Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

DIPLOMOVÁ PRÁCE

Hana Holmes

Levodistributivní algebry a uzly

Katedra algebry

Vedoucí diplomové práce:	doc. RNDr. David Stanovský, Ph.D.
Studijní program:	Matematika
Studijní obor:	Matematické metody informační bezpečnosti

Praha 2013

Na tomto místě bych ráda poděkovala svému vedoucímu Davidovi Stanovskému za všechny jeho rady a připomínky. Dále bych chtěla poděkovat své rodině a přátelům, především svým rodičům a manželovi Lucienovi, bez jejichž podpory bych tuto práci nejspíš nikdy nedokončila. A konečně, RW za inspiraci ve chvílích beznaděje.

“I always believe in myself, ... The thing I believed in is just getting better every week. If I can do that, you give yourself a chance.”

Prohlašuji, že jsem tuto diplomovou práci vypracovala samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V .... dne .... Podpis autora

Název práce: Levodistributivní algebry a uzly
Autor: Hana Holmes
Katedra: Katedra algebry
Vedoucí diplomové práce: doc. RNDr. David Stanovský, Ph.D., Katedra algebry

Abstrakt: V první části této práce shrneme základy teorie uzlů, části algebraické topologie zabývající se studiem matematických uzlů. Dále představíme algebraické struktury zvané quandly a stručně vysvětlíme, jak s teorií uzlů souvisí.
V hlavní části této práce pak odvodíme několik tvrzení o vlastnostech afinních quandlů, třídy quandlů odvozených od abelovských grup. Zavedeme novou terminologii, která nám umožní popsat afinní quandly z nového úhlu pohledu a dokázat větu, která dáva úplnou charakterizaci konečných afinních quandlů. Provedeme také nový podrobný důkaz již známých tvrzení, která plně popisují, za jakých podmínek jsou dva afinní quandly izomorfní.
V poslední kapitole představíme algoritmus, který na základě Cayleyho tabulky quandlu rozhodne, zda je quandle afinní. Tento algoritmus opět vychází z terminologie zavedené v předchozích sekcích a výrazně vylepšuje dosud známé výsledky.

Klíčová slova: Alexandrův invariant, uzlový quandle, afinní quandle, Cayleyho tabulka, algoritmus

Title: Selfdistributive Algebras and Knots
Author: Hana Holmes
Department: Department of Algebra
Supervisor of the master thesis: doc. RNDr. David Stanovský, Ph.D., Department of Algebra

Abstract: In the first part of this thesis we summarize the basics of knot theory, a part of algebraic topology that studies mathematical knots, introduce algebraic structures called quandles and briefly describe how they are used in knot theory.
In the main part of this thesis we derive some properties of affine quandles, a class of quandles associated with abelian groups. We introduce new terminology that allows us to describe affine quandles from a new perspective, and to prove a theorem that gives us a full characterization of finite affine quandles. Using this terminology, we give new detailed proofs of known results that fully describe the situation when two affine quandles are isomorphic.
In the end, we present an algorithm which decides from the Cayley table of a quandle if the quandle is affine. Again, it is based on the terminology and the claims from the previous sections, and significantly improves the previously known results.

Keywords: Alexander invariant, knot quandle, affine quandle, Cayley table, algorithm

Contents

Introduction

Knot theory is a part of algebraic topology that studies mathematical knots, embeddings of a circle in the Euclidean space $\mathbb{R}^3$. One might imagine a mathematical knot as a piece of string that has been tangled up and whose ends have been glued together. A knot is usually represented by a planar diagram, a projection of the knot onto a plane, where we store the information about relative height of each strand by showing the lower strand interrupted.

The fundamental problem in knot theory is to determine when two diagrams represent the same knot; in other words, when two knots are equivalent. To solve this, we use various knot invariants, functions that have the same outcome for two equivalent knots. We will introduce a few invariants, notably polynomial invariants, tricolorability and the knot group.

While studying knots, algebraic structures called quandles arise quite naturally. A quandle is an idempotent, left-distributive left quasigroup. We can associate a quandle with every knot diagram and we show that this is also a knot invariant, called a knot quandle. The knot quandle is a complete knot invariant: when two knots have isomorphic knot quandles, they can differ only in orientation. Unfortunately, determining when two quandles are isomorphic is quite difficult.

Another knot invariant related to quandles is knot coloring. We can "color" a knot by a quandle; that is, assign quandle elements to the arcs in a knot diagram in a way that the crossings correspond to the relations in the quandle (see Figure 1.3 on page 8). The number of different colorings of a knot by a given quandle is a knot invariant which proved to be quite strong. For a good example of this, see the website of Saito's project [20].

Many knot theorist have lately become interested in affine (or Alexander) quandles: a class of quandles derived from abelian groups and their automorphism. Some have focused on classification of finite affine quandles. In 2003, Nelson described all up to size 15 in [17] and later, together with Murillo, improved this result to size 16 in [15]. The most comprehensive results are presented in the article [8] by Hou, in which he describes all affine quandles of size p, p^2, p^3 and p^4 for a prime number p.

The inspiration for this thesis came mainly from two articles: Hou's detailed study of isomorphisms and automorphisms of affine quandles [7] and a paper written by Murillo, Nelson and Thompson [16] which presents an algorithm that, using the Cayley table (the multiplication table) of an affine quandle, determines whether the quandle is affine and finds its possible representations in the form of an abelian group and its automorphism.

While the first two chapters of this thesis are a compilation of known results from knot and quandle theory, the main parts of this thesis, chapters 3 and 4, either bring entirely new results or create new proofs of known facts. In Chapter 3, we introduce new terminology and we use it to prove a theorem that fully characterizes finite affine quandles, and to re-prove claims from Hou's article [7]. In Chapter 4, we again use this terminology to prove some technical properties of affine quandles; then, with their help, we construct an algorithm for recognizing affine quandles from the Cayley table, which significantly improves the results of Nelson, et al.

First we introduce some terminology that we will use thoughout the article, particularly two groups that are associated with every quandle Q: the group of left translations $\mathrm{LMlt}\,(Q)$ generated by the mappings

$$L_a : x \mapsto a * x, \quad a, x \in Q$$

and the group of displacements $\mathrm{Dis}\,(Q)$ generated by the mappings $L_a L_b^{-1}$, $a, b \in Q$. These groups tell us a great deal about the quandle. We prove a theorem that says that a quandle is affine if and only if there exists an abelian group A such that $\mathrm{LMlt}\,(Q) \leq \mathrm{Aff}\,(A)$ and $\mathrm{Dis}\,(Q) \leq \mathrm{Mlt}\,(A)$, where $\mathrm{Aff}\,(A)$ is a group of affine mappings on A and $\mathrm{Mlt}\,(A)$ is a group of translations of A. We continue to define a numerical value $m\,(Q)$ and show that every affine quandle Q has a subquandle Q' such that $m\,(Q') = 1$ and

$$Q \simeq Q' \times \mathrm{Proj}\,(m\,(Q))\,,$$

where $\mathrm{Proj}\,(n)$ is a projection quandle of size n: for every $x, y \in \mathrm{Proj}\,(n)$, $x*y = y$. We call this subquandle an essential subquandle.

The main result of this thesis is presented in sections 3.3 and 3.4. At first we introduce a new type of algebra: a partial algebra that we term an enveloping algebra, and a special case of this which we call an essential enveloping algebra. We show how it can be used to construct quandles, and that these quandles have properties very similar to affine quandles. In fact, we show that the class of quandles constructed from enveloping algebras contains the class of affine quandles. The problem that we encounter is that to show that a given quandle is affine, we first need to prove the existence of an abelian group with certain properties. This is a problem that we have been able to solve only partially, with the help of a module-theoretical lemma from Hou's article about classification of Alexander quandles [8], and there is certainly much room for future improvements for the infinite case. Nevertheless, we state a theorem which gives us a better characterization of finite affine quandles using the language of enveloping algebras; we further show that any quandle constructed from a finite essential enveloping algebra is affine. We also use this new terminology to rephrase and extend some of the claims from Hou's article [7] to describe fully the situation when two affine quandles are isomorphic.

In the last chapter we present an algorithm that, given a Cayley table of a quandle, decides whether the quandle is affine. This is a significant improvement over the algorithm from the article [16] by Nelson, et al. Their algorithm includes some guesswork in constructing an abelian group and its automorphism, since an affine quandle can be constructed from non-isomorphic abelian groups (see Example 8 on page 32). We avoid that by constructing an enveloping algebra that can be used to derive the affine quandle. This is a lot more efficient since we show that there is a deterministic process that assigns an essential enveloping algebra to any affine essential subquandle.

Chapter 1

From Knots to Quandles

1.1 Knot Equivalence

A mathematical knot is an embedding of a circle in the three-dimensional Euclidean space $\mathbb{R}^3$. We consider two knots to be equivalent if one can be turned into the other without cutting the string or passing one string through another. More formally, we say that the knots K_1 and K_2 are equivalent if there exists a deformation of $\mathbb{R}^3$ taking K_1 to K_2, called ambient isotopy: a continuous map $F : \mathbb{R}^3 \times [0,1] \to \mathbb{R}^3$ such that for every fixed $t \in [0,1]$, $F_t(x) = F(x,t)$ is a homeomorphism, $F_0(K_1) = K_1$ and $F_1(K_1) = K_2$.

The most common way to represent knots is the planar diagram. We project the knot onto a flat surface where we preserve the information about the relative height of each strand by drawing the lower strand interrupted at the crossing point, taking care that no three strands meet at one point. This turns a knot into a set of disjoint arcs. Knots can be oriented or non-oriented; here we will consider only oriented knots. Generally it is not true that we get an equivalent knot when we change the orientation of the knot.

In 1926, Kurt Reidemeister [19] (and a year later independently of him J. W. Alexander and G. B. Briggs [3]) discovered that two knots are equivalent if and only if their diagrams are connected through a finite sequence of changes in the diagrams that are now called *Reidemeister moves*. These moves are shown in the figure below; the diagram does not change outside the area depicted in the figures.

