \geq -1$, assume $\alpha^{-k} \triangleright \beta = \alpha^{-k}$. Then

$$\begin{aligned}
\alpha^{-(k+1)} \triangleright \beta &= (\alpha^{-k} \triangleleft c) \triangleright \beta \\
&= (\alpha^{-k} \triangleright \beta) \triangleleft (c \triangleright \beta) \\
&= \alpha^{-k} \triangleleft c \\
&= \alpha^{-(k+1)}.
\end{aligned}$$

Since when $k = -1$ we have $\alpha^{-(-1)} \triangleright \beta = \alpha^1 \triangleright \beta = \alpha \triangleright \beta = \alpha$ we have established $\alpha^{-k} \triangleright \beta = \alpha^{-k}$ for all $k \leq 0$.

Therefore $\alpha^k \triangleright \beta = \alpha^k$ for all $k \in \mathbb{Z}$.

(b) For some $j > 0$, assume $\alpha^k \triangleright \beta^j = \alpha^k$, for all $k \in \mathbb{Z}$. Then

$$\begin{aligned}
\alpha^k \triangleright \beta^{j+1} &= (\alpha^{k-1} \triangleright c) \triangleright (\beta^j \triangleright c) && \text{(definition } \alpha^k, \beta^{j+1}) \\
&= (\alpha^{k-1} \triangleright \beta^j) \triangleright c && \text{(distributivity)} \\
&= \alpha^{k-1} \triangleright c && \text{(definition } \triangleright) \\
&= \alpha^k && \text{(definition } \triangleright).
\end{aligned}$$

Since $\alpha^k \triangleright \beta^1 = \alpha^k \triangleright \beta = \alpha^k$ we have established $\alpha^k \triangleright \beta^j = \alpha^k$ for all $j > 0$.

Similarly, for some $j \geq -1$, assume $\alpha^k \triangleright \beta^{-j} = \alpha^k$ for all $k \in \mathbb{Z}$.

Then

$$\begin{aligned}
\alpha^k \triangleright \beta^{-(j+1)} &= (\alpha^{k-1} \triangleright c) \triangleright (\beta^{-(j+2)} \triangleright c) && \text{(definition } \alpha^k, \beta^{-(j+1)}\text{)}\\
&= (\alpha^{k-1} \triangleright \beta^{-(j+2)}) \triangleright c && \text{(distributivity)}\\
&= \alpha^{k-1} \triangleright c && \text{(definition } \triangleright\text{)}\\
&= \alpha^k && \text{(definition } \triangleright\text{).}
\end{aligned}$$

Since for $j = -1$ we have $\alpha^k \triangleright \beta^{-(-1)} = \alpha^k \triangleright \beta^1 = \alpha^k \triangleright \beta = \alpha^k$ we have established $\alpha^k \triangleright \beta^{-j} = \alpha^k$ for all $j \geq -1$.

Therefore $\alpha^k \triangleright \beta^j = \alpha^k$ for all $k, j \in \mathbb{Z}$. Again, as a result we have also established that $\alpha^k \triangleleft \beta^j = \alpha^k$.

3. We need to show that no words other than a^k, b^k, and c can be generated. Again, the number of cases to be checked can be reduced to four by writing α^k and β^k to mean either of a^k or b^k. The four cases to consider are:

   (a) We need $\alpha^m \triangleright \beta^n \in \{a^j, b^k, c\}$ which is established from equation (4.3.5) which gives $\alpha^m \triangleright \beta^n = \alpha^m \in \{a^j, b^k, c\}$ as required.

   Similarly, (4.3.7) gives $\alpha^m \triangleleft \beta^n = \alpha^m \in \{a^j, b^k, c\}$.

   (b) We need $\alpha^m \triangleright c \in \{a^j, b^k, c\}$ and we have by definition that $\alpha^m \triangleright c = \alpha^{m+1} \in \{a^j, b^k, c\}$.

   Similarly, by definition $\alpha^m \triangleleft c = \alpha^{m-1} \in \{a^j, b^k, c\}$.

(c) We need $c \triangleright \alpha^m \in \{a^j, b^k, c\}$ and we have from equation (4.3.4) above that $c \triangleright \alpha^m = c \in \{a^j, b^k, c\}$.

Similarly, from equation (4.3.6) we have $c \triangleleft \alpha^m = c \in \{a^j, b^k, c\}$.

(d) Finally axiomatically we have both $c \triangleright c = c \in \{a^j, b^k, c\}$ and $c \triangleleft c = c \in \{a^j, b^k, c\}$.

Therefore the set $\{a^j, b^k, c : j, k \in \mathbb{Z}\}$ defined by the presentation is closed under both the quandle operation and the inverse quandle operation.

Remark 4.3.10. Example 4.3.8 can be thought of as a subquandle of Example 4.3.4. That is, Example 4.3.8 is isomorphic to a subquandle of Example 4.3.4. We can construct the subquandle by taking any two distinct non-zero sequences, a and b, that are related by $\approx$. For example we can choose a_i and b_i such that $a_i = b_i$ for all $i > 0$, and $a_i = b_i = 0$ for all $i < 0$ and $a_0 = 0$ and $b_0 = 1$. Clearly $a \approx b$, therefore $a \triangleright b = a$ and $b \triangleright a = b$. We also need $a_j = 1$ for some $j > m$ for all $m > 0$. This ensures that $a \not\approx c$, where c is the zero sequence, that is, $c_i = 0$ for all $i \in \mathbb{Z}$.

Since $a \not\approx c$ therefore $a \triangleright c = l(a)$. Therefore we have $a^k = l^{k-1}(a)$. However, similarly $c \triangleright a = l(c)$ but we have chosen c carefully so that $l(c) = c$.

Therefore this sub-quandle is presented by $a \triangleright b = a$, $b \triangleright a = b$, $c \triangleright a = c$ and $c \triangleright b = c$ and so is isomorphic to Example 4.3.8.

Chapter 5

Averaging Quandles on $\mathbb{Q}$

In this chapter we investigate the structure of congruence classes in averaging quandles on the set of rational numbers, $\mathbb{Q}$. We will begin by investigating the averaging quandle in which the quandle operation is the simple arithmetic mean of the two elements. Later, we will extend our discussion to quandles where the operation is a weighted average, which is a generalisation of the arithmetic mean. Throughout, we will assume that the quandle is on $\mathbb{Q}$. However, typically the results can be extended to the set of real numbers, $\mathbb{R}$. Averaging quandles are examples of Alexander quandles.

5.1 The averaging quandle on $\mathbb{Q}$

5.1.1 Definition

We introduced the averaging quandle in Example 2.2.28, where we showed that the arithmetic mean of two numbers satisfies the quandle axioms. The averaging quandle is also an example of an Alexander quandle from Definition 2.2.20 with $t = \frac{1}{2}$ in $x \triangleright y = tx + (1-t)y$ and t acts on x by multiplication. More generally, we proved that any Alexander quandle is a quandle in Theorem 2.2.22. Here we formally define the averaging quandle.

Definition 5.1.1. The **averaging quandle** on $\mathbb{Q}$ is a quandle in which the binary operation in the quandle is

$$x \triangleright y = \frac{x+y}{2},$$

the arithmetic mean of the two quandle elements, x and y. We will write Q_A to refer to the averaging quandle.

In this section, we will show that in the averaging quandle, the congruence condition on the quandle operation implies the congruence condition on the inverse quandle operation. That is, in the averaging quandle a $\triangleright$-congruence implies a $\triangleleft$-congruence and therefore a quandle congruence. We show this in Section 5.1.4. Curiously, we will see in Section 5.1.5, that this implication does not flow in the opposite direction, that is a $\triangleleft$-congruence does not imply a $\triangleright$-congruence.

5.1.2 Structure of congruences on Q_A

We begin by investigating the structure of a $\triangleright$-congruence in the averaging quandle. Recall that for a $\triangleright$-congruence, $\sim$, whenever $a \sim b$ and $c \sim d$ we have the congruence condition

$$a \triangleright c \sim b \triangleright d.$$

For the averaging quandle, $Q_A = (\mathbb{Q}, \triangleright)$, this means that

$$\frac{a+c}{2} \sim \frac{b+d}{2}$$

whenever $a \sim b$ and $c \sim d$.

Since, by the reflexive property, in any $\triangleright$-congruence every element is related to itself then we can replace both c and d in the above expressions by any one element in the quandle. In particular, we can set $c = d = 0$ and we obtain, if $a \sim b$ then

$$\frac{a}{2} \sim \frac{b}{2}.$$

This process can be repeated inductively to show

$$\frac{a}{2^k} \sim \frac{b}{2^k}, \text{ for all } k \in \mathbb{N}. \tag{5.1.1}$$

More generally when $a \sim b$, for all $x \in Q_A$ we have

$$\frac{a+x}{2} \sim \frac{b+x}{2}. \tag{5.1.2}$$

By a sequence of clever choices of x we will show that any equivalence class, with more than one element, must be an infinite set that is dense in $\mathbb{Q}$.

Note that the inverse quandle operation for the averaging quandle can be seen to be an Alexander quandle with quandle operation

$$x \lhd y = tx + (1-t)y$$

by putting $t = \left(\frac{1}{2}\right)^{-1} = 2$ which acts by multiplication to obtain

$$x \lhd y = 2x - y \tag{5.1.3}$$

We will see in Section 5.2 that this is true in general for weighted average quandles where both the quandle operation and the inverse operation are weighted averages and therefore the inverse quandle operation is an Alexander quandle operation.

Through a series of lemmas we will show that provided a congruence class has two distinct elements then it must be an infinite set that is dense in $\mathbb{Q}$. As a consequence congruence classes have one of only two possible forms:

1. Singletons, $\{x\}$ for $x \in Q_A$;
2. Sets that are dense in $\mathbb{Q}$.

In fact, for a particular congruence it will turn out that every congruence class is of the same form. That is, every congruence class must be a singleton or every congruence class must be a set dense in $\mathbb{Q}$.

We build up the dense set by showing that that two distinct elements in a congruence class imply a third at the midpoint of the two elements. We can inductively apply that result to the new element and the previously known elements to effectively find new elements in vanishingly small intervals between any two elements.

In the first lemma, we show that the midpoint between any two elements in a congruence class must be in the congruence class that contains those two elements.

Lemma 5.1.2. *Let Q_A be the averaging quandle on $\mathbb{Q}$, $\sim$ a $\triangleright$-congruence, $[\alpha]$ a congruence class of Q_A and $a, b \in [\alpha] \subseteq Q_A$, with a and b distinct. Then*

$$\frac{a+b}{2} = a \triangleright b \in [\alpha].$$

Proof. We have $a \sim b$ and we apply the congruence condition with $x = a$ in equation (5.1.2). This gives

$$a = \frac{a+a}{2} \sim \frac{b+a}{2} = \frac{a+b}{2} = a \triangleright b.$$

□

Remark 5.1.3. Obviously, we can repeat this procedure with the constructed element, $\frac{a+b}{2}$, and both original elements, a and b, and any newly constructed elements indefinitely. Assuming without loss of generality $a < b$, this will give us every rational number in the interval $[a, b]$ of the form

$$a + (b - a)D,$$

where $D = \frac{n}{2^k}$ is a dyadic rational, with $0 \leq n \leq 2^k$, n an odd integer and $k \in \mathbb{Z}^*$, where $\mathbb{Z}^*$ is the set of non-negative integers. That is, the congruence class $[\alpha]$ is dense in the interval $[a, b]$ for any $a, b \in [\alpha]$, where we define a dense set on a subset of $\mathbb{Q}$ (or $\mathbb{R}$) in the usual way as we give below in Definitions 5.1.4 and 5.1.5.

Loosely, we will think of a dense subset as a subset in which any element in the overarching set, in our case the rational numbers $\mathbb{Q}$, is arbitrarily close to an element in the subset. Formally, we will use the following definition of a dense set.

Definition 5.1.4 (Dense set). Let $X = [a, b] \subseteq \mathbb{Q}$ be an interval of $\mathbb{Q}$. Then a subset $D \subseteq X$ is **dense** in X if for every point $x \in X$ either: $x \in D$; or x is the limit point of some sequence $\langle d_k \mid k \in \mathbb{N} \rangle$ where each $d_k \in D$.

Definition 5.1.5 (Dense set (alternative)). Let $X = [a, b] \subseteq \mathbb{Q}$ be an interval of $\mathbb{Q}$. Then a subset $D \subseteq X$ is **dense** in X if for every open interval $(c, d) \subseteq X$ with $c < d$ there exists $x \in D$ with $x \in (c, d)$.

We are now in a position to show that the non-trivial congruence classes of a $\triangleright$-congruence on the averaging quandle are dense in the averaging quandle. First, we will show that the congruence class is dense in the interval $[a, b]$ for any two elements with $a < b$ in a congruence class. Then we will show that the density extends over all of $\mathbb{Q}$.

Lemma 5.1.6. *Let Q_A be the averaging quandle on $\mathbb{Q}$, $\sim$ a $\triangleright$-congruence, $[\alpha]$ a congruence class of Q_A and $a, b \in [\alpha] \subseteq Q_A$ with $a < b$. Then $[\alpha] \cap [a, b]$ is dense in $[a, b]$.*

Proof. Let c be an arbitrary value in $[a, b]$. For $[\alpha]$ to be dense in $[a, b]$ we require either $c \in [\alpha]$ or for there to be a sequence in $[\alpha]$ that has c as a limit point.