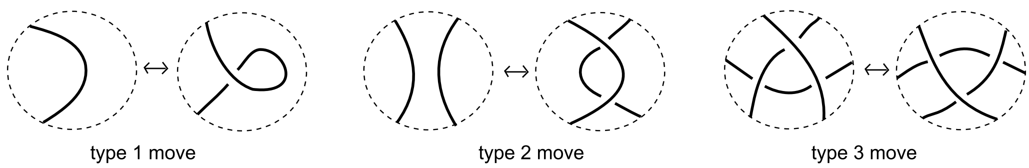

Figure 1.1: The Reidemeister moves.

1.2 Knot Invariants

Determining whether two knots are equivalent is a fundamental question in knot theory. Functions called knot invariants assign an element from a certain set (e.g. a polynomial or a group) to a knot. If two knots are equivalent, the outcome of the function must be the same. A stronger version, a complete knot invariant, gives the same outcome if and only if the two knots are equivalent. Even though there are many known powerful knot invariants, knot theorists are still in search of an easily computable complete knot invariant.

Reidemeister's result gives us a very powerful tool for proving that a certain function is a knot invariant. We do not need to prove that the outcome of the function is the same for every diagram of the knot, we only need to show that it does not change when we apply any one of the Reidemeister moves.

Knot invariants can be complex, such as polynomials or invariants based in topology or homology theory, but they can also be quite simple – not requiring any advanced theory. One of these is the crossing number: the minimum amount of crossings in a diagram taken over all possible diagrams of the knot. Clearly, it is a knot invariant, but it has the disadvantage of being fairly difficult to determine. Another simple example is tricolorability: a knot is tricolorable if it is possible to color each arc with one of the three colors in a way that at every crossings, each arc has a different color or all three arcs have the same color.

The first polynomial invariant was discovered by J. W. Alexander in 1923, and presented in an article from 1928 [2]. For a long time it was the only polynomial invariant, until the discovery of the Jones polynomial in 1980s [11] and others that followed shortly thereafter.

For all the well-known knot polynomials, there is a simple way to construct them. Let us take a knot diagram and choose one crossing. We denote the original knot by K_+. The knots K_- and K_0 are represented by diagrams that are the same as the original one, except for the crossing that is changed according to Figure 1.2: for K_- we switch the relative height of the two strands and for K_0 we reconnect the stands according to the orientation of the knot. The polynomials of K_+, K_- and K_0 then satisfy an equation that is called a *skein relation* and for every knot diagram, it is possible to construct a finite *resolving tree*. In each node of the tree we choose a crossing in the diagram and in its two children we switch and smooth the crossing. We visit each crossing at most once and the links in the leaves consist of one or more trivial components, for which the polynomial is known. A detailed description with a proof can be found in [1].

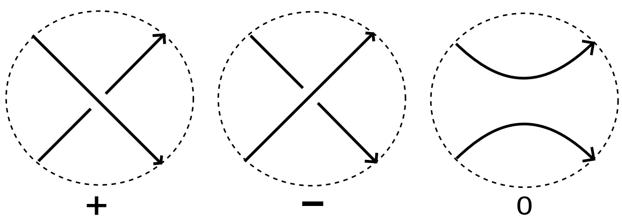

Figure 1.2: The neighborhood where the diagrams of K_+, K_- and K_0 differ.

Even though the skein relation for the Alexander polynomial was mentioned in Alexander's original article as something that the polynomials satisfy, the first definition of a polynomial invariant axiomatically based on skein relations came from John Conway. His polynomial can be obtained from Alexander polynomial by simple variable substitution, and sometimes the Alexander polynomial obtained from a diagram by skein relation is called Alexander-Conway polynomial.

After the discovery of Jones polynomial, many people started to research polynomial invariants. Among the more important finds was the HOMFLY polynomial, discovered independently by two groups of scientists who noticed the obvious similarities between the Alexander and Jones polynomials [4] and [18]. The HOMFLY polynomial is a polynomial in two variables. With simple substitutions in its skein relation, it can be turned into either Alexander or Jones polynomials.

Polynomial	**Skein relation**
Alexander polynomial ($\Delta_K(t)$)	$\Delta_{K_+} - \Delta_{K_-} = (t^{-1/2} - t^{1/2})\Delta_{K_0}$
Conway polynomial ($\nabla_K(z)$)	$\nabla_{K_+} - \nabla_{K_-} = z\nabla_{K_0}$
Jones polynomial ($V_K(t)$)	$t^{-1}V_{K_+} - tV_{K_-} = (t^{1/2} - t^{-1/2})V_{K_0}$
HOMFLY polynomial ($P_K(l,m)$)	$lP_{K_+} + l^{-1}P_{K_-} + mP_{K_0} = 0$

There are of course other ways to construct the polynomial invariants but their complexity limits their relevance to this work.

Another set of knot invariants can be derived from the complement of the knot in the three-dimensional sphere $\mathbb{S}^3$. This includes the knot group which is defined as the fundamental group of the knot complement. In 1989, Cameron Gordon and John Luecke proved in [5] that the knot complement is a complete invariant. More precisely, if we have two unoriented knots in $\mathbb{S}^3$ and there is an orientation preserving homeomorphism between their complements, then they are equivalent as unoriented knots. Unfortunately the knot group loses some significant properties and it is not a complete invariant [13].

1.3 The Knot Quandle

A knot quandle, another type of algebra that can be naturally associated with a knot, was first introduced by Joyce in [12] and Matveev in [14], who discovered it in 1982 independently of each other.

A quandle is a binary algebra $(Q, *)$ which is

- left distributive, i.e. $x * (y * z) = (x * y) * (x * z)$;
- left quasigroup, i.e. $\forall x, z \in Q$ there is a unique $y \in Q$ such that $x * y = z$;
- idempotent, i.e. $x * x = x$.

Given a knot diagram D with the set of arcs R, we can construct a quandle in a following way: we label all the arcs in the diagram and define the relations as $a * b = c$ where the arcs are marked according to Figure 1.3. Note that these relations depend on the orientation of the overcrossing arc.

$$Q_D = \langle R, a * b = c \text{ for every crossing} \rangle$$

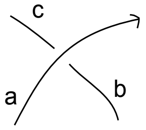

Figure 1.3: Knot quandle relation

We will show that this quandle is independent of the diagram from which it was constructed and therefore it is a knot invariant.

Let us take a diagram of a knot, and perform a Reidermeister move of type one. The two knot diagrams differ only in the small part shown in Figure 1.4, the generators and relations are identical except for a, b and c. But the crossing in the first picture gives us a relation $a * a = b$, and idempotency implies $a = b$. So the mapping that sends a to c and is identity everywhere else must be a quandle isomorphism.

As for type two, we can see from the picture that $a * b = c$ and $a * d = c$. But from the left quasigroup property, we find that $b = d$, and further, that if we define the mapping $a \mapsto e$, $b \mapsto f$ and $c \mapsto e * f$, we clearly get isomorphic quandles.

Type three is not much more complicated: we define a mapping of ordered sets $\varphi : \{a, b, c, d, e, f\} \mapsto \{g, h, i, j, h * j, l\}$ and we will show that it is a quandle isomorphism. The three crossings give us the following equations:

$$\begin{array}{ccc} a * b = c & a * e = f & b * d = e \\ g * h = i & g * j = k & i * k = l \end{array}$$

We can see that $\varphi(a * b) = \varphi(a) * \varphi(b)$ and

$$\varphi(b) * \varphi(d) = h * j = \varphi(e).$$

For the last equation, we use the left distributivity of the quandle:

$$\varphi(a) * \varphi(e) = g * (h * j) = (g * h) * (g * j) = i * k = l = \varphi(f).$$

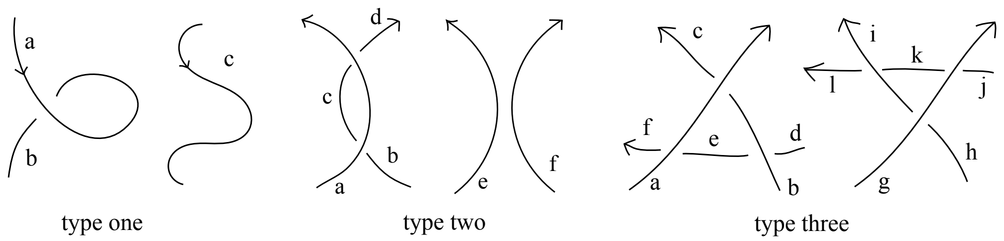

Figure 1.4: Quandle relations corresponding to Reidemeister moves

Should the orientation of the overstrands be opposite, they would be described analogously.

The knot quandle is a very powerful invariant. In fact, Joyce in [12] and Matveev in [14] proved in 1982 that the knot quandle is a complete invariant up to orientation: two diagrams give isomorphic quandles if only if the diagrams represent the same knot regardless of orientation. The problem remains that it is difficult to decide whether or not two quandles are isomorphic.

1.4 Relation of the Knot Quandle to Some Classical Invariants

Even though the isomorphism problem of knot quandles is difficult, there are other weaker (but still useful) knot invariants which can be derived from the knot quandle, and which are easier to calculate. We will show how the knot quandle relates to the knot group and the Alexander module.

Let us define a group: again we take the set of arcs in the knot diagram R and we define the relations at every crossing as $bab^{-1} = c$, where $a * b = c$ is the quandle relation for the same crossing. Since the knot quandle is an invariant, the group is independent of the chosen knot diagram as well. In fact, it is the same as the knot group defined earlier, the fundamental group of the knot complement, and this is called the Wirtinger presentation of the knot group. More about knot groups can be found for example in [13].

Another invariant that can be deduced from the knot quandle is the Alexander module. The Alexander module is a module over the Laurent polynomial ring $\mathbb{Z}[t, t^{-1}]$. The generators are the same as the generators of the knot quandle, and the relations in the form

$$a_k = a_i * a_j = (1 - t) a_i + t a_j$$

are given by each crossing. This gives us a set of linear equations where the variables correspond to the arcs $a_1, \ldots, a_n$ and the equations correspond to the crossings:

$$(1 - t) a_i + t a_j - a_k = 0.$$

The matrix given by these equations is the presentation matrix of the Alexander module. The ideal generated by the determinants of all submatrices of the size $n - 1$ is called the *Alexander ideal* and it is a knot invariant. This ideal is always principal and its generator is the Alexander polynomial. Details can be found in Alexander's article [2] or in the book by Manturov [13].

Chapter 2

Quandles

We will now have a closer look at quandles themselves. First we must introduce some basic definitions and properties of quandles.