Therefore, if $c \in [\alpha]$ we are done. So we assume $c \notin [\alpha]$. Now $a < c < b$. We will construct two sequences $\langle a_i \rangle$ and $\langle b_i \rangle$ such that for all $i \in \mathbb{Z}^*$, $a_i < c < b_i$ and $b_i - a_i = \frac{(b-a)}{2^i} \to 0$ as $i \to \infty$. Then c will be the limit point of both $\langle a_i \rangle$ and $\langle b_i \rangle$.

Lemma 5.1.2 guarantees that if $x, y \in [\alpha]$ then $x \triangleright y = \frac{x+y}{2} \in [\alpha]$. We begin with $a_0 = a$ and $b_0 = b$. Then inductively compare c with $a_i \triangleright b_i$ which is the midpoint of a_i and b_i. If $c < a_i \triangleright b_i$ then we set $a_{i+1} = a_i$ and $b_{i+1} = a_i \triangleright b_i$, and if $c > a_i \triangleright b_i$ then we set $a_{i+1} = a_i \triangleright b_i$ and $b_{i+1} = b_i$.

Then for all $i \in \mathbb{Z}^*$ we have $a_i < c < b_i$ and $b_i - a_i < \frac{b-a}{2^i}$ as required. Therefore c is the limit point of both $\langle a_i \rangle$ and $\langle b_i \rangle$ and $[\alpha]$ is dense in $[a, b]$. $\square$

We can extend the congruence class beyond the interval $[a, b]$ by showing that $b + (b - a)$ and $a - (b - a)$ are in the congruence class that contains a and b. Moreover these extensions can be repeated inductively and indefinitely in both directions.

Lemma 5.1.7. *Let* Q_A *be the averaging quandle on* $\mathbb{Q}$, $\sim$ *a* $\triangleright$*-congruence,* $[\alpha]$ *a congruence class of* Q_A *and* $a \in [\alpha]$ *and* $b \in [\alpha]$, *with* $a < b$. *Then*

$$(2b - a) = b + (b - a) = a + 2(b - a) \in [\alpha]$$

and similarly

$$a - (b - a) \in [\alpha].$$

Proof. We have $a \sim b$ and we apply the congruence condition with $x = 2b-a$ in equation (5.1.2). This gives

$$b = \frac{a + (2b - a)}{2} \sim \frac{b + (2b - a)}{2} = b + \frac{b - a}{2}.$$

This extends the region by half a step of size $(b-a)$. We repeat the procedure with $x = 3b - 2a$ to get

$$b + \frac{b - a}{2} = \frac{a + (3b - 2a)}{2} \sim \frac{b + (3b - 2a)}{2} = b + (b - a).$$

In combination these two half steps extend the region to the right by one interval of length $(b - a)$. By similar substitutions $x = 2a - b$ followed by $x = 3a - 2b$ we can extend the region to the left. We get respectively

$$a - \frac{b - a}{2} = \frac{a + (2a - b)}{2} \sim \frac{b + (2a - b)}{2} = a$$

and then from the second iteration

$$a - (b - a) = \frac{a + (3a - 2b)}{2} \sim \frac{b + (3a - 2b)}{2} = a - \frac{b - a}{2}.$$

$\square$

Remark 5.1.8. This process can be continued indefinitely in both directions thus by applying Lemma 5.1.6 to each new interval the see that any non-trivial congruence class of a $\triangleright$-congruence is a set that is dense over the entire rational number line $\mathbb{Q}$. Lemma 5.1.6 showed that the elements of a congruence class in the interval between any two distinct elements in the congruence class is a dense set. We can now extend beyond the two elements in both directions indefinitely with contiguous subsets of the congruence class that are dense thus our congruence class is a set that is dense in the rational numbers, $\mathbb{Q}$.

Remark 5.1.9. Thus any congruence class of a $\triangleright$-congruence with two distinct elements is necessarily a set that is an infinite subset of the rational numbers that is dense in $\mathbb{Q}$. The only other possible congruence classes of a $\triangleright$-congruence are sets containing only one element. In fact, we will see as a result of Corollary 5.1.12 that if any one congruence class is not a singleton then every congruence class is not a singleton. Therefore, conversely, if any congruence class of a $\triangleright$-congruence is a singleton every congruence class must be a singleton. That is, every congruence class, excepting the trivial case, in which every congruence class is a singleton, has the dense structure that we have described.

5.1.3 Differences in congruence classes

Armed with the lemmas in the previous section, we can now show that the set of all differences within a congruence class of a $\triangleright$-congruence must be a subgroup of $\mathbb{Q}$. It turns out that the set of differences within a congruence class is the same for all congruences classes of a $\triangleright$-congruence. We will see that the class $[0]$ is comprised of all of these differences in its own congruence class and so is a subgroup of $\mathbb{Q}$. Therefore all congruence classes are cosets of the class $[0]$, which is a subgroup of $\mathbb{Q}$.

We begin by defining the set of differences, D, in which every element, d, is the difference between two related elements. The set D is the set of all such elements:

$$D = \{x - y = d : x \sim y \text{ and } x, y \in Q_A\}.$$

Similarly, we define, the superficially more restricted sets of differences D_x, where each element, $d_x \in D_x$, is a difference from a particular element, x, and some other element related to x. The set D_x is the set of all such differences:

$$D_x = \{y - x = d_x : x \sim y\}.$$

Note, it is obvious that:

$$D = \bigcup_{x \in Q_A} D_x.$$

As foreshadowed above, it turns out that we can show that $D_x = D$ for all $x \in Q_A$.

In particular, it turns out to be easy to show that for any difference, $d \in D$, that $a \sim a + d$ for all $a \in Q_A$. We do this by first showing that for all $a \in Q_A$ if $a \sim a + d$ so that $d \in D$ then $\frac{d}{2} \in D$. That is, D is closed under multiplication by $\frac{1}{2}$.

Lemma 5.1.10. *Let Q_A be the averaging quandle on $\mathbb{Q}$, and let $\sim$ be a $\triangleright$-congruence, with a set of differences D in its congruence classes. Whenever $x \sim x + d$ for some $x \in Q_A$ then for all $a \in Q_A$ we have $a \sim a + \frac{d}{2}$.*

Proof. Given $d \in D$ there exist $x, y \in Q_A$ with $x \sim y$ and $y - x = d$. Therefore $x \sim x + d$. For any $a \in Q_A$ then

$$(2a - x) \triangleright x = \frac{2a - x + x}{2} = a.$$

Similarly,

$$(2a - x) \triangleright (x + d) = \frac{2a - x + x + d}{2} = a + \frac{d}{2}.$$

Therefore, since $x \sim x + d$ we have $a \sim a + \frac{d}{2}$. □

Corollary 5.1.11. *Let Q_A be the averaging quandle on $\mathbb{Q}$, and let $\sim$ be a $\triangleright$-congruence, with a set of differences D in its congruence classes. Then the set of differences D is closed under multiplication by $\frac{1}{2}$. That is, whenever $d \in D$ we have $\frac{d}{2} \in D$. Moreover, for all $a \in Q_A$, $\frac{d}{2} \in D_a$.*

Proof. For all $d \in D$ we have for some $x \in Q_A$, $x \sim x + d$ and therefore by Lemma 5.1.10 we have $a \sim a + \frac{d}{2}$ for all $a \in Q_A$ therefore $\frac{d}{2} \in D_a \subseteq D$ and D is closed under multiplication by $\frac{1}{2}$. □

The result of Lemma 5.1.10 can be extended to show that $a \sim a + d$ for all $a \in Q_A$ by applying the result to $a = a + \frac{d}{2}$. So we have that if d is any difference in a $\triangleright$-congruence then $a \sim a + d$ for all $a \in Q_A$. That means that all difference sets, D_x, are identical.

Corollary 5.1.12. *Let Q_A be the averaging quandle on $\mathbb{Q}$, and let $\sim$ be a $\triangleright$-congruence, with a set of differences D in its congruence classes. Then for any $d \in D$, $a \sim a + d$ for all $a \in Q_A$.*

Proof. From Lemma 5.1.10 we have that $a \sim a + \frac{d}{2}$ for all $a \in Q_A$. Applying that Lemma to $a + \frac{d}{2}$ we get $a + \frac{d}{2} \sim \left(a + \frac{d}{2}\right) + \frac{d}{2} = a + d$. Therefore, by transitivity we have $a \sim a + d$. $\square$

We are now in a position to state that in a $\triangleright$-congruence the set of differences are common in every congruence class. Moreover, the set of differences is therefore equal to the class of 0, [0].

Theorem 5.1.13. *For all $x \in Q_A$, the set of differences $D_x = D = [0]$.*

Proof. Apply Corollary 5.1.12 with $a = x$ to any difference $d \in D$. Then $x \sim x + d$ therefore $d \in D_x$. Obviously we also have for all $d_x \in D_x$, $d_x \in D$ since $D = \bigcup_{x \in Q_A} D_x$. Therefore $D = D_x$ for all $x \in Q_A$.

Similarly, for all $d \in D$, by Corollary 5.1.12 we have $0 \sim 0 + d = d$ and therefore $d \in [0]$. Conversely, for any $d \in [0]$ we have $d - 0 = d \in D_0 = D$ since we just showed that $D_x = D$ for all $x \in Q_A$. $\square$

We are now in a position to show that the set of differences D is a subgroup of $\mathbb{Q}$.

Theorem 5.1.14. *Let Q_A be the averaging quandle on $\mathbb{Q}$, and let $\sim$ be a $\triangleright$-congruence with a set of differences $D = \{x - y : x \sim y\}$. The set of differences, D, in the congruence classes of a $\triangleright$-congruence in the averaging quandle on $\mathbb{Q}$ is a subgroup of $\mathbb{Q}$.*

Proof. We prove that the set of differences is a subgroup directly. Suppose $u, v \in D$ then since $a \sim a+u$ and $a \sim a+v$ for all $a \in Q_A$ then $a+u \sim a+v$ and therefore $a + u - (a + v) = u - v \in D$. Therefore D is a subgroup of $\mathbb{Q}$. □

Theorem 5.1.15. *Let $\sim$ be a $\triangleright$-congruence on the averaging quandle on $\mathbb{Q}$. Then:*

1. *The congruence class $[0]$, is a subgroup of $\mathbb{Q}$.*
2. *All congruence classes are cosets of the zero class. That is, the congruence classes look like $[q] = q + [0]$, where $q \in \mathbb{Q}$ is any rational number, and the elements of $[q]$ are $q + d$, where $d \in [0]$.*

Proof. We consider the two claims.

1. Theorem 5.1.13 showed that $D = [0]$ and Theorem 5.1.14 showed that D is a subgroup of $\mathbb{Q}$ and therefore $[0] = D$ is a subgroup of $\mathbb{Q}$.

2. From any congruence class $[x]$, choose any $x' \in [x]$. Then since $x' \sim x$ we have $d = x' - x \in D = [0]$. Hence $x' = x + d \in x + [0]$.

$\square$

We are now in a position to show both that:

1. If $\sim$ is a $\triangleright$-congruence then the set of differences $D = \{x - y : x \sim y\}$ is a subgroup of $\mathbb{Q}$ that is closed under multiplication by $\frac{1}{2}$; and
2. If D is a subgroup of $\mathbb{Q}$ that is closed under multiplication by $\frac{1}{2}$ then the equivalence relation $\sim$ where $x \sim y$ if and only if $x - y \in D$ is a $\triangleright$-congruence.

We combine those results into a theorem.

Theorem 5.1.16. *Let Q_A be the averaging quandle.*

1. *Let $\sim$ be a $\triangleright$-congruence and let $D = \{x - y : x \sim y\}$ be the set of differences. Then D is a subgroup of $\mathbb{Q}$ that is closed under multiplication by $\frac{1}{2}$.*
2. *Let D be a subgroup of $\mathbb{Q}$ that is closed under multiplication by $\frac{1}{2}$ and define $\sim$ on Q_A such that $x \sim y$ if and only if $x - y \in D$. Then $\sim$ is a $\triangleright$-congruence.*

Proof. First assume that Q_A and that $\sim$ is a $\triangleright$-congruence. Define $D = \{x - y : x \sim y, x, y \in Q_A\}$. Then from Corollary 5.1.11, D is closed under multiplication by $\frac{1}{2}$, and by Theorem 5.1.14, D is a subgroup of $\mathbb{Q}$.

Conversely, let D be a subgroup of $\mathbb{Q}$ that is closed under multiplication by $\frac{1}{2}$. Define an equivalence relation, $\sim$, on Q_A by $x \sim y$ if and only if $x - y = d \in D$.

Now let $w, x, y, z \in Q_A$ with $x \sim w$ and $y \sim z$ so that we have $w - x = d_1$ and $z - y = d_2$ with $d_1, d_2 \in D$. Then consider

$$w \triangleright z = (x + d_1) \triangleright (y + d_2) = x \triangleright y + d_1 \triangleright d_2 = x \triangleright y + \left(\frac{d_1}{2} + \frac{d_2}{2}\right).$$

Since, D is a subgroup that is closed under multiplication by $\frac{1}{2}$ we have $\left(\frac{d_1}{2} + \frac{d_2}{2}\right) \in D$ and so $x \triangleright y \sim x \triangleright y + \left(\frac{d_1}{2} + \frac{d_2}{2}\right) = w \triangleright z$. Therefore $\sim$ is a $\triangleright$-congruence on Q_A. □

5.1.4 $\triangleright$-congruences imply quandle congruences

Now we can prove that a $\triangleright$-congruence on the averaging quandle on $\mathbb{Q}$ is a quandle congruence. That is, a $\triangleright$-congruence implies the congruence condition on the inverse operation. So whenever we have a $\triangleright$-congruence we are guaranteed to have both a $\triangleright$-congruence and a $\triangleleft$-congruence.

Theorem 5.1.17. *For the averaging quandle on $\mathbb{Q}$, Q_A, any $\triangleright$-congruence is a quandle congruence. That is, if $\sim$ is a $\triangleright$-congruence and for all $a, b, c, d \in Q_A$ if $a \sim b$ and $c \sim d$ then*

$$a \triangleleft c \sim b \triangleleft d.$$

Proof. Let $\sim$ be a $\triangleright$-congruence on the averaging quandle on $\mathbb{Q}$. Then for

$a, b, c, d \in Q_A$ and $a \sim b$ and $c \sim d$ we can write $b = a + s$ and $d = c + s'$ with $s, s' \in [0]$. Recall that $x \triangleleft y = 2x - y$. Now

$$\begin{aligned} b \triangleleft d &= 2(a+s) - (c+s') \\ &= (2a - c) + (2s - s') \\ &= a \triangleleft c + (2s - s') \\ &\sim a \triangleleft c, \end{aligned}$$

since we have $2s - s' \in [0]$ as a consequence of $[0]$ being a subgroup of $\mathbb{Q}$.

Thus $a \sim b$ and $c \sim d$ implies $a \triangleleft c \sim b \triangleleft d$ and therefore any $\triangleright$-congruence on the averaging quandle on $\mathbb{Q}$ is a $\triangleleft$-congruence and hence is a quandle congruence. $\square$

5.1.5 $\triangleleft$-congruences do not imply quandle congruences

Curiously, while in some sense $(Q, \triangleright, \triangleleft)$ is the same quandle as $(Q, \triangleleft, \triangleright)$ — they have the same set and the same two quandle operations and we are just viewing the primary quandle operation in either of these quandles as the inverse quandle operation in the other quandle and vice versa (recall by definition we call these dual quandles) — although we have shown that a congruence on the primary quandle operation in the averaging quandle implies a congruence condition on the inverse quandle operation, that does not apply in reverse. That is, a $\triangleright$-congruence in the averaging quandle implies a quandle congruence but that does not hold in the dual quandle of the averaging quandle which has the same set and the same two quandle operations.

We will show that with a counterexample.

Theorem 5.1.18. *For the averaging quandle a* $\triangleleft$*-congruence on the inverse quandle operation,* $x \triangleleft y = 2x - y$*, does not imply a quandle congruence.*

Proof. We construct a counterexample as follows.

Example 5.1.19. We start with the averaging quandle over $\mathbb{Q}$ and work with the inverse quandle operation. Let $D = \{\frac{n}{3}, \text{ for } n \in \mathbb{Z}\}$ and define a relation by $x \sim y$ if and only if $y - x \in D$. It is easy to see that this is an equivalence relation:

1. Reflexive: Since $0 = \frac{0}{3} \in D$ and $x - x = 0 \in D$ then $x \sim x$.

2. Symmetric: If $x \sim y$ then $y - x = \frac{n}{3}$ for some $n \in \mathbb{Z}$. Therefore $x - y = \frac{-n}{3} \in D$, since $-n \in \mathbb{Z}$ hence $y \sim x$.

3. Transitive: If $x \sim y$ then $y - x = \frac{n}{3}$, for some $n \in \mathbb{Z}$, and if $y \sim z$ then $z - y = \frac{m}{3}$, for some $m \in \mathbb{Z}$. Therefore

$$z - x = (y - x) + (z - y) = \frac{n}{3} + \frac{m}{3} = \frac{n+m}{3} \in D$$

since $m + n \in \mathbb{Z}$. Therefore $x \sim z$.

So $\sim$ is an equivalence relation. We can show $\sim$ is a $\triangleleft$-congruence by considering

$$\left(x + \frac{m}{3}\right) \triangleleft \left(y + \frac{n}{3}\right) = x \triangleleft y + \frac{m}{3} \triangleleft \frac{n}{3} = x \triangleleft y + 2\frac{m}{3} - \frac{n}{3} = x \triangleleft y + \frac{2m - n}{3}.$$

Since, for all $m, n \in \mathbb{Z}$, it is true that $2m - n \in \mathbb{Z}$ we have $\frac{2m-n}{3} \in D$ and therefore $x \lhd y \sim (x + \frac{m}{3}) \lhd (y + \frac{n}{3})$ as required and so $\sim$ is a $\lhd$-congruence.

However we cannot make the same deduction about the primary quandle operation in the averaging quandle, since

$$(x + \frac{m}{3}) \rhd (y + \frac{n}{3}) = x \rhd y + \frac{\frac{m+n}{3}}{2} = x \rhd y + \frac{m+n}{6}.$$

We need $\frac{m+n}{6} \in D$ for all $m, n \in \mathbb{Z}$. This is clearly not true. For example take $m = 1$ and $n = 0$ and we have $\frac{1}{6} \neq \frac{k}{3}$ for any $k \in \mathbb{Z}$. Alternatively, D isn't closed under multiplication by $\frac{1}{2}$.

Therefore for the averaging quandle a $\lhd$-congruence does not imply a $\rhd$-congruence. $\square$

This is an interesting property that we will see more of in the next section. We have, in the averaging quandle, an example of a quandle which has the property that every $\rhd$-congruence is a quandle congruence but the related dual-quandle does not have that property or alternatively in the averaging quandle there are $\lhd$-congruences that are not quandle congruences. In other words, in the averaging quandle every $\rhd$-congruence implies that we have a quandle congruence but a $\lhd$-congruence may be a half congruence.

This behaviour will be more fully described in Section 5.2, where we generalise Theorem 5.1.16 to see that a $\rhd$-congruence in a weighted average quandle with operation $x \rhd y = tx + (1-t)y$ corresponds to a choice of subgroup D of $\mathbb{Q}$ that is closed under multiplication by t. In fact, we prove a stronger result in Lemma 5.2.12 that, any $\triangleright$-congruence corresponds with a subgroup $D \subseteq \mathbb{Q}$ that is closed under multiplication by $\frac{1}{q}$ where $t = \frac{p}{q}$ with p and q relatively prime. For now, we can note that since the inverse quandle operation in the averaging quandle is $x \triangleleft y = 2x - y$, we require a subgroup that is closed under multiplication by 2, which is the multiplicative inverse of $\frac{1}{2}$, in order to have a $\triangleleft$-congruence. In order to have both a $\triangleright$-congruence and a $\triangleleft$-congruence we will see that we need a subgroup that is closed under multiplication by both $\frac{1}{2}$ and 2. Clearly, subgroups that are closed under multiplication by $\frac{1}{2}$ are necessarily closed under multiplication by 2 but the converse is not true. That explains why there exist $\triangleleft$-congruences that are not $\triangleright$-congruences, and why all $\triangleright$-congruences are $\triangleleft$-congruences in the averaging quandle, Q_A.

5.2 Weighted average quandles on $\mathbb{Q}$

5.2.1 Definition

The averaging quandle can be generalised by using a weighted average, rather than the arithmetic mean, as the quandle operation. A standard calculation of a weighted average with weight t is used. We introduced the weighted average quandle in Example 2.2.29. We repeat the definition of that example here to formally define a weighted average quandle.

Definition 5.2.1. A *weighted average quandle* on $\mathbb{Q}$ is a quandle with the quandle operation defined by

$$x \triangleright y = tx + (1-t)y$$

where $t \in \mathbb{Q} \setminus \{0\}$. We will write A_t for the weighted average quandle with weight t.

The averaging quandle in Section 5.1 is a weighted average quandle with $t = \frac{1}{2}$. In some contexts a weighted average would require $0 < t < 1$ or perhaps $0 \leq t \leq 1$ however, it is not necessary to impose such a restriction in this generalisation. Moreover, it is convenient to not do so as then, for example, the inverse quandle operation on the averaging quandle with weight $t = \frac{1}{2}$ can be viewed as a weighted average with weight $t = 2 = \left(\frac{1}{2}\right)^{-1}$. More generally, we showed in Example 2.2.29 that the inverse quandle operation for a weighted average quandle with weight t is a weighted average with weight t^{-1}.

The weighted average quandle is an Alexander quandle and so is a quandle. The quandle operation, $x \triangleright y = tx+(1-t)y$, t is defined by $t \in \mathbb{Q} \setminus \{0\}$ acting on $\mathbb{Q}$ by multiplication. We previously showed in Corollary 2.2.23 that the inverse operation in an Alexander quandle is

$$x \triangleleft y = t^{-1}x + (1-t^{-1})y.$$

That can be applied here to the weighted average quandle where $t \in \mathbb{Q} \setminus \{0\}$ and acts on the rational numbers by multiplication.

While it is convenient to extend the weights beyond the usual range $0 < t \leq 1$, it is necessary to exclude the weight $t = 0$ since in that case we do not have a quandle. In particular, the invertibility axiom does not hold for $t = 0$. That is, since $x \triangleright y = 0 \times x + y = y$ for all $x, y \in \mathbb{Q}$ the equation $x \triangleright y = z$ has no solution for $y \neq z$ and infinitely many solutions, any $q \in \mathbb{Q}$, when $y = z$. However, the quandle axioms require a unique solution.

In addition, when $t = 1$ the quandle operation collapses to $x \triangleright y = x + (1 - 1)y = x$ and we have the trivial quandle. The trivial quandle case often can be treated separately and so in what follows we will often only be dealing with $t \in \mathbb{Q} \setminus \{0, 1\}$.

5.2.2 Structure of congruence classes

In the case of the averaging quandle, where $t = \frac{1}{2}$, we saw that congruence classes were dense subsets of $\mathbb{Q}$. We also saw that the congruence class of zero was a subgroup of $\mathbb{Q}$ that was closed under halving. The latter result generalises to the weighted average quandle. Whilst the former has a limited generalisation. The congruence classes are dense sets provided the weight, t, is not an integer.

When $a \sim b$, the relationship expressed in equation (5.1.2),

$$\frac{a+x}{2} \sim \frac{b+x}{2},$$

has an analogous generalisation in the weighted average quandle. That is, for $a, b \in A_t$ and $a \sim b$ then for all $x \in A_t$ we have, since $a \rhd x \sim b \rhd x$:

$$ta + (1-t)x \sim tb + (1-t)x. \tag{5.2.1}$$

By putting $x = a$ we obtain

$$a \sim a + t(b-a). \tag{5.2.2}$$

For $0 < t < 1$, the right hand side of equation (5.2.2) is a value in the closed interval $[a, b]$. As for the averaging quandle, this process can be repeated indefinitely to fill out the interval $[a, b]$ with a dense set. This is analogous to the result in Lemma 5.1.6.

Lemma 5.2.2. *Let A_t be the weighted average quandle with a weight in the range $0 < t < 1$, $\sim$ a $\rhd$-congruence on A_t, $[\alpha]$ a congruence class and $a, b \in [\alpha] \subseteq A_t$ with $a < b$. Then $[\alpha] \subseteq \mathbb{Q}$ is dense in $[a, b]$.*

Remark 5.2.3. To prove Lemma 5.2.2 we will mimic the proof in the averaging case. The proof in the averaging case was a little more straightforward. This was because, implicitly, the proof exploited the symmetry of the weight $t = \frac{1}{2}$, that is, $t = 1 - t$. Given $c \in [a, b]$ with $c \notin [\alpha]$ we will construct sequences $\langle a_k \rangle$, $\langle b_k \rangle$ such that $a_k, b_k \in [\alpha]$, $a_k < c < b_k$, and $b_k - a_k \to 0$ as $k \to \infty$. At each step the new points a_k, b_k are found by subdividing the current interval $[a_k, b_k]$ into two subintervals, and choosing whichever c belongs to.

For $t = \frac{1}{2}$ these two subintervals have the same length, due to the symmetry of the weight $t = \frac{1}{2}$, that is $t = 1 - t$. Thus $b_{k+1} - a_{k+1} = \frac{b_k - a_k}{2}$ for all k. However in the general case with $0 < t < 1$ the intervals are asymmetric, with lengths in the ratio $t : (1-t)$, so we have either $b_{k+1} - a_{k+1} = t(b_k - a_k)$ or $b_{k+1} - a_{k+1} = (1-t)(b_k - a_k)$. To account for the asymmetry we will let $\lambda = \max\{t, 1-t\} < 1$, so that we get $b_{k+1} - a_{k+1} \leq \lambda(b_k - a_k)$ for all k.

Proof. Let c be an arbitrary value in $[a, b]$. For $[\alpha]$ to be dense in $[a, b]$ we require either $c \in [\alpha]$ or for there to be a sequence in $[\alpha]$ that has c as a limit point.

Therefore, if $c \in [\alpha]$ then we are done. So, we assume $c \notin [\alpha]$. Let $\lambda = \max\{t, 1-t\}$ and note that $0 < \lambda < 1$. We will construct sequences $\langle a_k \rangle$ and $\langle b_k \rangle$ such that $a_k < c < b_k$ and $b_k - a_k \leq \lambda^k(b-a) \to 0$ as $k \to \infty$. Before we begin the construction, note that since $0 < \lambda < 1$ and $b - a$ is finite therefore $\lambda^k(b-a) \to 0$ as $k \to \infty$.