2.1 Basic Properties and Examples

The left translation by x, denoted by L_x, is a mapping on Q such that $L_x(y) = x * y$. It follows from left distributivity of $*$ that each left translation is an endomorphism of Q, and from the left quasigroup property that it is a bijection. Therefore each L_x is an automorphism of Q.

There are two subgroups of $\mathrm{Aut}(Q)$ associated with each quandle that we will be using throughout the text. The first is the left multiplication group

$$\mathrm{LMlt}(Q) = \langle L_x \ : \ x \in Q \rangle$$

and the second is the group of displacements

$$\mathrm{Dis}(Q) = \langle L_x L_y^{-1} \ : \ x, y \in Q \rangle.$$

Natural examples of quandles come from groups:

- **Conjugation quandles**. If we take any group G and define the binary operation
$$a * b = aba^{-1},$$
it can be easily confirmed that the resulting structure is a quandle.

- **Affine quandles**. Let $(A, +)$ be an abelian group and $k \in Aut(A)$. Then $(A, *_k)$ with the operation
$$x *_k y = (1 - k)(x) + k(y)$$
is referred to as *affine* or *Alexander* quandle. We will denote it by $Q = \mathrm{Aff}(A, k)$.

- **Galkin quandles**: let G be any group, $H \leq G$ and $\varphi \in \mathrm{Aut}(G)$ such that $\varphi \restriction_H = \mathrm{id}$. Then $\mathrm{Gal}(G, H, \varphi)$ with the operation defined as
$$xH * yH = x\varphi\left(x^{-1}\right)\varphi(y)H$$
is a quandle. We will say that a quandle Q has a Galkin representation if there exist G, H and φ such that $Q = \mathrm{Gal}(G, H, \varphi)$. We can see immediately that $\mathrm{Aff}(A, k) = \mathrm{Gal}(A, 1, k)$, so every affine quandle is Galkin.

- **Projection quandles**. Any set with the operation

$$a * b = b$$

is a quandle. A projection quandle of size m will be denoted by $\mathrm{Proj}\,(m)$.

We say that a quandle is *connected* if $\mathrm{LMlt}\,(Q)$ is transitive on Q; i.e. for every $x, y \in Q$, there exists $f \in \mathrm{LMlt}\,(Q)$ such that $f\,(x) = y$. The following results have been presented in [9].

Proposition 1. *The orbits of the action of* $\mathrm{Dis}\,(Q)$ *on* Q *are the same as the orbits of* $\mathrm{LMlt}\,(Q)$.

Proof. The proof can be found in [9].

□

It is a corollary of the previous proposition that Q is connected if and only if $\mathrm{Dis}\,(Q)$ is transitive on Q.

Connected quandles have a natural Galkin representation, see [9] if Q is a connected quandle, we can find a Galkin representation of Q on the group $\mathrm{LMlt}\,(Q)$ (*canonical representation*) or on $\mathrm{Dis}\,(Q)$ (*minimal representation*).

A quandle Q is called *latin* if the equation $x * a = b$ has a unique solution for every $a, b \in Q$; i.e., if the right translations are permutations as well. Clearly, every latin quandle is connected. The converse is true for finite affine quandles; it will come as a Corollary 6 in the next chapter.

A quandle is *medial* if $(x * y) * (u * v) = (x * u) * (y * v)$.

Proposition 2. *1. Every affine quandle is medial;*

2. Every connected medial quandle is affine;

3. Quandle Q *is medial if an only if* $\mathrm{Dis}\,(Q)$ *is abelian.*

Proof.
(1) It is easy to check that every affine quandle is medial:

$$\begin{aligned}(x * y) * (u * v) &= (1-k)\left((1-k)\,(x) + k\,(y)\right) + k\left((1-k)\,(u) + k\,(v)\right)\\ &= (1-k)^2\,(x) + (1-k)\,(k\,(y)) + k\left((1-k)\,(u)\right) + k^2\,(v)\\ &= (1-k)\left((1-k)\,(x) + k\,(u)\right) + k\left((1-k)\,(y) + k\,(v)\right)\\ &= (x * u) * (y * v)\end{aligned}$$

because the endomorphisms k and $1-k$ commute:

$$\begin{aligned}(1-k)\,(k\,(x)) &= k\,(x) - k^2\,(x)\\ k\left((1-k)\,(x)\right) &= k\,(x) - k^2\,(x)\,.\end{aligned} \tag{2.1}$$

(2) and (3) The complete proof can be found in [9]. The fact every connected medial quandle is affine is a corollary of the fact that a quandle Q is medial if and only if $\mathrm{Dis}\,(Q)$ is abelian; and further providing that we can find a Galkin representation of Q on the group $\mathrm{Dis}\,(Q)$.

□

2.2 Coloring Knots by Quandles

In the first chapter we mentioned tricolorability of a knot as a knot invariant. It is in fact the simplest form of coloring a knot by a non-trivial quandle, $Q = \text{Aff}(\mathbb{Z}_3, k)$, where k is multiplication by 2. In general, this quandle Q is a member of the class of affine quandles that are called dihedral quandles: $Q = \text{Aff}(\mathbb{Z}_n, -1)$. The quandle operation is then $a * b = 2a - b$; we can imagine the operation as a reflection of y by x.

We can extend the notion of coloring knots by three colors to as many colors as there are arcs in the knot diagram. Let us consider a diagram D_K of the knot K. The set of arcs in the diagram is marked R. We define a set of "colors" C, a binary algebra $C = (C, *)$, and a mapping $c : R \to C$ that assigns a color $c(\alpha)$ to each $\alpha \in R$ such that

$$c(\alpha) * c(\beta) = c(\gamma)$$

as in Figure 1.3 on page 8: travelling on the arc α according to its orientation, we pass β on the right side and γ on the left. The function c is called a coloring of D by C. It is easy to show that the number of all colorings of D by C is a knot invariant if and only if C is a quandle. It is denoted by $\text{Col}_C(K)$; and in fact, it is true that

$$\text{Col}_C(K) = |\,\text{Hom}(Q(K), C)\,|$$

where $Q(K)$ denotes the knot quandle of K.

Computing the number of colorings by finite quandles is relatively easy: more information and results can be found on the website [20].

2.3 The Alexander Invariant

When we derived the Alexander invariant from the knot quandle, we assigned a relation to each crossing that resembles the operation of affine quandles. So now, let c be a coloring of a knot diagram by an affine quandle. We know that the equation for each crossing are in the form

$$(1-k)(c(\alpha)) + k(c(\beta)) = c(\gamma)$$

and if we look at them as equations with coefficients in $\mathbb{Z}[k]$, they correspond to the relations of the Alexander module. Now it is clear that for an affine quandle Q and a knot K we can determine $\text{Col}_Q(K)$ solely from the Alexander invariant. Detailed explanation and proof can be found in article by Inoue [10].

Chapter 3

Affine Quandles

3.1 Basic Properties

The left multiplication group and even more so the group of displacements of affine quandles behave very nicely; together with the abelian group A, they give us a complete characterization of affine quandles. First we will have a closer look at the left translations, and then we will state the characterization theorem.
The left translation by $a \in Q$ is of the form

$$L_a(x) = (1-k)(a) + k(x)$$

which immediately yields that $L_0 = k$, and

$$L_a = L_b \Leftrightarrow \exists x \in Q \;\; L_a(x) = L_b(x) \Leftrightarrow a - b \in \operatorname{Ker}(1-k). \tag{3.1}$$

Theorem 3. *Let $(Q, *)$ be a quandle. Then Q is affine if and only if there exists an abelian group $A = (Q, +)$ such that*

- $\operatorname{LMlt}(Q) \leq \operatorname{Aff}(A) = \{x \mapsto c + f(x) \;:\; c \in A,\; f \in \operatorname{Aut}(A)\}$*;*
- $\operatorname{Dis}(Q) \leq \operatorname{Mlt}(A) = \{x \mapsto c + x \;:\; c \in A\}$*.*

Proof. Let Q be an affine quandle with the underlying group A and $k \in \operatorname{Aut}(A)$. Then each left translation on Q is of the form

$$L_a(x) = (1-k)(a) + k(x),$$

Since $(1-k)(a)$ is a constant in A and $k \in \operatorname{Aut}(A)$, all generators of $\operatorname{LMlt}(Q)$ are affine mappings on A. Therefore $\operatorname{LMlt}(Q)$ forms a subgroup of $\operatorname{Aff}(A)$.
As for the group of displacements, we have

$$L_a L_b^{-1}(x) = (1-k)(a-b) + x$$

which is a translation on A by the constant $(1-k)(a-b)$. Since $\operatorname{Dis}(Q)$ is the group generated by these mappings, it must be a subgroup of $\operatorname{Mlt}(A)$.

Conversely, let A be an abelian group which satisfies the given conditions. Every left translation on Q is an affine mapping on A, which means that for every $x \in Q$ there exist $a_x \in A$ and $f_x \in \mathrm{Aut}(A)$ such that $L_x(y) = a_x + f_x(y)$. From idempotency of the quandle operation, we get

$$L_x(x) = x = a_x + f_x(x)$$
$$a_x = (1 - f_x)(x)$$

and see that the left translations take a similar form to affine quandles :

$$L_x(y) = (1 - f_x)(x) + f_x(y)$$

Now if we show that the automorphisms f_x are actually the same for every $x \in Q$, the proof is complete. From above, we have

$$L_x L_y^{-1}(z) = a_x - f_x f_y^{-1}(a_y) + f_x f_y^{-1}(z).$$

We know that $\mathrm{Dis}(Q) \leq \mathrm{Mlt}(A)$. So for every $L_x L_y^{-1} \in \mathrm{Dis}(Q)$, there is a mapping $g \in \mathrm{Mlt}(A)$, $g : x \mapsto c + x$ such that $g = L_x L_y^{-1}$; thus for every $x, y, z \in Q$

$$f_x f_y^{-1}(z) = z \quad \Rightarrow \quad f_x = f_y$$

which is what we needed to show.