Let $a_0 = a$ and $b_0 = b$ and so we have $a_0 < c < b_0$ with

$$b_0 - a_0 = b - a = \lambda^0(b-a).$$

Assume $a_k < c < b_k$ with $a_k, b_k \in [\alpha]$ and $b_k - a_k \leq \lambda^k(b-a)$. We can inductively construct a_{k+1} and b_{k+1} by considering

$$a_k \triangleright b_k = ta_k + (1-t)b_k = a + (1-t)(b-a) \in [\alpha]$$

and noting that $a_k \triangleright b_k$ lies between a_k and b_k since $0 < 1 - t < 1$. We now consider two exhaustive possibilities. Either

1. If $a_k < c < a_k \triangleright b_k$ then we set $a_{k+1} = a_k$ and $b_{k+1} = a_k \triangleright b_k$;
2. If $a_k \triangleright b_k < c < b_k$ then we set $a_{k+1} = a_k \triangleright b_k$ and $b_{k+1} = b_k$.

Also note that $a_k \triangleright b_k - a_k = (1-t)(b_k - a_k)$ and $b_k - a_k \triangleright b_k = t(b_k - a_k)$ so

$$b_{k+1} - a_{k+1} \leq \max\{t, 1-t\}(b_k - a_k) = \lambda(b_k - a_k).$$

Therefore

$$b_{k+1} - a_{k+1} \leq \lambda(b_k - a_k) \leq \lambda\lambda^k(b - a) = \lambda^{k+1}(b - a).$$

Since c is sandwiched between a_k and b_k and $b_k - a_k \to 0$ as $k \to \infty$ we have c is a limit point of both $\langle a_k \rangle$ and $\langle b_k \rangle$ with both $a_k \in [\alpha]$ and $b_k \in [\alpha]$ for all $k \in \mathbb{N}$ as required. Therefore $[\alpha]$ is dense in $[a, b]$. □

Just as in the case of the averaging quandle the congruence class extends indefintely in both directions. We can extend the congruence classes indefinitely as the result of an analogous result to that in Lemma 5.1.7. Again, here in the weighted average quandle, we have to work a little harder to prove this result than we did in the analagous result for the averaging quandle. The proof depends on the invertibility of both t and $(1 - t)$ which is obviously no problem when t is any value other than 0 or 1, which we have excluded as for $t = 0$ we do not have a quandle and for $t = 1$ we have the trivial quandle. It will become a problem later when we try to extend the results in this chapter to more general Alexander quandles in which the action of $1 - t$ is not necessarily invertible.

Lemma 5.2.4. *Let A_t be a weighted average quandle with weight t, $\sim$ a $\triangleright$-congruence, $[\alpha]$ a congruence class, $a, b \in [\alpha]$ with $a < b$. Then $(2b - a) = b + (b - a) \in [\alpha]$. Similarly $a - (b - a) \in [\alpha]$.*

Remark 5.2.5. Note for this lemma we do not need $0 < t < 1$. The congruence class extends irrespective of the value of $t \in \mathbb{Q} \setminus \{0, 1\}$. However we will be using this lemma here to extend the result in Lemma 5.2.2 to a congruence class being a dense set in $\mathbb{Q}$ for $0 < t < 1$. Later we will extend Lemma 5.2.2 for other values of t by other methods.

Proof. Let $x = \frac{b-ta}{1-t}$ then

$$a \triangleright x = a \triangleright \frac{b - ta}{1 - t} = b$$

and

$$b \triangleright \frac{b - ta}{1 - t} = b + t(b - a).$$

Since $a \sim b$ therefore $b \sim b + t(b - a)$.

Similarly, let $x = \frac{b-a+tb}{t}$ then

$$x \triangleright a = \frac{b - a + tb}{t} \triangleright a = b + t(b - a)$$

and

$$\frac{b - a + tb}{t} \triangleright b = 2b - a = b + (b - a).$$

Again, since $a \sim b$ we have established that $b \sim b + t(b - a) \sim b + (b - a)$. Therefore since $a \sim b$ and $b \sim b + t(b - a)$ and $b + t(b - a) \sim b + (b - a)$ we have $a \sim b + (b - a) \in [\alpha]$.

By swapping the roles of a and b, we can similarly establish that $b \sim a + (a - b) = a - (b - a)$. Thus we have extended the congruence classes by an interval of length $b - a$ in each direction.[1] $\square$

Remark 5.2.6. As in the averaging quandle, by repeated applications of Lemma 5.2.4, these augmentations to the interval between any two elements in congruence classes can be extended indefinitely in both directions. Moreover, for $0 < t < 1$, on each of the closed intervals

$$\cdots [a - (b - a), a], [a, b], [b, b + (b - a)], \cdots$$

we can apply Lemma 5.2.2 to show that the closed interval contains a dense subset of the congruence class to which a and b belong. Therefore any congruence class with at least two distinct elements and a weight $0 < t < 1$ is a dense subset of $\mathbb{Q}$. However, as we will see we can do better.

5.2.3 Differences in congruence classes

When we examine the congruence classes it is useful to consider the set of the differences between an element and the elements in its congruence class, D_x, which we will define as $D_x = \{y - x : y \in [x]\}$. It turns out that D_x is the same for every x, that is, it is independent of x. We begin to show

---

[1] The value $x = \frac{b-ta}{1-t}$, in this proof, comes from solving the equation $a \triangleright x = b$. That equation is solvable in a weighted average quandle since $1 - t$ is invertible. Similarly, the value $x = \frac{b-a+tb}{t}$ comes from solving the equation $x \triangleright a = b$. That equation is necessarily solvable by the invertibility axiom.

this by showing that for any difference, d, in a set of differences, D_x, that $a \sim a + d$ for all $a \in A_t$, a weighted average quandle.

Lemma 5.2.7. *Let A_t be a weighted average quandle, with $t \in \mathbb{Q} \setminus \{0, 1\}$, $\sim$ a $\triangleright$-congruence, $[\alpha]$ a congruence class with $y, y + d \in [\alpha]$. Then $a \sim a + d$ for all $a \in A_t$.*

Proof. For all $a \in A_t$ we can solve the equation

$$\begin{aligned} & x \triangleright y = a \\ \Rightarrow \quad & tx + (1 - t)y = a \\ \Rightarrow \quad & x = \frac{a - (1 - t)y}{t}. \end{aligned}$$

Now we calculate

$$\frac{a - (1 - t)y}{t} \triangleright (y + d) = a + (1 - t)d.$$

Therefore

$$a \sim a + (1 - t)d$$

for all $a \in A_t$.

Similarly for all $a \in A_t$ we can solve the equation

$$\begin{aligned} & y \triangleright x = a \\ \Rightarrow \quad & ty + (1 - t)x = a \\ \Rightarrow \quad & x = \frac{a - ty}{1 - t}. \end{aligned}$$

Note, the existence of a solution, x, of the equation $y \triangleright x = a$, is a special feature of the weighted average quandle and is not, in general, a requirement of a quandle — not all quandles have both left and right invertibility. In particular, the solution is not valid for the trivial quandle, which would be represented here by a weight of $t = 1$, hence that value is excluded in the statement of the lemma.

Now we calculate

$$(y + d) \triangleright \frac{a - ty}{1 - t} = a + td.$$

Therefore $a \sim a + td$ for all $a \in A_t$. Moreover, since for all a, $a \sim a + (1 - t)d$ we can apply this relationship to $a + (1 - t)d$ to see that

$$a \sim a + (1 - t)d \sim a + (1 - t)d + td = a + d$$

for all $a \in A_t$ as required. $\square$

Given that we have shown that every difference d between any two related elements implies that every element, $a \in A_t$, is related to $a + d$ we have that the sets of differences, D_x and D are equal. Moreover those sets of differences are precisely the congruence class of the zero element.

Theorem 5.2.8. *Let A_t be a weighted average quandle with weight $t \neq 1$ and $\sim$ a $\triangleright$-congruence. Let $D_x = \{y - x, y \in [x]\}$ and $D = \{x - y : x \sim y; x, y \in A_t\}$. Then $D_x = D = [0]$ for all $x \in A_t$.*

The proof of the corresponding result Theorem 5.1.13 for $t = \frac{1}{2}$ was independent of t, and Theorem 5.2.8 follows by the same argument, using Lemma 5.2.7 in place of Corollary 5.1.12. We therefore omit repeating the proof here. After which, the analogy of Theorems 5.1.14 and 5.1.15, also independent of t, follow in a similar manner. The equivalent results are stated here without proof.

Theorem 5.2.9. *The set of differences in a congruence class of any weighted average quandle on* $\mathbb{Q}$ *with weight* $t \notin \{0, 1\}$ *is a subgroup of* $\mathbb{Q}$.

Theorem 5.2.10. *Let* $\sim$ *be a* $\triangleright$*-congruence on a weighted average quandle on* $\mathbb{Q}$*. Then:*

1. *The congruence class* $[0]$*, is a subgroup of* $\mathbb{Q}$.
2. *All congruence classes are cosets of the zero class. That is, the congruence classes look like* $[q] = q + [0]$*, where* $q \in \mathbb{Q}$ *is any rational number, and the elements of* $[q]$ *are* $q + d$*, where* $d \in [0]$.

We saw in the proof of Lemma 5.2.7 that whenever $d \in D = [0]$ we have $td \in D$. This means that a set of differences is closed under multiplication by t. In fact, it is true that the set of differences can be used to determine a congruence on a weighted average quandle if and only if the set of differences is a subgroup that is closed under multiplication by the weight, t.

Lemma 5.2.11. *Let* A_t *be a weighted average quandle of* $\mathbb{Q}$ *with weight* $t \in \{0, 1\}$*. Let* $D \subseteq \mathbb{Q}$ *and define on* A_t $x \sim y$ *if and only if* $x - y \in D$*. Then* $\sim$ *is a* $\triangleright$*-congruence if and only if* D *is an additive subgroup closed under multiplication by* t.

Proof. If a set of differences defines a $\triangleright$-congruence then Theorem 5.2.9 shows that the set of differences is a subgroup of $\mathbb{Q}$. The congruence condition $a \triangleright c \sim b \triangleright d = (a+\delta) \triangleright (c+\delta')$ whenever $a \sim b = a + \delta$ and $c \sim d = c + \delta'$ gives us that

$$a \triangleright c \sim (a+\delta) \triangleright (c+\delta') = a \triangleright c + \delta \triangleright \delta' = a \triangleright c + t\delta + (1-t)\delta'.$$

Therefore $t\delta + (1-t)\delta' \in D$ for all $\delta, \delta' \in D$. In particular when $\delta' = 0$ we have $t\delta \in D$ for all $\delta \in D$. That shows that D is closed under multiplication by t.

On the other hand given a set, D, that is a subgroup that is closed under multiplication by t we define a relation, $\sim$, such that $a \sim b$ whenever $\delta = a - b \in D$. Now given $a, b \in A_t$ and $\delta, \delta' \in D$ we have

$$(a+\delta) \triangleright (b+\delta') = a \triangleright b + \delta \triangleright \delta' = a \triangleright b + t\delta + (1-t)\delta'.$$

We have that $t\delta + (1-t)\delta' \in D$ since D is a subgroup and $t\delta \in D$ and $(1-t)\delta' = \delta' - t\delta' \in D$. Therefore $a \triangleright b \sim (a+\delta) \sim (b+\delta')$ and so the relation is a $\triangleright$-congruence. $\square$

Moreover, it turns out that the subgroup, D, in Lemma 5.2.11 is closed under multiplication by $\frac{1}{q}$ where $t = \frac{p}{q}$ is a fraction in its simplest form, that is, with p and q relatively prime. We show this by showing that a subgroup closed under multiplication by $\frac{1}{q}$ is necessarily closed under multiplication by

$t = \frac{p}{q}$ and then by showing the converse based on Bézout's Lemma [3,5].[2]

Lemma 5.2.12. *Let A_t be a weighted average quandle with weight, $t \notin \{0, 1\}$ on $\mathbb{Q}$ with $t = \frac{p}{q}$ where $p, q \in \mathbb{Z}$ and $\gcd(p, q) = 1$. Given a subset D of $\mathbb{Q}$ define a relation $\sim$ on $\mathbb{Q}$ by $x \sim y$ if and only if $x - y \in D$. Then $\sim$ is a $\triangleright$-congruence if and only if D is a subgroup of $\mathbb{Q}$ that is closed under multiplication by $\frac{1}{q}$.*

Proof. If a subgroup is closed under multiplication by $\frac{1}{q}$ then whenever $d \in D$ we have $\frac{d}{q} \in D$ and therefore that

$$\frac{d}{q}, \frac{d}{q} + \frac{d}{q} = \frac{2d}{q}, \ldots, \frac{pd}{q} = td \in D.$$

Therefore the subgroup is closed under multiplication by t and by Lemma 5.2.11 we have a $\triangleright$-congruence.

On the other hand, also by Lemma 5.2.11, if we have a $\triangleright$-congruence then we have a subgroup that is closed under multiplication by $t = \frac{p}{q}$. Since p and q are relatively prime we have by Bézout's Lemma that there exist $m, n \in \mathbb{Z}$ such that

$$mp + nq = 1.$$

---

[2] Etienne Bézout published this well-known result in *Théorie générale des équations algébrique* in 1779. His result applied more generally to polynomials. One hundred and fifty five years earlier, in 1624 Claude Gaspar Bachet de Méziriac had stated and proved the theorem for integers in the second edition of *Problemes Plaisans Et delectables, qui se font par les nombres.*

Dividing by q and multiplying by any $d \in D$ we obtain

$$\frac{mpd}{q} + nd = m(td) + nd = \frac{1}{q}d.$$

Now since $d \in D$ and $td \in D$ then because D is a subgroup both $m(td) \in D$ and $nd \in D$ and therefore their sum $\frac{1}{q}d \in D$. Therefore D is closed under multiplication by $\frac{1}{q}$ as required. $\square$

We can use Lemma 5.2.12 to show that the non-trivial congruence classes are dense in $\mathbb{Q}$. For any open interval (u, v) we can choose k large enough so that, for some a, b in a congruence class, $\frac{b-a}{q^k} < v-u$. Then we can find $n \in \mathbb{Z}$ so that, for example, $a + n\frac{b-a}{q^k} \in (u, v)$. Since each non-trivial congruence class is a coset of $[0]$ it is sufficient to show that $D = [0]$ is dense. We will require $q > 1$. For $q = 1$ the congruence classes are not necessarily dense.

Theorem 5.2.13. *Let A_t be a weighted average quandle on $\mathbb{Q}$ with weight $\frac{p}{q} = t \in \mathbb{Q} \setminus \{0, 1\}$ with $\gcd(p, q) = 1$ and $q > 1$ and let $\sim$ be a non-trivial $\triangleright$-congruence. Then the congruence class $[0]$ is dense in $\mathbb{Q}$.*

Proof. For any $u, v \in \mathbb{Q}$ with $u < v$ we need to show that there exists $\alpha \sim 0$ with $\alpha \in (u, v)$. We have $d \neq 0$ with $d \in [0]$ since $\sim$ is a non-trivial congruence. From Lemma 5.2.12 we can construct, for all $n \in \mathbb{Z}$ and for any $k \in \mathbb{N}$, $n\frac{d}{q^k} \in [0]$. We can choose k so that $\frac{d}{q^k} < v - u$ which is possible since $q > 1$.

Now there must exist n^* such that

$$n^* \frac{d}{q^k} \in (u, v).$$

If not then there must exist n' such that

$$u > n' \frac{d}{q^k} = u - \delta_1 \text{ and } v < (n' + 1)\frac{d}{q^k} = v + \delta_2$$

with $\delta_1, \delta_2 \geq 0$ but then by subtracting we get

$$v - u + \delta_1 + \delta_2 = \frac{d}{q^k} \geq v - u$$

which contradicts our choice of k.

Therefore the congruence class $[0]$ of a non-trivial $\triangleright$-congruence is dense in $\mathbb{Q}$. □

Corollary 5.2.14. *Let A_t be a weighted average quandle on $\mathbb{Q}$ with weight $\frac{p}{q} = t \in \mathbb{Q} \setminus \{0, 1\}$ with $\gcd(p, q) = 1$ and $q > 1$ and let $\sim$ be a non-trivial $\triangleright$-congruence. Then the congruence classes for all $x \in A_t$, $[x]$ are dense in $\mathbb{Q}$.*

Proof. This follows from Theorem 5.2.13 and from Theorem 5.2.10 that showed that for all $x \in A_t$ the congruence class $[x] = x + [0]$ and so is a coset of $[0]$.

For any $u, v \in \mathbb{Q}$ with $u < v$ and for any $x \in A_t$ we need to show that there exists $\xi \in [x]$ with $\xi \in (u, v)$. Since $[x]$ is a coset of $[0]$ we have $[x] = x + [0]$. Therefore for any $\xi \in [x]$ there exists $\omega \in [0]$ such that $\xi = x + \omega$. We can apply the argument in Theorem 5.2.13 to show that there exists $\omega \in (u - x, v - x)$. Then $\xi = x + \omega \in (u, v)$ as required and so the non-trivial congruence classes of a $\triangleright$-congruence are dense in $\mathbb{Q}$. □

5.2.4 Integer weights

This leaves us with the weights $t \in \mathbb{Z} \setminus \{0, 1\}$ to be investigated. In these cases we can show that there exist congruence classes that are not dense sets. We will work with the set of differences $D = \{nq \text{ for all } n \in \mathbb{Z}\}$ for some $q \in \mathbb{Q}$ and show that this is a possible congruence class for $t \in \mathbb{Z}$ and that it can only be a congruence class if $t \in \mathbb{Z}$.

Lemma 5.2.15. *Let A_t be a weighted average quandle on $\mathbb{Q}$ with weight $t \in \mathbb{Z} \setminus \{0, 1\}$. For $q \in \mathbb{Q}$, $D = \{nq \text{ for all } n \in \mathbb{Z}\}$ define $x \sim y$ if and only if $x - y \in D$. Then $\sim$ is a $\triangleright$-congruence. Moreover, if q is non-zero, for $\sim$ to be a $\triangleright$-congruence it is both necessary and sufficient for $t \in \mathbb{Z}$.*

Proof. If $q = 0$ then since the differences are all zero the equivalence classes are all singletons and we have the trivial case. For the remainder of the proof therefore assume $q \neq 0$.

It is straightforward to show that $\sim$ is an equivalence relation.

1. Reflexive: Since $0 = 0q \in D$ then $x \sim x$.

2. Symmetric: If $x \sim y$ then $x - y = nq \in D$ therefore $y - x = (-n)q \in D$ and hence $y \sim x$.

3. Transitive: If $x \sim y$ then $x - y = n_1 q$ and if $y \sim z$ then $y - z = n_2 q$ therefore $x - z = (n_1 + n_2)q \in D$ and hence $x \sim z$.

Now consider $(x + n_1 q) \triangleright (y + n_2 q) = (x \triangleright y) + (n_1 q \triangleright n_2 q)$. For all $n_1, n_2 \in \mathbb{Z}$, we require $(n_1 q \triangleright n_2 q) = t n_1 q + (1-t) n_2 q = nq$ for some $n \in \mathbb{Z}$ in order for $\sim$ to be a $\triangleright$-congruence.

We need $t n_1 + (1-t) n_2 = n \in \mathbb{Z}$ for all integers n_1 and n_2. Putting $n_2 = 0$ we have $t n_1 \in \mathbb{Z}$ for all $n_1 \in \mathbb{Z}$. Suppose $n_1 = 1$ then we require $t \in \mathbb{Z}$, as stated in the lemma. So it is necessary that t be an integer.

On the other hand if $t \in \mathbb{Z}$ then $t n_1 q + (1-t) n_2 q = [t n_1 + (1-t) n_2]q = n'q$ since $n' = t n_1 + (1-t) n_2 \in \mathbb{Z}$. It is also sufficient that t be an integer. $\square$

5.2.5 Conclusion

We can now classify the behaviour of congruences based on the value of the parameter t in a weighted average congruence. If $t = \frac{p}{q}$ is a fraction in reduced form then according to Lemma 5.2.12 we have a $\triangleright$-congruence provided we have a difference set, D, that is, a subgroup closed under multiplication by $\frac{1}{q}$. Similarly, we will have a $\triangleleft$-congruence provided we have a difference set, D, that is a subgroup closed under multiplication by $\frac{1}{p}$. Therefore, we have quandle congruences if and only if the difference set, D, is closed under multiplication by both $\frac{1}{q}$ and $\frac{1}{p}$ that is, since p and q are relatively prime, the difference set must be closed under multiplication by $\frac{1}{pq}$.

The averaging quandle, where $t = \frac{1}{2}$ is an example of a special case, with $\frac{1}{t} \in \mathbb{Z}$. In those cases, $p = 1$ and therefore $\frac{1}{pq} = \frac{1}{q}$ and the condition for a quandle congruence is met whenever we have a $\triangleright$-congruence. However, it is easy to construct difference sets that are not closed under multiplication by $\frac{1}{pq} = \frac{1}{q} = t$. Therefore $\triangleleft$-congruences are not necessarily quandle congruences.

Similarly, in the case where $t \in \mathbb{Z}$ then $q = 1$ and it is straightforward to construct a $\triangleright$-congruence that is based on a subgroup that is not closed under multiplication by $\frac{1}{pq} = \frac{1}{p} = \frac{1}{t}$. Therefore a $\triangleright$-congruence does not imply a quandle congruence. However, in this case every $\triangleleft$-congruence is a quandle congruence.

In the more general case where $t = \frac{p}{q}$ with $p \neq 1$ and $q \neq 1$ we have a quandle congruence if and only if the difference set is closed under multiplication by $\frac{1}{pq}$. On the other hand if we have a difference set that is closed under multiplication by $\frac{1}{p}$ but not closed under multiplication by $\frac{1}{q}$ then we have $\triangleleft$-congruences that are not quandle congruences and conversely if we have a difference set that is closed under multiplication by $\frac{1}{q}$ but not closed under multiplication by $\frac{1}{p}$ then we have $\triangleright$-congruences that are not quandle congruences.

We put all of this together in the following theorem. The proof of the theorem is omitted as it is essentially a consolidation of the results proved in this chapter.

Theorem 5.2.16 (Weighted average quandle congruences). *Let* A_t *be a weighted average quandle with weight* $t = \frac{p}{q}$ *in reduced form. Let* $\sim$ *be a equivalence relation with an associated difference set* $D = \{x - y : x \sim y, x, y \in A_t\}$. *Then*

1. *We have a* $\triangleright$*-congruence if and only if* D *is closed under multiplication by* $\frac{1}{q}$.
2. *We have a* $\triangleleft$*-congruence if and only if* D *is closed under multiplication by* $\frac{1}{p}$.
3. *We have a quandle congruence if and only if* D *is closed under multiplication by* $\frac{1}{pq}$.

Consequently,

4. *If* $t \in \mathbb{Z} \setminus \{0, 1\}$ *then every* $\triangleleft$*-congruence is a* $\triangleright$*-congruence but it is not true that every* $\triangleright$*-congruence is a* $\triangleleft$*-congruence.*
5. *If* $\frac{1}{t} \in \mathbb{Z} \setminus \{0, 1\}$ *then every* $\triangleright$*-congruence is a* $\triangleleft$*-congruence but it is not true that every* $\triangleleft$*-congruence is a* $\triangleright$*-congruence.*
6. *If* $t \notin \mathbb{Z}$ *and* $\frac{1}{t} \notin \mathbb{Z}$ *then neither* $\triangleright$*-congruences nor* $\triangleleft$*-congruences imply quandle congruences.*

Chapter 6

Congruences in Alexander Quandles

6.1 Definition and examples

Previously, in Definition 2.2.20 we defined Alexander quandles. The averaging quandle and weighted average quandle discussed in Chapter 5 are examples of Alexander quandles. In this chapter, we will investigate the nature of congruences and congruence classes more generally in Alexander quandles. For clarity and context, we begin by repeating the definition of an Alexander quandle, from Definition 2.2.20, here:

Definition 6.1.1 (Alexander quandle). Let X be a module over the Laurent ring $\mathbb{Z}[t, t^{-1}]$. Then for $x, y \in X$,

$$x \triangleright y = tx + (1 - t)y \tag{6.1.1}$$

defines a quandle operation on X. The quandle $(X, \triangleright)$ is an *Alexander quandle.*

Remark 6.1.2. Also, as previously commented on in Remark 2.2.21 a helpful view of an Alexander quandle is an abelian group, X, acted on by t, where t is a group automorphism of X. The quandle operation is defined as in Definition 6.1.1 as $x \triangleright y = tx + (1-t)y$. In the averaging quandle (where $t = \frac{1}{2}$) and weighted average quandles discussed in Chapter 5 the abelian group was $\mathbb{Q}$ and the group automorphism was the action of $t \in \mathbb{Q}$ by multiplication. In general, t does not have to be in the abelian group but just needs to define an automorphism of the group.

Remark 6.1.3. We showed in 2.2.22 that an Alexander quandle was a quandle and that the inverse quandle operation for an Alexander quandle is defined as

$$x \triangleleft y = t^{-1}x + (1 - t^{-1})y \tag{6.1.2}$$

in Corollary 2.2.23.

In addition, in Corollary 2.2.23 we showed that whenever $(X, \triangleright)$ is an Alexander quandle then the dual quandle, $(X, \triangleleft)$, is an Alexander quandle with the automorphic role of t taken by t^{-1}. If an Alexander quandle is viewed as an abelian group with an automorphic action of t on the group, as noted above, then necessarily t^{-1} acts automorphically on the same abelian group and therefore defines an Alexander quandle structure.

Swapping the roles of t and t^{-1} is an isomorphism in the Laurent ring $\mathbb{Z}[t, t^{-1}]$ defined by $\phi : \mathbb{Z}[t, t^{-1}] \to \mathbb{Z}[t, t^{-1}]$ with $\phi(t) = t^{-1}$. In Alexander quandles, this isomorphism will allow us to work with $\triangleright$-congruences and deduce analogous results for $\triangleleft$-congruences.

6.2 Sets of differences in congruences

As in Chapter 5, on averaging quandles and weighted average quandles, we will find it useful to define some sets of differences in congruences in Alexander quandles. We define four sets of differences of elements that are related by a congruence that respects either or both of the Alexander quandle operations.

Definition 6.2.1. Let A be an abelian group with an equivalence relation $\sim$ then we define the following four sets:

1. For each $x \in A$ let $D_x = \{y - x : x \sim y\}$;
2. For each $x \in A$ let $D_{[x]} = \{y - z : x \sim y, x \sim z\}$;
3. For the set A let $D = \{x - y : x \sim y, x, y \in A\}$;
4. The intersection set $D_A = \bigcap\limits_{x \in A} D_x$.