□

Note 4. Every abelian group A is isomorphic to its group of translations $\mathrm{Mlt}(A)$ where the element $a \in A$ corresponds to the translation by a. Just now we showed that for an affine quandle $Q = \mathrm{Aff}(A, k)$, the group of displacements is a subgroup of $\mathrm{Mlt}(A)$, and in the proof we saw that

$$\mathrm{Dis}(Q) = \{L_x L_0^{-1} : x \in Q\} = \{x \mapsto x + c : c \in \mathrm{Im}(1 - k)\} \simeq \mathrm{Im}(1 - k). \quad (3.2)$$

Note that this means that the size of $\mathrm{Dis}(Q)$ corresponds exactly to the number of different left translations in Q, since L_x is determined by the value of $(1 - k)(x)$.

We know that $\mathrm{Dis}(Q) \leq \mathrm{LMlt}(Q) \leq \mathrm{Aut}(Q)$ for any quandle. It is easy to see that for affine quandles, any translation $\varphi_x : a \mapsto x + a$ is a quandle automorphism (i.e., $\mathrm{Mlt}(A) \leq \mathrm{Aut}(Q)$):

$$\varphi_x(a) * \varphi_x(b) = (1 - k)(x + a) + k(x + b) = x + (1 - k)(a) + k(b) = \varphi_x(a * b)$$

which means that φ_x is a quandle endomorphism. It is a permutation since it is a well known fact that every group translation is a permutation.

A quandle is connected when the action of $\mathrm{Dis}(Q)$ on Q is transitive. For quandles that are not connected, it is interesting to look at the orbits of this action, $Q_x = \{\alpha(x) : \alpha \in \mathrm{Dis}(Q)\}$. For an affine quandle $Q = \mathrm{Aff}(A, k)$, we know that every mapping in $\mathrm{Dis}(Q)$ is a translation by an element of $\mathrm{Im}(1 - k)$ in the group A, hence the orbits correspond to the cosets of $\mathrm{Im}(1 - k)$ in A:

$$Q_x = \{x + d : d \in \mathrm{Im}(1 - k)\} = x + \mathrm{Im}(1 - k) \quad (3.3)$$

and since $\mathrm{Im}(1 - k) \simeq \mathrm{Dis}(Q)$ by equation (3.2), we know that

$$|Q_x| = |\,\mathrm{Dis}(Q)\,| \quad (3.4)$$

for every $Q_x \subseteq Q$. We will keep that in mind while investigating the following claims.

Proposition 5. *Let $Q = \operatorname{Aff}(A, k)$ be an affine quandle. Then for every $x, y \in Q$*

1. $k(Q_x) = Q_x$ *and* $Q_x \leq Q$;
2. $Q_x \simeq \operatorname{Aff}\left(\operatorname{Im}(1-k), k\restriction_{\operatorname{Im}(1-k)}\right)$;
3. *either* $(1-k)Q_x = (1-k)Q_y$ *or* $(1-k)Q_x \cap (1-k)Q_y = \emptyset$.

Proof.
(1) Since $d_x = (1-k)(x) \in \operatorname{Im}(1-k)$, we have

$$k(x) = x - d_x \in Q_x$$

and $k(Q_x) \subseteq Q_x$. This is true for every $Q_x \subseteq Q$, Q is a union of Q_x and k is a bijection, hence it must be true that $k(Q_x) = Q_x$. By equality (3.3), $Q_x = x + \operatorname{Im}(1-k)$, thus Q_x is closed under the quandle operation given by k because

$$(x+a) *_k (x+b) = x + (1-k)(a) + k(b) \in x + \operatorname{Im}(1-k).$$

(2) Let again $\varphi_x : \operatorname{Im}(1-k) \to Q_x$ be the translation by x. It is a quandle homomorphism and clearly, φ_x is onto from the definition of Q_x. It is also injective, since it is a translation in a group. Therefore φ_x is a quandle isomorphism.
(3) Every $Q_x = x + \operatorname{Im}(1-k)$ is a coset of $\operatorname{Im}(1-k)$ in A and

$$(1-k)Q_x = (1-k)(x) + \operatorname{Im}(1-k)^2$$

is a coset of $\operatorname{Im}(1-k)^2$ in $\operatorname{Im}(1-k)$; and cosets in quotient groups are either disjoint or identical.

$\square$

Corollary 6. *An affine quandle $Q = (A, k)$ is connected if and only if $\operatorname{Im}(1-k) = A$; i.e., $1-k$ is onto A. Every finite affine quandle is latin.*

Proof. This is a direct corollary to Q being connected when the action of $\operatorname{Dis}(Q)$ is transitive on Q and $\operatorname{Im}(1-k)$ being an orbit of $\operatorname{Dis}(Q)$. A surjective endomorphism of a finite quandle is an automorphism, so the equation $x * a = b$ has the unique solution

$$x = (1-k)^{-1}(b - k(a)),$$

which confirms that every finite connected affine quandle is latin.

$\square$

As we can see, $\operatorname{Im}(1-k)$ carries much of the information about the quandle. It is isomorphic to $\operatorname{Dis}(Q)$ and the quandle $\operatorname{Aff}\left(\operatorname{Im}(1-k), k\restriction_{\operatorname{Im}(1-k)}\right)$ is isomorphic to every orbit of the action of $\operatorname{Dis}(Q)$ on Q.

Our goal is to show that the knowledge of the group $\operatorname{Im}(1-k)$, the restriction $k\restriction_{\operatorname{Im}(1-k)}$ and a certain numerical value related to the number of orbits of $\operatorname{Dis}(Q)$ determines the quandle uniquely up to isomorphism.

To conclude this section we should point out one important fact about finite affine quandles: while examining finite affine quandles, it is sufficient to look at quandles of size p^n where p is a prime number. This is because by the fundamental theorem of finite abelian groups, every finite abelian group can be expressed as a product of cyclic groups of prime power order; and for two groups A and B such that their orders are coprime,

$$\mathrm{Aut}\left(A \times B\right) \simeq \mathrm{Aut}\left(A\right) \times \mathrm{Aut}\left(B\right).$$

So if we have a finite affine quandle whose size is not a prime power, it can be expressed as a direct product of finite affine quandles of prime power order [6].

Example 1. We will take a quandle with 16 elements, $Q = \mathrm{Aff}\left(\mathbb{Z}_4 \times \mathbb{Z}_2^2, k\right)$ where $k = \left(\begin{smallmatrix} 1 & 2 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$.

x	$(0,0,0)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$
$k(x)$	$(0,0,0)$	$(0,0,1)$	$(2,1,0)$	$(2,1,1)$	$(1,1,0)$	$(1,1,1)$	$(3,0,0)$	$(3,0,1)$
$(1-k)(x)$	$(0,0,0)$	$(0,0,0)$	$(2,0,0)$	$(2,0,0)$	$(0,1,0)$	$(0,1,0)$	$(2,1,0)$	$(2,1,0)$
x	$(2,0,0)$	$(2,0,1)$	$(2,1,0)$	$(2,1,1)$	$(3,0,0)$	$(3,0,1)$	$(3,1,0)$	$(3,1,1)$
$k(x)$	$(2,0,0)$	$(2,0,1)$	$(0,1,0)$	$(0,1,1)$	$(3,1,0)$	$(3,1,1)$	$(1,0,0)$	$(1,0,1)$
$(1-k)(x)$	$(0,0,0)$	$(0,0,0)$	$(2,0,0)$	$(2,0,0)$	$(0,1,0)$	$(0,1,0)$	$(2,1,0)$	$(2,1,0)$

Table 3.1: Q with the endomorphisms k and $1-k$

We can see that

$$\mathrm{Im}\left(1-k\right) = \left\{\left(0,0,0\right), \left(2,0,0\right), \left(0,1,0\right), \left(2,1,0\right)\right\} = \left\{0,2\right\} \times \left\{0,1\right\} \times \left\{0\right\} \simeq \mathbb{Z}_2^2.$$

It is clearly isomorphic to the group $\mathbb{Z}_2^2$. There are four cosets of $\mathrm{Im}\left(1-k\right)$ in $\mathbb{Z}_4 \times \mathbb{Z}_2^2$: $\mathrm{Im}\left(1-k\right)$, $Q_{(1,0,0)}$, $Q_{(0,0,1)}$ and $Q_{(1,0,1)}$. The mappings in $\mathrm{Dis}\left(Q\right)$ are identity and

$$\begin{aligned} L_{(0,1,0)}L_{(0,0,0)}^{-1} &: x \mapsto \left(1-k\right)\left(\left(0,1,0\right)\right) + x = \left(2,0,0\right) + x \\ L_{(1,0,0)}L_{(0,0,0)}^{-1} &: x \mapsto \left(1-k\right)\left(\left(1,0,0\right)\right) + x = \left(0,1,0\right) + x \\ L_{(1,1,0)}L_{(0,0,0)}^{-1} &: x \mapsto \left(1-k\right)\left(\left(1,1,0\right)\right) + x = \left(2,1,0\right) + x \end{aligned}$$

3.2 Symmetries and Decomposition

First, we will prove a simple lemma from group theory.

Lemma 7. *Let $G \geq K \geq H$ be groups such that K and H are subgroups of G. Then*

$$\left[G : H\right] = \left[G : K\right] \cdot \left[K : H\right].$$

Proof. Let us consider a transversal T of G/K and define a mapping ψ as

$$\psi : aH \mapsto \left(aK, g^{-1}aH\right), \quad g \in T \text{ such that } aH \subseteq gK.$$

Such $g \in T$ always exists because $H \leq K$, and it is uniquely determined by the transversal. Because $aH \subseteq gK$ there exists $k \in K$ such that $a = gk$, so

$g^{-1}aH = g^{-1}gkH = kH \subseteq K$ and $g^{-1}aH \in K/H$.
We will show that this mapping is a bijection. If we have $a, b \in G$ such that $aK = bK = gK$ where $g \in T$ and $g_a^{-1}aH = g_b^{-1}bH$, $aK = bK$ if and only if $g_a = g_b = g$ and

$$g^{-1}aH = g^{-1}bH \Leftrightarrow \left(g^{-1}b\right)^{-1} g^{-1}a \in H \Leftrightarrow b^{-1}a \in H \Leftrightarrow aH = bH$$

showing that ψ is well defined and injective. It is also onto because for every $(aK, bH) \in H/K \times K/H$, there exists $g \in T$ such that $aK = gK$ and $gbH \subseteq aK$ so

$$\psi\left(gbH\right) = \left(gbK, g^{-1}gbH\right) \stackrel{b \in K}{=} \left(aK, bH\right).$$

□

For an affine quandle $Q = (A, k)$, we define

$$m\left(Q\right) = \left[\mathrm{Ker}\left(1-k\right) : \mathrm{Im}\left(1-k\right) \cap \mathrm{Ker}\left(1-k\right)\right]$$

We will call a quandle Q such that $m\left(Q\right) = 1$ an *essential quandle*. Note that $m\left(Q\right) = 1$ is equivalent with $\mathrm{Ker}\left(1-k\right) \subseteq \mathrm{Im}\left(1-k\right)$. We will show that this number is a very important property of affine quandles. But first, let us give an alternative definition of an essential quandle.