For weighted average quandles we effectively found that these difference sets were equal. Which in turn helped us describe the nature of the congruences that could be formed. In the case of weighted average quandles, we were able to establish that whenever for some $x \in A$, $x \sim x + d$ we had for all $a \in A$ that $a \sim a + d$. We established this by showing that for all $a \in A$ both $a \sim a+(1-t)d$ and $a \sim a+td$ held and so $a \sim a+(1-t)d+td = a+d$. Those results relied on the invertibility of t, in the first case, and the invertibility of $(1 - t)$, in the second case. In general, in an Alexander quandle, while we have t is invertible by definition, we do not have that $(1 - t)$ is invertible. Therefore we cannot run the above argument.

However, the first observation that we can make is that if for some $x \in A$, $x \sim x + d$ then for all $a \in A$, $a \sim a + (1-t)d$. This establishes that if $d \in D_x$ then $(1-t)d \in D_x$ and $(1-t)d \in D_A$. By repeating this argument inductively, we get a hierarchical structure that if for some $x \in A$, there exists $d \in D_x$ with $d \neq 0$ then $(1 - t)^k d \in D_A$ for $k \in \mathbb{N}$. Provided the automorphism t is not the identity then $D_A \neq \{0\}$. That is there is potential for a top level of differences that are peculiar to particular congruence classes and below that a set of common differences that are shared by every congruence class and this will be the typical case when $[x]$ has more than one element and for some x, $D_x \neq D_A$. For any particular Alexander quandle there is no necessity for the top level of differences to exist as we saw in weighted average quandles in which the sets of differences were common.

Lemma 6.2.2. *Let A be an Alexander quandle and let $\sim$ be a $\triangleright$-congruence. Suppose there exists $x, y \in A$ with $x \sim y = x + d$. Then for all $a \in A$, $a \sim a + (1 - t)d$.*

Proof. Let A be an Alexander quandle with $x \in A$ and $x \sim x + d$. Then for all $a \in A$ we can construct the element

$$\alpha = t^{-1}a + (1 - t^{-1})x \in A.$$

We note that

$$\alpha \triangleright x = a + (t - 1)x + (1 - t)x = a,$$

and

$$\alpha \triangleright (x + d) = a + (t - 1)x + (1 - t)(x + d) = a + (1 - t)d.$$

Therefore, since $x \sim x + d$ we have $a \sim a + (1 - t)d$ for all $a \in A$. $\square$

Remark 6.2.3. As noted prior to the theorem, provided there exists $d \neq 0$ and t is not the identity automorphism then this necessarily means that $D_A \neq \{0\}$. That is, there are necessarily non-zero common differences in D_A.

In the case of averaging quandles, we saw that we could extend this argument indefinitely in the quandle to get that whenever $x \sim x + d$ we had for all $a \in A$ that for all $n \in \mathbb{Z}$, $a \sim a + n(1 - t)d$ was true. Actually, in the averaging quandles we had the stronger result that $a \sim a + d$ and it was that interval that we extended. The more limited result based on $(1 - t)d$ is true in an Alexander quandle and we will state it here without proof. Although, that argument from Chapter 5 will shortly become redundant when we see that for any equivalence relation on an abelian group, G, the set of common differences, D_G, is a subgroup. Therefore, whenever $d \in D_x$ we necessarily have $nd \in D_x$ for $n \in \mathbb{Z}$, which applied here to D_a means that $n(1-t)d \in D_a$ with $n \in \mathbb{Z}$.

Corollary 6.2.4. *Let A be an Alexander quandle and let $\sim$ be a $\triangleright$-congruence. Suppose there exists $x, y \in A$ with $x \sim y = x + d$. Then for all $a \in A$ and for all $n \in \mathbb{Z}$, $a \sim a + n(1-t)d$.*

Similarly, in the case of averaging quandles we saw that when $x \sim x + d$ that for all $a \in A$ we had $a \sim a + t^n d$. As shown, here we only have $a \sim a + (1-t)d$ as our base case but that can be extended by repeated applications of Lemma 6.2.2 to get for all $a \sim a + (1-t)^n d$. We state that result without proof.

Corollary 6.2.5. *Let A be an Alexander quandle and let $\sim$ be a $\triangleright$-congruence. Suppose there exists $x, y \in A$ with $x \sim y = x + d$. Then for all $a \in A$ and for all $n \in \mathbb{N}$, $a \sim a + (1-t)^n d$.*

The results in Corollaries 6.2.4 and 6.2.4 can be combined to give that whenever for some $x \in A$, $x \sim x + d$ then for all $a \in A$, for all $m \in \mathbb{Z}$, and for all $n \in \mathbb{N}$, $a \sim a + m(1-t)^n d$.

Remark 6.2.6. Previously, for the weighted average quandles we were able to show, in addition, that if $x \sim x + d$ for some $x \in A$ that $a \sim a + td$ for all $a \in A$. If true, combining that result with the result in Lemma 6.2.2 we would be able to establish

$$a \sim a + (1-t)d \sim a + (1-t)d + td = a + d$$

and so we would have for all $a \in A$, $a \sim a + d$. However, that result relied on the invertibility of $(1 - t)$. We could construct the element

$$\alpha' = (1 - t)^{-1}(a - tx) \tag{6.2.1}$$

and show by the calculation of

$$x \triangleright \alpha' = a$$

and

$$(x + d) \triangleright \alpha' = a + td$$

that $a \sim a + td$.

In general, in an Alexander quandle, the element $(1 - t)^{-1}(a - tx)$ does not necessarily exist. In the special case where $a - tx = (1 - t)a'$ for some $a' \in A$ then we can deduce that $a \sim a + d$ whenever $x \sim x + d$ for some $x \in A$. This is the case in an averaging quandle where we can just divide by $(1 - t)$ for $t \in \mathbb{Q} \setminus \{0, 1\}$ to get equation (6.2.1).

This difference in the properties of the special cases of averaging quandles and the general case of Alexander quandles suggests a possible interesting structure to the sets of differences in congruence classes. In the case of averaging quandles we had the structure that if for some $x \in A$ we had $d \in D_x$ we could deduce that for all $a \in A$, $n \in \mathbb{Z}^*$, $t^n d \in D_a$. Therefore every difference set D_a was precisely the same.

In general, in Alexander quandles we see there is a similar structure but with the exception that when for some $x \in A$, $x \sim x + d$ we do not necessarily have for all $a \in A$ that $a \sim a + d$. That is, the common structure that we found for differences in weighted average quandles begins below some top level of differences that may not be shared by all congruence classes. This suggests the possibility that the sets D_x may be different, at a top level, but be identical below that. We will later show some examples of congruence classes in which the difference sets are not equal for all elements of the Alexander quandle.

As foreshadowed, we can establish in any abelian group G that the set D_G is a subgroup of G.

Lemma 6.2.7. *Let G be an abelian group, $\sim$ be an equivalence relation on G, and $D_x = \{d = y - x : x \sim y\}$. Then $D_G = \bigcap\limits_{x \in G} D_x$ is a subgroup of G.*

Remark 6.2.8. Firstly, note that the identity is in D_G. We have $0 \in D_G$ since an equivalence relation is reflexive, for all $x \in G$, $x \sim x$, therefore $x - x = 0 \in D_x$. That is, the identity element of the abelian group is a member of $D_G = \bigcap\limits_{x \in G} D_x$.

Secondly, note that the inverses are in D_G. Since $d \in D_G$ implies that for all $x \in G$, $x \sim x + d$ we can apply that relationship to $x - d$ we have $x - d \sim x - d + d = x$ and therefore $-d \in D_G$. That is, the inverse element of every element $d \in D_G$ is in D_G.

Those are trivial observations. We will prove that D_G is a subgroup using the one-step subgroup test.

Proof. For all $d, e \in D_G$ we have for all $x \in G$ that $x \sim x + d$ and $x \sim x + e$ therefore $x + d \sim x + e = (x + d) + (e - d)$ and therefore $d - e \in D_{x+d}$. Substitute $y = x + d$ then we have for all $y \in G$, $y \sim y + (e - d)$ and therefore $e - d \in D_y$ and $e - d \in D_G$. This is the one-step subgroup test. Therefore D_G is a subgroup of G. □

Remark 6.2.9. For any Alexander Quandle, $(A, \triangleright)$, the set A together with the binary operation of addition, $(A, +)$, is a group. Since any congruence in an Alexander quandle is an equivalence relation Lemma 6.2.7 applies to the congruence. Therefore Lemma 6.2.7 can be applied to an Alexander quandle with a $\triangleright$-congruence, a $\triangleleft$-congruence, or a quandle congruence.

Corollary 6.2.10. *Let A be an Alexander quandle, $\sim$ a congruence (either a $\triangleright$-congruence or a $\triangleleft$-congruence) on A, and $D_A = \bigcap\limits_{x \in A} D_x$ where $D_x = \{d = y - x : x \sim y\}$. Then D_A is a subgroup of A.*

Corollary 6.2.11. *Let A be an Alexander quandle, $\sim$ a quandle congruence on A, and $D_A = \bigcap\limits_{x \in A} D_x$ where $D_x = \{d = y - x : x \sim y\}$. Then D_A is a subgroup of A.*

While we do not have for all $a \in A$ that $d \in D_a$ whenever we have some $x \sim x + d$, we are able to show a slightly weaker result that $td \in D_A$ whenever $d \in D_A$. Therefore D_A is closed under multiplication by t. Again this leaves open the possibility of a top level in which different elements have different sets of differences but it shows that there is considerable structure to the set of common differences.

Remark 6.2.12. We use 'multiplication by t', here and elsewhere, to mean the action of t on the abelian group in the quandle. In some cases this action is by multiplication, as for example in the weighted average quandles. In general, the action (multiplication) is some automorphism on the quandle elements.

Lemma 6.2.13. *Let A be an Alexander quandle, $\sim$ a $\triangleright$-congruence on A, $D_A = \bigcap_{x \in A} D_x$ where $D_x = \{d = y - x : x \sim y\}$. Then D_A is closed under multiplication by t.*

Proof. For all $d \in D_A$ and for all $x \in A$ there exists $y \in A$ with $x \sim y$ and $y = x + d$. Since $\sim$ is a $\triangleright$-congruence we have:

$$\begin{aligned} x &= x \triangleright x \\ &\sim y \triangleright x \\ &= (x+d) \triangleright x \\ &= t(x+d) + (1-t)x \\ &= tx + (1-t)x + td \\ &= x + td. \end{aligned}$$

Therefore for all $d \in D_A$ we have for all $x \in A$ that $x \sim x + td$ and so

$td \in D_x$ and hence $td \in D_A$. Since $td \in D_A$ for all $d \in D_A$, D_A is closed under multiplication by t. □

Similarly, we can prove that the corresponding set of differences for a $\triangleleft$-congruence is closed under multiplication by t^{-1}.

Lemma 6.2.14. *Let A be an Alexander quandle, $\sim$ be a $\triangleleft$-congruence on A, $D_A = \bigcap\limits_{x \in A} D_x$ where $D_x = \{d = y - x : x \sim y\}$. Then D_A is closed under multiplication by t^{-1}.*

Proof. The proof follows the proof in Lemma 6.2.13 with $\triangleright$ replaced by $\triangleleft$ and t replaced by t^{-1} or equivalently applying Lemma 6.2.13 to the dual quandle $(A, \triangleleft)$ where the inverse operation in $(A, \triangleright)$ is thought of as the primary operation. □

Combining the results in Lemmas 6.2.13 and 6.2.14 we can show that if $\sim$ is a quandle congruence then D_A is closed under multiplication by both t and t^{-1}.

Corollary 6.2.15. *Let A be an Alexander quandle, $\sim$ be a quandle congruence on A, $D_A = \bigcap\limits_{x \in A} D_x$ where $D_x = \{d = y - x : x \sim y\}$. Then D_A is closed under multiplication by t and t^{-1}.*

6.3 Constructing a Congruence from a Subgroup

We have shown that if we have a congruence on an Alexander quandle then the intersection of the sets of differences $D_x = \{d = y - x : x \sim y\}$ is a subgroup of the quandle, A, that is closed under multiplication by either t or t^{-1} depending on whether the congruence is a $\triangleright$-congruence or a $\triangleleft$-congruence respectively and closed under both t and t^{-1} when we have a quandle congruence.

Conversely we can show that if we have a subgroup $D \leq A$ that is closed under multiplication by t then we can define an equivalence relation that is a $\triangleright$-congruence on A. Similarly, if we have a subgroup $D \leq A$ that is closed under multiplication by t^{-1} then we can define an equivalence relation that is a $\triangleleft$-congruence on A.

Lemma 6.3.1. *Let D be a subgroup, that is closed under multiplication by t, of an Alexander quandle, A. Define $\sim$ such that $x \sim y$ if and only if $d = x - y \in D$. Then $\sim$ is a $\triangleright$-congruence.*

Proof. First we show that $\sim$ is an equivalence relation.

1. Since D is a subgroup $0 \in D$ therefore $x \sim x$. Therefore $\sim$ is reflexive.

2. Since D is a subgroup for all $d \in D$ we have $-d \in D$ therefore if $x \sim y$ where $x-y = d$ then $y \sim x$ since $y-x = -d$. Therefore $\sim$ is symmetric.

3. Since D is a subgroup for all $x, y, z \in A$ where $x \sim y$ and $y \sim z$ with $x - y = d_1$ and $y - z = d_2$ we have that $-d_1 - d_2 \in D$ and therefore that $x \sim x - d_1 - d_2 = y - d_2 = z$. Therefore $\sim$ is transitive.

Therefore $\sim$ is an equivalence relation.

Now we show that this equivalence relation is a $\triangleright$-congruence.

For all $x \sim y$ and $w \sim z$ we have $x - y = d_1 \in D$ and $w - z = d_2 \in D$. Now we compute $y \triangleright z$:

$$\begin{aligned} y \triangleright z &= (x - d_1) \triangleright (w - d_2) \\ &= (x \triangleright w) - (d_1 \triangleright d_2) \\ &= (x \triangleright w) - \big(td_1 + (1-t)d_2\big) \end{aligned}$$

Since D is a subgroup that is closed under multiplication by t then $td_1 + (1 - t)d_2 \in D$ and $(x \triangleright w) \sim (y \triangleright z)$. Therefore $\sim$ is a $\triangleright$-congruence. $\square$

Remark 6.3.2. Similar reasoning shows that an equivalence relation defined by subgroup closed under multiplication by t^{-1} defines a $\triangleleft$-congruence. Moreover an equivalence relation defined by a subgroup closed under multiplication by both t and t^{-1} defines a quandle congruence. Therefore we have the following immediate corollaries.

Corollary 6.3.3. *Let D be a subgroup, that is closed under multiplication by t^{-1}, of an Alexander quandle, A. Define $\sim$ such that $x \sim y$ if and only if $d = x - y \in D$. Then $\sim$ is a $\triangleleft$-congruence.*

Corollary 6.3.4. *Let D be a subgroup, that is closed under multiplication by t and t^{-1}, of an Alexander quandle, A. Define $\sim$ such that $x \sim y$ if and only if $d = x - y \in D$. Then $\sim$ is a quandle congruence.*

Remark 6.3.5. We have established two similar and related but not completely reciprocal properties. Firstly that if we have a subgroup closed under multiplication by t^{α} with $\alpha \in \{-1, 1\}$ then we can construct a congruence (either a $\triangleright$-congruence or a $\triangleleft$-congruence depending on the value of α). Secondly, that if we have a congruence then the set $D_A = \bigcap_{x \in A} D_x$ with $D_x = \{y - x : x \sim y\}$ has the properties that D_A is a subgroup that is closed under multiplication by t^{α}.

In the latter case, as we will see in Sections 6.4 and 6.5, it is possible that for some $x \in A$, there exist $\xi \in [x]$ with $\xi - x = d_{\xi} \in D_x$ with $d_{\xi} \notin D_A$, so that it is not true that for all $y \in A$ that $d_{\xi} \in D_y$. That is, not every congruence on an Alexander quandle A arises from a subgroup D of A as described in Lemma 6.3.1 and Corollaries 6.3.3 and 6.3.4. We show however that the congruences that we get from Corollary 6.3.4 are precisely the congruences where the quotient is again an Alexander quandle.

Theorem 6.3.6. *Let A be an Alexander quandle and $\sim$ be a quandle congruence on A. Then the quotient $A/{\sim}$ is an Alexander quandle if and only if there is a subgroup D of A that is closed under multiplication by t and t^{-1} such that the congruence classes of $\sim$ are the cosets of D.*

Proof. First assume that we have an Alexander quandle, A, with a congruence, $\sim$, whose congruence classes are cosets of a subgroup of A which is closed under multiplication by t and t^{-1}. Let the subgroup that defines the congruence classes be $D = [0]$.

We need to show that

$$[p] \triangleright [q] = t[p] + (1 - t)[q] = [p \triangleright q] = [tp + (1 - t)q]$$

is well defined. To establish this we need to show that $[p] + [q] = [p + q]$ is well defined and that $t[p] = [tp]$ is well defined.

The operation $[p] + [q] = [p + q]$ is well defined since for any $p_i \in [p]$ and $q_j \in [q]$ we have $p_i = p + d_i$ and $q_j = q + d_j$ with $d_i, d_j \in D$ the subgroup of A that defines the cosets of A that are the congruence classes of $\sim$. Now $p_i + q_j = p + d_i + q + d_j = (p + q) + (d_i + d_j) \in [p + q]$ since $d_i + d_j \in D$.

For any $p_i \in [p]$ we have $p_i = p+d_i$ with $d_i \in D$. Therefore $tp_i = tp+td_i \in [tp]$ since $td_i \in D$ as D is closed under multiplication by t. Similarly, $t^{-1}[p] = [t^{-1}p]$ is well defined.

Therefore the operations $[p] \triangleright [q] = t[p] + (1 - t)[q]$ and $[p] \triangleleft [q] = t^{-1}[p] + (1 - t^{-1})[q]$ are well defined.

Since the Alexander operations are well defined, we can apply Theorem 3.2.9 to establish that the quotient is an Alexander quandle.

Now assume we have an Alexander quandle $(A/{\sim}, \triangleright)$ on the quotient formed from some congruence $\sim$ on an Alexander quandle A. Since $(A/{\sim}, +)$ is a group with $+$ defined as $[p]+[q]=[p+q]$ we can define the group homomorphism $\phi : A \to A/{\sim}$ with $\phi(p)=[p]$.

Since ϕ is a homomorphism we have $A/{\sim} \cong A/\ker\phi$ and $\ker\phi$ is a subgroup of A. Therefore $[p]=[q]$ if and only if $\phi(p)=\phi(q)$, that is, if and only if $p+\ker\phi = q+\ker\phi$ and therefore the congruence classes are cosets of $\ker\phi$.

Finally we need to show that $\ker\phi$ is closed under multiplication by t and t^{-1}. For all $d \in \ker\phi$ we have $d \sim 0$ therefore $d \triangleright 0 = td \sim 0 \triangleright 0 = 0$ and $td \in \ker\phi$. Similarly, $t^{-1}d \in \ker\phi$ and the subgroup $\ker\phi$ is closed under multiplication by t and t^{-1}. □

6.4 Examples of $D_x \neq D_A$

In Remark 6.3.5 we suggested the possibility that $D_x \neq D_A$. We construct such an example. The idea is to construct a set of common differences and construct sets of differences that include the common differences and other differences that are not common for all elements. We will work in $A = \mathbb{Z}[t,t^{-1}]$ which may be viewed as a module over itself and hence has a natural Alexander quandle structure with the standard Alexander quandle operation given in equation (6.1.1).

Example 6.4.1. Let $A = \mathbb{Z}[t,t^{-1}]$, with the natural Alexander quandle structure. We define the following two sets:

$$D = \{p(t) \in \mathbb{Z}[t] : p(1) = 0\};$$

$$E = \{p(t) \in \mathbb{Z}[t] : p(1) = 1\}.$$

We will use these two sets to construct difference sets for elements of A that are congruent to each other.

Note that D is a subgroup of $\mathbb{Z}[t]$. For the one-step subgroup test we need for $p(t), q(t) \in D$, $p(t) - q(t) \in D$. Since for all $p(t), q(t) \in D$, $p(1) - q(1) = 0 - 0 = 0$, therefore $p(t) - q(t) \in D$. Also note that D is non-empty, $0 \in D$ for example, and is closed under multiplication by t as for any $d \in D$ we have $d(1) = 0$ therefore $td(t)|_{t=1} = 1 \cdot 0 = 0$ and so $td \in D$.

We define a congruence based on sets of differences at $f(t, t^{-1}) = f(t)$ as follows.[1] Let

$$D_f = D_{f(t)} = \begin{cases} D \cup E \text{ if } f(1) \text{ is even;} \\ D \cup (-E) \text{ if } f(1) \text{ is odd,} \end{cases}$$

then $f \sim g$ if and only if $g - f \in D_f$. We claim this defines a $\triangleright$-congruence on A. The difference sets for the elements in a congruence class, $[f]$, will be one of two types depending on the parity of $f(1)$.

To show that this is a $\triangleright$-congruence we need to show that $\sim$ is an equivalence relation and then that the equivalence relation respects the quandle operation.

---

[1] We typically write, for $f \in \mathbb{Z}[t, t^{-1}]$, $f(t)$ to mean the same as $f(t, t^{-1})$. For example, if we had $f = t^{-1} + t$ we will typically refer to this as $f(t)$ rather than $f(t, t^{-1})$. Consequently and for clarification, we will calculate $f(1)$ as $f(1) = 1^{-1} + 1 = 2$.

Equivalence Relation

1. **Reflexive**

   First we check that $\sim$ is an equivalence relation. Since $f - f = 0$ and $0 \in D \subseteq D_f$ we have that $\sim$ is reflexive.

2. **Symmetric**

   For symmetry we need if $f \sim g$ then $g \sim f$. If $f \sim g$ then $g(t) = f(t) + p(t)$ and $g - f = p(t)$. Therefore $f - g = -p(t)$.

   (a) If $p(1) = 0$ then $p(t) \in D$ and $-p(1) = 0$ therefore $-p(t) \in D \subseteq D_g$ and $g \sim f$.

   (b) If $p(1) = 1$ then $p(t) \in E$ and $f(1)$ is even. Therefore $g(1) = f(1) + p(1)$ is odd. Since $-p(1) = -1$ we have $-p(t) \in -E \subseteq D_g$ and $g \sim f$.

   (c) If $p(1) = -1$ then $-p(t) \in -E$ and $f(1)$ is odd. Therefore $g(1) = f(1) + p(1)$ is even. Since $-p(1) = 1$ we have $-p(t) \in E \subseteq D_g$ and $g \sim f$.

   Therefore $\sim$ is symmetric.

3. **Transitivity**

   For transitivity we need to show that if $f \sim g$ and $g \sim h$ then $f \sim h$. If $f \sim g$ and $g \sim h$ then $g = f + p(t)$ and $h = g + q(t)$ therefore $h = f + p(t) + q(t)$.

(a) If $p(1) = 0$.

   i. If $q(1) = 0$ then $p(1) + q(1) = 0$ and $p(t) + q(t) \in D \subseteq D_f$ and $f \sim h$.

   ii. If $q(1) = 1$ then $g(1)$ is even which implies that $f(1) = g(1) - p(1) = g(1)$ is even. Therefore since $p(1) + q(1) = 1$ we have $p(t) + q(t) \in E \subseteq D_f$ and $f \sim h$.

   iii. If $q(1) = -1$ then $g(1)$ is odd which implies that $f(1) = g(1) - p(1)$ is odd. Therefore since $p(1) + q(1) = -1$ we have $p(t) + q(t) \in (-E) \subseteq D_f$ and $f \sim h$.

(b) If $p(1) = 1$ then $p(t) \in E$ and $f(1)$ is even. Therefore $g(1) = f(1) + p(1)$ is odd and $q(t) \in D \cup (-E)$ so $q(1) \in \{0, -1\}$.

   i. If $q(1) = 0$ then $p(1) + q(1) = 1$ and therefore $p(t) + q(t) \in E \subseteq D_f$ and $f \sim h$.

   ii. If $q(1) = -1$ then $p(1) + q(1) = 0$ and therefore $p(t) + q(t) \in D \subseteq D_f$ and $f \sim h$.

(c) If $p(1) = -1$ then $p(t) \in (-E)$ and $f(1)$ is odd. Therefore $g(1) = f(1) + p(1)$ is even and $q(t) \in D \cup E$ so $q(1) \in \{0, 1\}$.

   i. If $q(1) = 0$ then $p(1) + q(1) = -1$ and therefore $p(t) + q(t) \in -E \subseteq D_f$ and $f \sim h$.

   ii. If $q(1) = 1$ then $p(1) + q(1) = 0$ and therefore $p(t) + q(t) \in$

$D \subseteq D_f$ and $f \sim h$.

Therefore $\sim$ is transitive.

Quandle operation respected

Finally, we need to check that $\sim$ respects the quandle operation. We require for all $e, f, g, h \in A$ whenever $e \sim f$ and $g \sim h$ that $e \triangleright g \sim f \triangleright h$. That is, the difference $(f \triangleright h) - (e \triangleright g) \in D_{e \triangleright g}$.

We can write $f(t) = e(t) + p(t)$ with $p(t) \in D_e$ and $h(t) = g(t) + q(t)$ with $q(t) \in D_g$ although only the former conclusion will turn out to be important. Note

$$\begin{aligned} f \triangleright h &= (e + p) \triangleright (g + q) \\ &= e \triangleright g + p \triangleright q \\ &= e \triangleright g + tp(t) + (1 - t)q(t) \\ &= e \triangleright g + r(t). \end{aligned}$$

Also note that since $(e \triangleright g)(1) = 1.e(1) + (1 - 1).g(1) = e(1)$, $e(1)$ and $(e \triangleright g)(1)$ necessarily have the same parity. Since $r(1) = 1.p(1)+(1-1)q(1) = p(1)$ then $p(t) \in D_e$ implies $r(t) \in D_{e \triangleright g}$ and $(e \triangleright g) \sim (f \triangleright h)$. Therefore $\sim$ respects the quandle operation.

In conclusion of this example, we have shown that we have an equivalence relation that respects the quandle operation. So we have an example of a $\triangleright$-congruence on an Alexander quandle with a common set of differences,

D, but with different sets of differences, either $D \cup E$ or $D \cup (-E)$, for $f \in A$, depending on the parity of $f(1)$ — if $f(1)$ is even then $f \sim g$ if $g - f \in D_f = D \cup E$ and if $f(1)$ is odd then $f \sim g$ if $g - f \in D_f = D \cup (-E)$.