Lemma 8. *Let $Q = \mathrm{Aff}\left(A, k\right)$ be an affine quandle. Then Q is essential if and only if $\left(1-k\right) Q_x \cap \left(1-k\right) Q_y = \emptyset$ for every $Q_x \neq Q_y \subseteq Q$.*

Proof. Let $Q_x, Q_y \subseteq Q$ be arbitrary orbits in Q. By Proposition 5, the sets $\left(1-k\right) Q_x, \left(1-k\right) Q_y$ are either identical or disjoint. If they are disjoint for any $Q_x \neq Q_y$, it means that $\left(1-k\right)\left(x\right) = \left(1-k\right)\left(y\right)$ implies $y \in Q_x$, and that is equivalent to

$$\left(y - x \in \mathrm{Ker}\left(1-k\right) \Rightarrow y - x \in \mathrm{Im}\left(1-k\right)\right) \Leftrightarrow \mathrm{Ker}\left(1-k\right) \subseteq \mathrm{Im}\left(1-k\right),$$

so Q is an essential quandle.
On the other hand, if we have an essential quandle and $\left(1-k\right) Q_x = \left(1-k\right) Q_y$, then there exists $z \in Q_y$ such that $\left(1-k\right)\left(x\right) = \left(1-k\right)\left(z\right)$. That means that $z - x \in \mathrm{Ker}\left(1-k\right) \subseteq \mathrm{Im}\left(1-k\right)$, so $z \in Q_x$ and $Q_x = Q_y$.

□

Example 2. Let us have a look at the quandle Q from Example 1. We can see that

$$\mathrm{Ker}\left(1-k\right) = \left\{\left(0,0,0\right), \left(2,0,0\right), \left(0,0,1\right), \left(2,0,1\right)\right\} = \left\{0,2\right\} \times \left\{0\right\} \times \left\{0,1\right\}$$

which in turn indicates that $\mathrm{Im}\left(1-k\right) \cap \mathrm{Ker}\left(1-k\right) = \left\{\left(0,0,0\right), \left(2,0,0\right)\right\}$ and $m\left(Q\right) = 2$.

Proposition 9. *Let $Q = \mathrm{Aff}\left(A, k\right)$ be an affine quandle. Then*

1. *the number of orbits of $\mathrm{Dis}\left(Q\right)$ is $m\left(Q\right) \cdot \left[A : \mathrm{Ker}\left(1-k\right) \cdot \mathrm{Im}\left(1-k\right)\right]$;*

2. $|Q| = m(Q) \cdot [A : \mathrm{Ker}(1-k) \cdot \mathrm{Im}(1-k)] \cdot |\,\mathrm{Im}(1-k)\,|$.

Proof.
(1) By the second isomorphism theorem,

$$\mathrm{Ker}(1-k) \,/\, \mathrm{Ker}(1-k) \cap \mathrm{Im}(1-k) \simeq \mathrm{Ker}(1-k) \cdot \mathrm{Im}(1-k) \,/\, \mathrm{Im}(1-k)$$

so $m(Q) = [\mathrm{Ker}(1-k) \cdot \mathrm{Im}(1-k) : \mathrm{Im}(1-k)]$. The number of orbits of $\mathrm{Dis}(Q)$ is $[A : \mathrm{Im}(1-k)]$ because the orbits are cosets of $\mathrm{Im}(1-k)$ in A. So we can apply Lemma 7 to the groups $A \geq \mathrm{Im}(1-k) \cdot \mathrm{Ker}(1-k) \geq \mathrm{Im}(1-k)$ and we obtain

$$\begin{aligned}[A : \mathrm{Im}(1-k)] &= [A : \mathrm{Ker}(1-k) \cdot \mathrm{Im}(1-k)] \cdot [\mathrm{Ker}(1-k) \cdot \mathrm{Im}(1-k) : \mathrm{Im}(1-k)] \\ &= [A : \mathrm{Ker}(1-k) \cdot \mathrm{Im}(1-k)] \cdot m(Q)\end{aligned}$$

(2) Clear from $|A| = [A : \mathrm{Im}(1-k)] \cdot |\,\mathrm{Im}(1-k)\,|$ and (1).

□

For finite quandles we can derive a formula that is nicer and easier to work with since we do not have to consider the group $\mathrm{Ker}(1-k) \cdot \mathrm{Im}(1-k)$, a product which does not naturally arise when working with affine quandles:

Proposition 10. *Let $Q = \mathrm{Aff}(A, k)$ be a finite affine quandle. Then*

1. *the number of orbits of $\mathrm{Dis}(Q)$ is $m(Q) \cdot \dfrac{|\,\mathrm{Im}(1-k)\,|^2}{|\,\mathrm{Im}(1-k)^2\,|}$;*

2. $|Q| = m(Q) \cdot \dfrac{|\,\mathrm{Im}(1-k)\,|^2}{|\,\mathrm{Im}(1-k)^2\,|}$.

Proof. (1) Since $Q = \mathrm{Aff}(A, k)$ and $1 - k \in \mathrm{End}(A)$, the first isomorphism theorem gives us

$$|Q| = |\,\mathrm{Ker}(1-k)\,| \cdot |\,\mathrm{Im}(1-k)\,|$$

and since all the orbits are isomorphic to $\mathrm{Im}(1-k)$ by Proposition 5, the number of orbits is $|\,\mathrm{Ker}(1-k)\,|$.

$$\begin{aligned}|\,\mathrm{Ker}(1-k)\,| &= \frac{|\,\mathrm{Ker}(1-k)\,|}{|\,\mathrm{Im}(1-k) \cap \mathrm{Ker}(1-k)\,|} \cdot |\,\mathrm{Im}(1-k) \cap \mathrm{Ker}(1-k)\,| \\ &= m(Q) \cdot |\,\mathrm{Im}(1-k) \cap \mathrm{Ker}(1-k)\,| \\ &= m(Q) \cdot \frac{|\,\mathrm{Im}(1-k)\,|}{|\,\mathrm{Im}(1-k)^2\,|}\end{aligned}$$

This works because $(1-k) \restriction_{\mathrm{Im}(1-k)}$ is an endomorphism of $\mathrm{Im}(1-k)$, so again by the first isomorphism theorem

$$|\,\mathrm{Im}(1-k)\,| / |\,\mathrm{Im}(1-k) \cap \mathrm{Ker}(1-k)\,| = |\,\mathrm{Im}(1-k)^2\,|.$$

(2) Immediately from the previous statement and the fact that all the orbits are of size $|\,\mathrm{Im}(1-k)\,|$.

□

Example 3. For Q from Example 1 on page 16, $\operatorname{Im}(1-k)^2 = \{(0,0,0),(2,0,0)\}$, so Proposition 10 confirms the results calculated in the example:

$$\begin{aligned} \text{number of orbits } &= m(Q) \cdot \frac{\operatorname{Im}(1-k)}{\operatorname{Im}(1-k)^2} = 2 \cdot 2 = 4; \\ |Q| &= 4 \cdot |\operatorname{Im}(1-k)| = 16. \end{aligned}$$

Now let $Q = \operatorname{Aff}(A,k)$ be an affine quandle. We consider the following sets:

- a transversal I of $\operatorname{Im}(1-k) / \operatorname{Im}(1-k)^2$;
- a transversal X of $A/\operatorname{Im}(1-k)$ such that $(1-k)X = I$;
- $X' \subseteq X$ such that for every $a \in I$ there is exactly one $x \in X'$ such that $(1-k)(x) = a$; i.e., $1-k$ is a bijection of X' and I.

We will call any set X' such that $1-k$ is a bijection from X' to a transversal of $\operatorname{Im}(1-k) / \operatorname{Im}(1-k)^2$ an *essential set* of Q. The set

$$Q' = \bigcup_{x \in X'} Q_x$$

is clearly a subquandle of Q since it is a union of orbits, and since for every two orbits $Q_x * Q_y \subseteq Q_y$. We will call it an *essential subquandle* of Q.

Note 11. There always exists such X and X' because $1-k$ maps the cosets of $A/\operatorname{Im}(1-k)$ to the cosets of $\operatorname{Im}(1-k) / \operatorname{Im}(1-k)^2$. Also notice that:

- if $0 \in Q'$, then $\operatorname{Im}(1-k) \subseteq Q'$ because $Q_0 = \operatorname{Im}(1-k)$;
- $\operatorname{Im}(1-k) = \operatorname{Im}((1-k)\restriction_{Q'})$ because we chose X' such that $(1-k)X' = I$ and Q' is a union of the cosets $x + \operatorname{Im}(1-k)$ for $x \in X'$;
- $\operatorname{Dis}(Q) = \operatorname{Dis}(Q')$, since $\operatorname{Dis}(Q)$ is generated by the mappings $L_x L_y^{-1}$, $x, y \in Q$, the left translation L_x is determined by the value $(1-k)(x)$ and $\operatorname{Im}(1-k) = \operatorname{Im}((1-k)\restriction_{Q'})$, so $\{L_x : x \in Q\} = \{L_y : y \in Q'\}$.

Example 4. Again we will look at the quandle Q from Example 1 on page 16. We take $I = \{(0,0,0),(0,1,0)\}$ and we can put

$$\begin{aligned} X &= \{(0,0,0),(1,0,0),(0,0,1),(1,0,1)\} \\ X' &= \{(0,0,0),(1,0,0)\} \\ Q' &= \operatorname{Im}(1-k) \cup Q_{(1,0,0)}. \end{aligned}$$

Lemma 12. *Let $Q = \operatorname{Aff}(A,k)$ be an affine quandle. Then $Q' \leq Q$ is an essential subquandle of Q if and only if $\operatorname{Im}(1-k) = \operatorname{Im}((1-k)\restriction_{Q'})$ and $(1-k)Q_x \cap (1-k)Q_y = \emptyset$ for every $Q_x \neq Q_y \subseteq Q'$.*

Proof. Let Q' be an essential quandle. We showed that $\operatorname{Im}(1-k) = \operatorname{Im}((1-k)\restriction_{Q'})$ for every essential subquandle, and from Proposition 5 we know that either $(1-k)Q_x = (1-k)Q_y$ or $(1-k)Q_x \cap (1-k)Q_y = \emptyset$. But we defined the essential set X' such that there is exactly one orbit Q_x, $x \in X'$ such that $(1-k)Q_x = a + \operatorname{Im}(1-k)^2$ where $a \in (1-k)X'$, so $(1-k)Q_x \cap (1-k)Q_y = \emptyset$

for every $x, y \in X'$, $x \neq y$.
On the contrary, let I be a transversal of $\operatorname{Im}(1-k) / \operatorname{Im}(1-k)$, X a set of orbit representatives such that $(1-k) X = I$ and $X' = X \cap Q'$. In that case, clearly $(1-k) X' = I$ since $(1-k) Q' = \operatorname{Im}(1-k)$. Now let $x, y \in X'$ be such that $(1-k)(x) = (1-k)(y)$. But we assumed that $(1-k) Q_x \cap (1-k) Q_y = \emptyset$ for every $Q_x \neq Q_y \subseteq Q'$, so $y \in Q_x$ and since both $x, y \in X'$ are orbit representatives, $x = y$, so Q' is an essential subquandle.

$\square$

Note that this lemma gives us an alternative definition of an essential subquandle. It is also clear that if $Q' \leq Q$ is affine, then it is an essential quandle by Lemma 8; i.e., $m(Q') = 1$.

Now we proceed to the most important theorem of this section.

Theorem 13. *Let $Q = \operatorname{Aff}(A, k)$ be an affine quandle and $Q' \leq Q$ an essential subquandle of Q. Then $Q \simeq Q' \times \operatorname{Proj}(m(Q))$.*

Proof. We consider X_0 to be a transversal of $\operatorname{Ker}(1-k) / \operatorname{Im}(1-k) \cap \operatorname{Ker}(1-k)$ and we index the set $X_0 = \{x_i : i < m(Q)\}$. We define a mapping $\varphi : Q' \times \operatorname{Proj}(m(Q)) \to Q$ as follows:

$$\varphi((a, i)) = a + x_i,$$

and we show that it is a quandle isomorphism. Let $(a, i), (b, j) \in Q' \times \operatorname{Proj}(m(Q))$.

$$\begin{aligned}
\varphi((a, i)) * \varphi((b, j)) &= (a + x_i) * (b + x_j) \\
&= (1-k)(a + x_i) + k(b + x_j) \\
&= (1-k)(a) + (1-k)(x_i) + k(b) + k(x_j) \\
&= (1-k)(a) + k(b) + x_j \qquad (3.5) \\
&= \varphi((a * b, j))
\end{aligned}$$

Equality (3.5) holds because $x_i, x_j \in \operatorname{Ker}(1-k)$, and therefore $(1-k)(x_i) = 0$ and $k(x_j) = x_j$.
Now we need to show that φ is a bijection. Let $(a, i), (b, j) \in Q' \times \operatorname{Proj}(m(Q))$ be such that $\varphi((a, i)) = \varphi((b, j))$, i.e. $a + x_i = b + x_j$. It means that

$$x_i - x_j = b - a \in \operatorname{Ker}(1-k) \Rightarrow (1-k)(a) = (1-k)(b).$$

We know that $a, b \in Q'$ and we chose the cosets in Q' in a way that for each $d \in \operatorname{Im}(1-k)$ there is exactly one coset $Q_x \subset Q'$ such that $d \in (1-k) Q_x$. It then follows that there is a coset $Q_x \subset Q'$ such that $a, b \in Q_x$. As above, we have

$$b - a = x_i - x_j \in \operatorname{Im}(1-k),$$

which means that $x_i \in Q_{x_j}$ and since x_i and x_j are coset representatives, we have $x_i = x_j$.
It remains to show that φ is onto; i.e., for every $x \in Q$ there is $a \in Q'$ and $x_i \in X_0$ such that $x = a + x_i$. We take $a' \in Q'$ such that

$$(1-k)(a') = (1-k)(x).$$

It always exists because $\mathrm{Im}\,(1-k) = \mathrm{Im}\,((1-k)\restriction_{Q'})$. Now since $x - a' \in \mathrm{Ker}\,(1-k)$ and X_0 is a transversal of $\mathrm{Ker}\,(1-k) \,/\, \mathrm{Ker}\,(1-k) \cap \mathrm{Im}\,(1-k)$, there is a unique decomposition $x - a' = x_i + b$ where $x_i \in X_0$ and $b \in \mathrm{Ker}\,(1-k) \cap \mathrm{Im}\,(1-k)$. Hence $a' + b \in Q_{a'} \subseteq Q'$ and

$$\varphi\,(b + a', i) = x,$$

so φ is onto.

□

Example 5. We can see that the quandle $Q' \leq Q$ from Example 4 on page 16 is isomorphic to $\mathrm{Aff}\,(\mathbb{Z}_4 \times \mathbb{Z}_2, k')$ where $k = \{(0,1) \mapsto (2,1)\,, (1,0) \mapsto (1,1)\}$; and

$$Q \simeq Q' \times \mathrm{Proj}\,(2)\,.$$

3.3 Enveloping Algebras and Quandles

In Theorem 3 we used the properties of $\mathrm{LMlt}\,(Q)$ and $\mathrm{Dis}\,(Q)$ to define a condition that is sufficient to show that a certain quandle is affine. We still presumed the existence of an underlying abelian group and we used its properties, namely the properties of its translations and affine transformations, to prove that Q is affine. Nevertheless we saw that only some translations and affine transformations correspond to elements of $\mathrm{Dis}\,(Q)$ and $\mathrm{LMlt}\,(Q)$. They are the ones that use the constant from the subgroup $\mathrm{Im}\,(1-k)$.

In this section we define a partial algebra that is in a way similar to abelian groups, but we weaken some of the properties that we expect abelian groups to have. Our goal is to show that we can construct quandles from these structures; and also that these quandles have a lot in common with affine quandles.

Definition 1. Let us define an *enveloping algebra* as a partial algebra $E = (E, +, -, 0, \alpha)$ with a unary operation α, a partial binary operation $+ : \mathrm{Im}\,(\alpha) \times E \to E$, a partial unary operation $- : \mathrm{Im}\,(\alpha) \to \mathrm{Im}\,(\alpha)$ and a constant $0 \in \mathrm{Im}\,(\alpha)$ such that

1. $(\mathrm{Im}\,(\alpha)\,, +, -, 0)$ is an abelian group;
2. the operation $+$ is satisfies partial associativity and $0 \in E$ is the only additive identity: for every $x \in E$ and $a, b \in \mathrm{Im}\,(\alpha)$

   $$(a + b) + x = a + (b + x) \;\text{ and } 0 + x = 0$$

   and if $a + x = x$ for some $a \in \mathrm{Im}\,(\alpha)$, then $a = 0$;
3. α is a endomorphism of E and the mapping $(-\alpha + 1)\restriction_{\mathrm{Im}(\alpha)}$ is an automorphism of $\mathrm{Im}\,(\alpha)$.

Example 6. For any abelian group $A = (A, +, -, 0)$ with $k \in \mathrm{Aut}\,(A)$, $E = (A, +, -, 1-k, 0)$ is an enveloping algebra since $k = 1 - (1-k)$ is an automorphism and we showed in Proposition 5(1) that $k\,(\mathrm{Im}\,(1-k)) = \mathrm{Im}\,(1-k)$, so the restriction to $\mathrm{Im}\,(1-k)$ is an automorphism as well.

Lemma 14. *Let E be an enveloping algebra. The mapping k on E such that $k : x \mapsto -\alpha(x) + x$ is an automorphism of E.*

Note 15. We will write $k = -\alpha + 1$. Notice that k restricted on $\mathrm{Im}(\alpha)$ is the group automorphism $(-\alpha + 1) \restriction_{\mathrm{Im}(\alpha)}$.

Proof. First we will show that $k(a + x) = k(a) + k(x)$ for every $x \in E$ and $a \in \mathrm{Im}(\alpha)$:

$$\begin{aligned} k(a + x) &= -\alpha(a + x) + (a + x) \\ &= -(\alpha(a) + \alpha(x)) + (a + x) && \text{by (3) of Definition 2} \\ &= (-\alpha(a) + a) + (-\alpha(x) + x) && \text{by (2) and (1) of Definition 2} \\ &= k(a) + k(x). \end{aligned}$$

Now we need to show that k is also injective: if $k(x) = k(y)$, then necessarily $x = y$. So let us have $x, y \in B$ such that $(-\alpha + 1)(x) = (-\alpha + 1)(y)$; we can use partial associativity to rewrite the equation into

$$(\alpha(y) - \alpha(x)) + x = y \tag{3.6}$$

and apply α on both sides. From the properties of α and the fact that $\mathrm{Im}(\alpha)$ is an abelian group we can see that

$$\alpha(\alpha(y) - \alpha(x)) = \alpha(y) - \alpha(x)$$

and therefore $\alpha(y) - \alpha(x)$ is in $\mathrm{Ker}\left((-\alpha + 1) \restriction_{\mathrm{Im}(\alpha)}\right)$. Since $(-\alpha + 1) \restriction_{\mathrm{Im}(\alpha)}$ is an automorphism of $\mathrm{Im}(\alpha)$, it follows that $\alpha(y) - \alpha(x) = 0$ and from equality (3.6) we can see that $x = y$.
Next we show that k is also onto: for any $y \in E$, we need to show that there exists $x \in E$ such that $k(x) = y$. We know that $k(y) = -\alpha(y) + y$ and from partial associativity we get

$$y = \alpha(y) + k(y). \tag{3.7}$$

Since $(-\alpha + 1) \restriction_{\mathrm{Im}(\alpha)}$ is an automorphism of $\mathrm{Im}(\alpha)$, there exists $a \in \mathrm{Im}(\alpha)$ such that $(-\alpha + 1)(a) = \alpha(y)$ and we get

$$y = \alpha(y) + k(y) = (-\alpha + 1)(a) + k(y) = k(a + y),$$

therefore k is a bijection on E. □

This lemma gives us a corollary about abelian groups that we will use a little later.