Similar equivalence relations can be formed based on differences of the form $p(1) = n$ with $n \in \mathbb{Z}$. This is because for $f(t) = e(t) + p(t)$ and $h(t) = g(t) + q(t)$ we have

$$\begin{aligned} \big(e(t) + p(t)\big) \triangleright \big(g(t) + q(t)\big) &= \big(e(t) \triangleright g(t)\big) + \big(p(t) \triangleright q(t)\big) \\ &= \big(e(t) \triangleright g(t)\big) + \big(tp(t) + (1-t)q(t)\big) \\ &= \big(e(t) \triangleright g(t)\big) + r(t), \end{aligned}$$

with $r(1) = p(1)$. Therefore since $p(t) \in D_e$ we have $r(t) \in D_e$.

Since $(e \triangleright g)(1) = e(1)$ we have $D_{e \triangleright g} = D_e$. Therefore $r(t) \in D_{e \triangleright g}$ and $(e \triangleright g) \sim (f \triangleright h)$ and so $\sim$ is a $\triangleright$-congruence.

Here is an example with three difference sets defined based on the value of $f(1)$ modulo 3. In Section 6.5, that example will be extended to difference sets based on the n congruence classes in $\mathbb{Z}_n$.

Example 6.4.2. Let $A = \mathbb{Z}[t, t^{-1}]$, with the natural Alexander quandle structure. We define the following three sets:

$$\begin{aligned} D_0 &= \{p(t) \in \mathbb{Z}[t] : p(1) = 0\}; \\ D_1 &= \{p(t) \in \mathbb{Z}[t] : p(1) = 1\}; \\ D_2 &= \{p(t) \in \mathbb{Z}[t] : p(1) = 2\}. \end{aligned}$$

Define sets of differences at $f(t)$ by:

$$D_f = D_{f(t)} = \begin{cases} D_0 \cup D_1 \cup D_2 \text{ if } f(1) \equiv 0 \bmod 3; \\ D_0 \cup D_1 \cup (-D_1) \text{ if } f(1) \equiv 1 \bmod 3; \\ D_0 \cup (-D_1) \cup (-D_2) \text{ if } f(1) \equiv 2 \bmod 3. \end{cases}$$

Let $f \sim g$ if and only if $g - f \in D_f$. We have, by a similar argument to that in Example 6.4.1, that D_0 is a subgroup closed under multiplication by t and the equivalence relation is a congruence on A. We omit showing that directly by deferring to the arguments in Example 6.5.1 which is a more general example of the same type.

6.5 A more general example of $D_x \neq D_A$

The feature in the two previous examples that enabled us to create classes of elements with differing difference sets was that we partitioned the integers, in Example 6.4.1 into even and odd integers, and in Example 6.4.2 into congruence classes modulo 3. That partitioning approach can be generalised. That is we define an equivalence relation on the Alexander quandle based on congruence modulo n.

Example 6.5.1. Let $A = \mathbb{Z}[t, t^{-1}]$, with the natural Alexander quandle structure. For some $n > 1$, $n \in \mathbb{Z}$ define an equivalence relation $\sim$ on A

such that $f \sim g$ if and only if for some $k \in \mathbb{Z}$ and $\alpha, \beta \in \{0, 1, 2, \cdots, n-1\}$, $f(1) = kn + \alpha$ and $g(1) = kn + \beta$ and $g - f \in \mathbb{Z}[t]$ and so the difference $g - f$ depends only on the non-negative powers of t.

For example, if $n = 5$ and $f(1) = 13 = 2 \times 5 + 3$ then $f \sim g$ if and only if $g(1) \in \{10, 11, 12, 13, 14\}$ and $g - f \in \mathbb{Z}[t]$.

It is easy to see that $\sim$ is an equivalence relation. Choose any $f, g, h \in A$ such that $f \sim g$ and $g \sim h$. Since $f \sim g$ and $g \sim h$ we have for some $k \in \mathbb{Z}$ and $\alpha, \beta, \gamma, \in \{0, 1, 2, \cdots, n-1\}$ that $f(1) = kn + \alpha$, $g(1) = kn + \beta$ and $h = kn + \gamma$. We also have that $g - f \in \mathbb{Z}[t]$ and $h - g \in \mathbb{Z}[t]$.

For reflexivity, obviously $f \sim f$ since trivially $k = k$ and $f(1) = kn + \alpha$ and by definition $\alpha \in \{0, 1, 2, \cdots, n-1\}$ and $f - f = 0 \in \mathbb{Z}[t]$ as required.

For symmetry, since $f \sim g$ we have $f = k_f n + \alpha$ and $g = k_g n + \beta$ with $k_f = k_g$ and both $\alpha, \beta \in \{0, 1, 2, \cdots, n-1\}$ and $f - g = -(g - f) \in \mathbb{Z}[t]$ we have that whenever $f \sim g$, $g \sim f$. So we have symmetry.

For transitivity, since, in addition, $g \sim h$ we have $h = k_h n + \gamma$ with $k_h = k_g = k_f$ and $\gamma \in \{0, 1, 2, \cdots, n-1\}$ therefore we have that both $\alpha, \gamma \in \{0, 1, 2, \cdots, n-1\}$. We also have that if $g - f \in \mathbb{Z}[t]$ and $h - g \in \mathbb{Z}[t]$ that $h - f = (h - g) - (g - f) \in \mathbb{Z}[t]$ and therefore $f \sim h$ and so we have transitivity.

We need to check that $\sim$ is a congruence. Note that the equivalence relation is dependent on the value of elements of A at $t = 1$. It is useful to note that for $f, g \in A$ that

$$(f \triangleright g)|_{t=1} = (f \triangleright g)(1) = (tf + (1-t)g)|_{t=1} = f(1). \tag{6.5.1}$$

Consider $e, f, g, h \in A$ with $e \sim f$ and $g \sim h$. We can write $f = e + p(t)$ and similarly $h = g + q(t)$ for some $p(t), q(t) \in \mathbb{Z}[t]$. Now,

$$f \triangleright h = (e+p) \triangleright (g+q) = e \triangleright g + p \triangleright q,$$

from which we can see from utilising equation (6.5.1)

$$(f \triangleright h)|_{t=1} = e(1) + p(1).$$

Since $e \sim f = e + p$ we have $e(1) = (e \triangleright g)|_{t=1}$ and $f(1) = (f \triangleright h)|_{t=1} = e(1) + p(1)$. We also have the

$$\begin{aligned} f \triangleright h - e \triangleright g &= p \triangleright q \\ &= tp + (1-t)q \\ &\in \mathbb{Z}[t] \end{aligned}$$

since $p, q \in \mathbb{Z}[t]$. Therefore $e \triangleright g \sim f \triangleright h$ and so $\sim$ is a $\triangleright$-congruence on A.

Returning to the case where $n = 5$, for illustrative purposes, and looking at the sets of differences $\{f - g : f \sim g\}$. When $f(1) \equiv 0 \bmod 5$ then $g(1) - f(1) \in \{0, 1, 2, 3, 4\}$ and so $g - f \in \{p(t) \in \mathbb{Z}[t] : p(1) \in \{0, 1, 2, 3, 4\}$. When $f(1) \equiv 1 \bmod 5$ then $g(1) - f(1) \in \{-1, 0, 1, 2, 3\}$ and so $g - f \in$

$\{p(t) \in \mathbb{Z}[t] : p(1) \in \{-1, 0, 1, 2, 3\}$.

In the general case, we will have, for $k \in \{0, 1, 2, \cdots, n-1\}$, the following sets of differences:

$$D_k = \{p(t) \in \mathbb{Z}[t] : p(1) = k\}. \tag{6.5.2}$$

Since some differences will be based on $p(1) < 0$, we also need the definition that

$$D_{-k} = -D_k = \{p(t) \in \mathbb{Z}[t] : p(1) = -k\}. \tag{6.5.3}$$

For any particular $f \in A$ we will have n of these sets of differences in play. The difference set at each f will be

$$D_{f(t)} = \bigcup_{k=0}^{n-1} D_{k-f(1)_n}, \tag{6.5.4}$$

where $f(1)_n$ is the value of $f(1)$ modulo n.

This is a generalisation of Examples 6.4.1, where $n = 2$, and 6.4.2, where $n = 3$. This example could be presented in a similar manner to those examples by first defining the difference sets, D_k, from equation (6.5.2) and then the difference set at f, D_f, from equation (6.5.4) and then defining the equivalence relation $f \sim g$ if and only if $g - f \in D_f$.

Bibliography

[1] Jennifer Anderson, Alexis Brownell, Harrison Potter, and David Yetter. Quandle basics. 2006.

[2] Unknown Author. A subquandle non-example. `https://abearoflittlebrain.wordpress.com/2011/04/20/a-subquandle-non-example/`, 2011. Accessed: 2022-03-28.

[3] Claude Gaspar Bachet. *Problemes Plaisans Et delectables, qui se font par les nombres: Partie recueillis de diuers autheurs...* Rigaud, 2nd edition, 1624. (French).

[4] Yongju Bae and Seonmi Choi. On properties of commutative Alexander quandles. *J. Knot Theory Ramifications*, 23(7):1460013, 8, 2014.

[5] Etienne Bézout. *Théorie générale des équations algébrique.* De l'imprimerie de Ph. D. Pierres, 1779. (French).

[6] Stephen Mark Budden. *Knots and Quandles.* PhD thesis, University of Auckland, 2009.

[7] E. Bunch, P. Lofgren, A. Rapp, and D. N. Yetter. On quotients of quandles. *J. Knot Theory Ramifications*, 19(9):1145–1156, 2010.

[8] C. Burstin and W. Mayer. Distributive gruppen von endlicher ordnung. *Journal für die reine und angewandte Mathematik*, 160:111–130, 1929. (German).

[9] C. Burstin and W. Mayer. Distributive gruppen endlicher ordnung [finite distributive groups]. `https://arxiv.org/abs/1403.6326`, 2014. Translater: Ansgar Wenzel, Accessed: 2022-05-15. (English translation from German).

[10] J.C. Conway and G. C. Wraith. Private correspondence. 1959.

[11] Alissa Susan Crans. *Lie 2-algebras*. ProQuest LLC, Ann Arbor, MI, 2004. Thesis (Ph.D.)–University of California, Riverside.

[12] Patrick Dehornoy. Some aspects of the SD-world. In *Nonassociative mathematics and its applications*, volume 721 of *Contemp. Math.*, pages 69–96. Amer. Math. Soc., [Providence], RI, [2019] ©2019.

[13] Mohamed Elhamdadi and Sam Nelson. *Quandles—an introduction to the algebra of knots*, volume 74 of *Student Mathematical Library*. American Mathematical Society, Providence, RI, 2015.

[14] Roger Fenn and Colin Rourke. Racks and links in codimension two. *J. Knot Theory Ramifications*, 1(4):343–406, 1992.

[15] David Joyce. A classifying invariant of knots, the knot quandle. *J. Pure Appl. Algebra*, 23(1):37–65, 1982.

[16] David Edward Joyce. *An algebraic approach to symmetry with applications to knot theory.* ProQuest LLC, Ann Arbor, MI, 1979. Thesis (Ph.D.)–University of Pennsylvania.

[17] Seiichi Kamada. Quandles derived from dynamical systems and subsets which are closed under quandle operations. *Topology Appl.*, 157(1):298–301, 2010.

[18] Pedro Lopes and Dennis Roseman. On finite racks and quandles. *Comm. Algebra*, 34(1):371–406, 2006.

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

[20] Sujoy Mukherjee and Józef H. Przytycki. On the rack homology of graphic quandles. In *Nonassociative mathematics and its applications*, volume 721 of *Contemp. Math.*, pages 183–197. Amer. Math. Soc., [Providence], RI, [2019] ©2019.

[21] Sam Nelson. Quandles and racks. `https://www1.cmc.edu/pages/faculty/VNelson/quandles.html`. Accessed: 2022-05-15.

[22] Sam Nelson and Chau-Yim Wong. On the orbit decomposition of finite quandles. *J. Knot Theory Ramifications*, 15(6):761–772, 2006.

[23] Takefumi Nosaka. *Quandles and topological pairs.* SpringerBriefs in Mathematics. Springer, Singapore, 2017. Symmetry, knots, and cohomology.

[24] C. S. Peirce. On the Algebra of Logic. *Amer. J. Math.*, 3(1):15–57, 1880.

[25] Józef H. Przytycki. Distributivity versus associativity in the homology theory of algebraic structures. *Demonstratio Math.*, 44(4):823–869, 2011.

[26] Kurt Reidemeister. Elementare Begründung der Knotentheorie. *Abh. Math. Sem. Univ. Hamburg*, 5(1):24–32, 1927. (German).

[27] Hayley Ryder. The congruence structure of racks. *Comm. Algebra*, 23(13):4971–4989, 1995.

[28] Hayley Jane Ryder. *The structure of racks.* PhD thesis, University of Warwick, 1993.

[29] Mituhisa Takasaki. Abstraction of symmetric transformations. *Tôhoku Math. J.*, 49:145–207, 1943. (Japanese).

[30] Gerhard Thomsen. *Grundlagen der Elentargeometrie in gruppen algebraischer Behandlung.* Hamburger Math. Einzelschr., no15, Teubner, Leipzig, 1933.

[31] Gavin Wraith. A personal story about knots. `http://www.wra1th.plus.com/gcw/math/Rack.html`. Accessed: 2022-05-29.