Corollary 16. *Let A be an abelian group and α an endomorphism of A such that $(-\alpha + 1) \restriction_{\mathrm{Im}(\alpha)}$ is an automorphism of $\mathrm{Im}(\alpha)$. Then $-\alpha + 1$ is an automorphism of A.*

Proof. If α is an endomorphism of A, then certainly $-\alpha + 1$ is an endomorphism as well. Clearly, A is an enveloping algebra, therefore by lemma 14, $-\alpha + 1$ is a permutation.

$\square$

We showed that if we define $k = -\alpha + 1$, it is an automorphism of E. We define a binary operation $*$ on E

$$x * y = \alpha(x) + k(y)$$

and we denote $(E, *)$ by $\mathrm{Aff}(E)$.

Lemma 17. *Let E be an enveloping algebra. Then* $\mathrm{Aff}(E)$ *is a medial quandle.*

Proof. Let us denote $Q = \mathrm{Aff}(E)$. Idempotency is clear since by equality (3.7) we know that $\alpha(x) + k(x) = x$. For the left quasigroup property, the element y such that $x * y = z$ for any given $x, z \in Q$ is uniquely determined because

$$\begin{aligned}
\alpha(x) + k(y) = z & \quad \Leftrightarrow \\
-\alpha(x) + (\alpha(x) + k(y)) = -\alpha(x) + z & \quad \Leftrightarrow \text{ (by partial associativity)} \\
k(y) = -\alpha(x) + z & \quad \Leftrightarrow \text{ (k is a bijection)} \\
y = k^{-1}(-\alpha(x) + z).
\end{aligned}$$

Now we show that the mediality law is satisfied; i.e., for every $x, y, u, v \in Q$:

$$(x * y) * (u * v) = (x * u) * (y * v).$$

Before we proceed, we make the observation that

$$\begin{aligned}
k(\alpha(y)) &= -\alpha(\alpha(y)) + \alpha(y) \qquad (3.8)\\
\alpha(k(y)) &= \alpha(-\alpha(y) + y) = -\alpha(\alpha(y)) + \alpha(y)
\end{aligned}$$

which indicates that the mappings α and k commute on E, and $k(\alpha(x)) \in \mathrm{Im}(\alpha)$. So for the mediality law, we have

$$\begin{aligned}
(x * y) * (u * v) &= \alpha(\alpha(x) + k(y)) + k(\alpha(u) + k(v)) \\
&= (\alpha(\alpha(x)) + \alpha(k(y))) + (k(\alpha(u)) + k(k(v))) \\
&= \alpha(\alpha(x)) + \alpha(k(u)) + (k(\alpha(y)) + k(k(v))) \\
&= \alpha(\alpha(x) + k(u)) + k(\alpha(y) + k(v)) \\
&= (x * u) * (y * v).
\end{aligned}$$

We used freely the properties of enveloping algebras and the automorphism k. For the proof of left distributivity, we use the mediality law and idempotency: for every $x, y, z \in Q$

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

which concludes the proof of left distributivity and confirms that Q really is a medial quandle.

$\square$

Let E be an enveloping algebra. We can see that for $a \in \mathrm{Im}(\alpha)$

$$(1 - k)(a) = a - k(a) = a - (-\alpha(a) + a) = \alpha(a) \qquad (3.9)$$

since $\mathrm{Im}(\alpha)$ is an abelian group. We showed in (3.8) that $k(\alpha(x)) \in \mathrm{Im}(\alpha)$; so surely $(\mathrm{Im}(\alpha), *) \leq \mathrm{Aff}(E)$ is an affine quandle $\mathrm{Aff}\left(\mathrm{Im}(\alpha), k\restriction_{\mathrm{Im}(\alpha)}\right)$.

Now we derive properties of $\mathrm{Aff}(E)$ that are analogous to some properties of affine quandles.

Proposition 18. *Let $E = (E, +, -, \alpha, e)$ be an enveloping algebra, $k = -\alpha + 1$ and $Q = \mathrm{Aff}\,(E)$. Then the following statements are true:*

1. $\mathrm{LMlt}\,(Q) = \langle x \mapsto d + k\,(x) \ : \ d \in \mathrm{Im}\,(\alpha)\rangle$*;*
2. $\mathrm{Dis}\,(Q) = \{x \mapsto d + x \ : \ d \in \mathrm{Im}\,(\alpha)\} \simeq \mathrm{Im}\,(\alpha)$*, thus* $Q_x = \mathrm{Im}\,(\alpha) + x$*;*
3. *for every orbit* Q_x*,* $k\,(Q_x) = (Q_x)$*,* $Q_x \leq Q$ *and* $Q_x \simeq \mathrm{Aff}\left(\mathrm{Im}\,(\alpha)\,, k\restriction_{\mathrm{Im}(\alpha)}\right)$*;*
4. *for every orbit* Q_x*, the set* $\alpha\,(Q_x)$ *is a coset of* $\mathrm{Im}\,(\alpha^2)$ *in* $\mathrm{Im}\,(\alpha)$*;*
5. $L_e = k$ *and* $\alpha\,(x) = \alpha\,(y) \Leftrightarrow L_x = L_y \Leftrightarrow$ *there exists* $a \in E$ *such that* $L_x\,(a) = L_y\,(a)$*;*
6. *the mapping* $T_a : x \mapsto a + x$ *is an automorphism of* Q *for every* $a \in \mathrm{Im}\,(\alpha)$*.*

Proof.
(1) Left translations are in the form

$$L_a\,(x) : x \mapsto \alpha\,(a) + k\,(x)$$

and $\mathrm{LMlt}\,(Q)$ is generated by these mappings by definition.
(2) The left division by $b \in E$ is in the form $L_b^{-1}\,(x) = x \mapsto k^{-1}\,(-\alpha\,(b) + x)$, so the generators of $\mathrm{Dis}\,(Q)$ are

$$L_a L_b^{-1}\,(x) = \alpha\,(a) + k\left(k^{-1}\,(-\alpha\,(b) + x)\right) = \alpha\,(a) - \alpha\,(b) + x. \tag{3.10}$$

Since $\mathrm{Im}\,(\alpha)$ is an abelian group, $\alpha\,(a) - \alpha\,(b) \in \mathrm{Im}\,(\alpha)$ for every $a, b \in Q$, so $L_a L_b^{-1}$ is a translation by $\alpha\,(a) - \alpha\,(b)$ in E. The composition is also a translation by an element of $\mathrm{Im}\,(\alpha)$:

$$L_a L_b^{-1} L_c L_d^{-1}\,(x) = \alpha\,(a) - \alpha\,(b) + \alpha\,(c) - \alpha\,(d) + x,$$

and the inverse is $\left(L_a L_b^{-1}\right)^{-1} = L_b L_a^{-1}$. So every mapping in $\mathrm{Dis}\,(Q)$ is in the form $x \mapsto a + x$ where $a \in \alpha\,(x)$. In particular for every $a \in Q$,

$$L_a L_e^{-1} : x \mapsto \alpha\,(a) + x$$

because $\alpha\,(e) = e$ and $\alpha\,(a) - e = \alpha\,(a)$. So clearly $\varphi : a \mapsto (x \mapsto a + x)$ is an isomorphism of the groups $\mathrm{Im}\,(\alpha)$ and $\mathrm{Dis}\,(Q)$, and the orbits of $\mathrm{Dis}\,(Q)$ are the sets $Q_x = \{a + x : a \in \mathrm{Im}\,(\alpha)\} = \mathrm{Im}\,(\alpha) + x$.
(3) Using Lemma 14 on the elements of $k\,(Q_x)$, we get

$$k\,(Q_x) = \{k\,(\alpha\,(a)) + k\,(x)\}.$$

But since $k\,(x) = -\alpha\,(x) + x \in Q_x$, $k\,(\alpha\,(a)) = \alpha\,(k\,(a))$ by equality (3.8) and $\alpha\,(k\,(a)) - \alpha\,(x) \in \mathrm{Im}\,(\alpha)$ because $\mathrm{Im}\,(\alpha)$ is an abelian group, $k\,(Q_x) \subseteq Q_x$. From this it is clear that $Q_x \leq Q$. This is true for every orbit, Q is a disjoint union of the orbits and by Lemma 14, k is a permutation of Q. Hence $k\,(Q_x) = Q_x$ for every $Q_x \leq Q$.
For every orbit Q_x, we define a mapping $\varphi_x : \mathrm{Aff}\left(\mathrm{Im}\,(\alpha)\,, k\restriction_{\mathrm{Im}(\alpha)}\right) \to Q_x$ as $\alpha\,(a) \mapsto \alpha\,(a) + x$. It is a bijection since $Q_x = \mathrm{Im}\,(\alpha) + x$ as proved above; and

we will show that it is a quandle homomorphism. By equality (3.9) we know that for $a \in \mathrm{Im}(\alpha)$, $\alpha(a) = (1-k)(a)$, so

$$\varphi_x((1-k)(\alpha(a)) + k(\alpha(b))) = \alpha^2(a) + k(\alpha(b)) + x$$

and

$$\begin{aligned}\alpha(\varphi_x(\alpha(a))) + k(\varphi_x(\alpha(b))) &= \alpha(\alpha(a)+x) + k(\alpha(b)+x) \\ &= \big(\alpha^2(a) + \alpha(x)\big) + (k(\alpha(b)) + k(x)) \\ &= \alpha^2(a) + k(\alpha(b)) + (\alpha(x) + k(x)) \\ &= \alpha^2(a) + k(\alpha(b)) + x.\end{aligned}$$

We use the partial associativity and the properties of the abelian group $\mathrm{Im}(\alpha)$ freely; the last equality comes from $k = -\alpha + 1$.
(4) Since α is an endomorphism of the enveloping algebra E, and we proved that $Q_x = \mathrm{Im}(\alpha) + x$, $\alpha(Q_x)$ is the coset $\mathrm{Im}(\alpha^2) + \alpha(x)$ of $\mathrm{Im}(\alpha^2)$ in $\mathrm{Im}(\alpha)$.
(5) The first statement and equivalence are plainly a corollary of the fact that $L_a = x \mapsto \alpha(a) + k(x)$ and $\alpha \restriction_{\mathrm{Im}(\alpha)}$ is an endomorphism of the abelian group $\mathrm{Im}(\alpha)$ with the unit e, hence $\alpha(e) = e$ and $e + x = x$ for every $x \in Q$. We have to show the one remaining implication: let $w \in E$ be such that $L_x(w) = L_y(w)$. This means that

$$\alpha(x) + k(w) = \alpha(y) + k(w) \Leftrightarrow \alpha(x) - \alpha(w) + w = \alpha(y) - \alpha(w) + w \Leftrightarrow$$
$$\alpha(x) + w = \alpha(y) + w \Leftrightarrow w = \alpha(x) - \alpha(y) + w \Leftrightarrow \alpha(x) - \alpha(y) = e \Leftrightarrow$$
$$\alpha(x) = \alpha(y) \Leftrightarrow L_x = L_y$$

from the uniqueness of the additive identity on E.
(6) For every $a \in \mathrm{Im}(\alpha)$ there exists $x \in E$ such that $\alpha(x) = a$. Then $T_a = L_x L_e^{-1} \in \mathrm{Dis}(Q)$, therefore it is a quandle automorphism.

□

Definition 2. We will call an enveloping algebra such that $\alpha(Q_x) \cap \alpha(Q_y) = \emptyset$ for every $Q_x \neq Q_y$, Q_x, Q_y orbits of the action of $\mathrm{Dis}(\mathrm{Aff}(E))$, an *essential enveloping algebra.*

Example 7. Let $Q = \mathrm{Aff}(A, k)$ be an affine quandle.

- Let Q be an essential quandle. As in Example 6, $E = (A, +, -, 0, 1-k)$ is an enveloping algebra. By Lemma 8, $(1-k)Q_x \cap (1-k)Q_y = \emptyset$ for every $Q_x \neq Q_y \subseteq Q$. Hence E is an essential enveloping algebra and $\mathrm{Aff}(A, k) = \mathrm{Aff}(E)$ as stated in Lemma 17, since $\alpha = 1-k$ and $-\alpha+1 = -1+k-1 = k$.

- If $m(Q) > 1$, we consider the decomposition from Theorem 13 $Q \simeq Q' \times \mathrm{Proj}(m(Q))$ such that $0 \in Q'$. By note 11, $0 \in Q'$ means that $\mathrm{Im}(1-k) \subseteq Q'$ and Q' is a union of the cosets $\mathrm{Im}(1-k) + x$, so again as in Example 6, $E' = (Q', +, -, 0, (1-k) \restriction_{Q'})$ is an enveloping algebra. By Lemma 12, $(1-k)Q_x \cap (1-k)Q_y = \emptyset$ for $Q_x \neq Q_y$, so E' is an essential enveloping algebra and $Q' = \mathrm{Aff}(E')$.

Now we will state a theorem that describes the situation when two quandles constructed from two different essential enveloping algebras are isomorphic.

Theorem 19. *Let E, E' be two essential enveloping algebras. Then there exists a quandle isomorphism $f : \mathrm{Aff}(E) \to \mathrm{Aff}(E')$ such that $f(e) \in \mathrm{Im}(\alpha')$ if and only if there exists a group isomorphism $\varphi : \mathrm{Im}(\alpha) \to \mathrm{Im}(\alpha')$, and $\varphi(-\alpha + 1)(a) = (-\alpha' + 1)\varphi(a)$ for every $a \in \mathrm{Im}(\alpha)$.*

Proof. Let us first suppose that $f : \mathrm{Aff}(E) \to \mathrm{Aff}(E')$ is a quandle isomorphism. We can assume that $f(e) = e'$ because if it does not, we can put $f' = T_{-f(e)} \circ f$ where $T_{-f(e)}$ is a translation by $-f(e) \in \mathrm{Im}(\alpha')$, thus by Proposition 18(6) an automorphism of $\mathrm{Aff}(E')$. The composition of a quandle automorphism with an isomorphism is an isomorphism as well, so

$$f'(e) = T_{-f(e)}(f(e)) = -f(e) + f(e) = e'.$$

We will show that the restriction of the quandle isomorphism f to $\mathrm{Im}(\alpha)$ is in fact the group isomorphism φ that we are looking for. By setting the first and second variable in the quandle isomorphism equation consecutively to e, we get:

$$f((-\alpha + 1)(y)) = (-\alpha' + 1)(f(y)) \tag{3.11}$$
$$f(\alpha(x)) = \alpha'(f(y)). \tag{3.12}$$

Equation (3.11) is exactly the desired condition from the theorem. From equation (3.12) we can see that $f(\mathrm{Im}(\alpha)) \subseteq \mathrm{Im}(\alpha')$. We can add the second equation to the first and we get

$$\begin{aligned} f(\alpha(x)) + f((-\alpha + 1)(y)) &= \alpha'(f(y)) + (-\alpha' + 1)(f(y)) \quad f \text{ homomorphism} \\ &= f(\alpha(x) + (-\alpha + 1)(y)). \end{aligned} \tag{3.13}$$

Let $x, y \in E$ be arbitrary, for any $y \in E$ there is $z \in E$ such that $(-\alpha + 1)(\alpha(z)) = \alpha(y)$ because $-\alpha + 1$ is an automorphism of $\mathrm{Im}(\alpha)$. Then we get:

$$\begin{aligned} f(\alpha(x) + \alpha(y)) &= f(\alpha(x) + (-\alpha + 1)(\alpha(z))) && \text{by (3.13)} \\ &= f(\alpha(x)) + f((-\alpha + 1)(\alpha(z))) \\ &= f(\alpha(x)) + f(\alpha(y)), \end{aligned}$$

making f a homomorphism of the groups $\mathrm{Im}(\alpha) \to \mathrm{Im}(\alpha')$. Clearly $f \restriction_{\mathrm{Im}(\alpha)}$ is injective because f is a bijection from E to E'. We show that it is also onto $\mathrm{Im}(\alpha')$. For any $a' \in \mathrm{Im}(\alpha')$ there exists $y \in E'$ such that $\alpha(y) = a'$ and since f is a bijection, we can put $x = f^{-1}(y) \in E$. Then for $a = \alpha(x)$ and we have

$$f(a) = f(\alpha(x)) \overset{(3.12)}{=} \alpha'(f(x)) = \alpha'\left(f f^{-1}(y)\right) = \alpha'(y) = a'$$

and $f \restriction_{\mathrm{Im}(\alpha)}$ is a group isomorphism.
For the opposite implication, let φ be the group isomorphism from $\mathrm{Im}(\alpha)$ to $\mathrm{Im}(\alpha')$ such that $\varphi(-\alpha + 1)(a) = (-\alpha' + 1)\varphi(a)$ for every $a \in \mathrm{Im}(\alpha)$. We make an observation: φ is a group homomorphism, so:

$$-\alpha'\varphi(a) + \varphi(a) = (-\alpha' + 1)\varphi(a) = \varphi(-\alpha(a) + a) = -\varphi\alpha(a) + \varphi(a)$$

meaning that for every $a \in \mathrm{Im}\,(\alpha)$, we have

$$\varphi\alpha\,(a) = \alpha'\varphi\,(a)\,. \tag{3.14}$$

We will show that $\varphi\,(\mathrm{Im}\,(\alpha^2)) = \mathrm{Im}\,(\alpha')^2$ and therefore the quotient groups $\mathrm{Im}\,(\alpha)\,/\,\mathrm{Im}\,(\alpha^2)$ and $\mathrm{Im}\,(\alpha')\,/\,\mathrm{Im}\,(\alpha')^2$ are isomorphic. We take any $x \in \mathrm{Aff}\,(E)$ and

$$\varphi\alpha^2\,(x) \overset{(3.14)}{=} \alpha'\varphi\alpha\,(x) \in \mathrm{Im}\,(\alpha')^2$$

because $\varphi\,(\mathrm{Im}\,(\alpha)) = \mathrm{Im}\,(\alpha')$, so there exists $y \in E'$ such that $\varphi\alpha\,(x) = \alpha'\,(y)$ for every $x \in E$; and $\varphi\,(\mathrm{Im}\,(\alpha^2)) \subseteq \mathrm{Im}\,(\alpha')^2$.
We will use a similar trick to show that $\varphi \restriction_{\mathrm{Im}(\alpha)^2}$ is onto $\mathrm{Im}\,(\alpha')^2$. For every $a \in \mathrm{Im}\,(\alpha')^2$ we need to find $b \in \mathrm{Im}\,(\alpha^2)$ such that $\varphi\,(b) = a$. Let $a = \alpha'\,(a')$ where $a' \in \mathrm{Im}\,(\alpha')$ and since φ is an isomorphism, there exists $b' \in \mathrm{Im}\,(\alpha)$ such that $\varphi\,(b') = a'$. Then certainly

$$a = \alpha'\,(a') = \alpha'\varphi\,(b') \overset{(3.14)}{=} \varphi\,(\alpha\,(b'))$$

where $b = \alpha\,(b') \in \mathrm{Im}\,(\alpha^2)$.
Let us consider a transversal I of $\mathrm{Im}\,(\alpha)\,/\,\mathrm{Im}\,(\alpha^2)$ such that $0 \in I$ and define $J = \varphi\,(I)$. Because $\varphi\,(\mathrm{Im}\,(\alpha^2)) = \mathrm{Im}\,(\alpha')^2$, we can be sure that J is a transversal of $\mathrm{Im}\,(\alpha')\,/\,\mathrm{Im}\,(\alpha')^2$. We know by Proposition 18 (4) that if we take the orbits Q_x of $\mathrm{Dis}\,(Q)$ in $\mathrm{Aff}\,(E)$, the sets $\alpha\,(Q_x)$ correspond exactly to the cosets of $\mathrm{Im}\,(\alpha^2)$ in $\mathrm{Im}\,(\alpha)$ and in essential enveloping algebras, they are pairwise disjoint. Therefore there exists a set of orbit representatives $X \subset E$ such that $\alpha\,(X) = I$ and similarly, there exists $X' \subset E'$ a set of orbit representatives such that $\alpha'\,(X') = J$.

$$\begin{array}{ccc} I & \xrightarrow{\varphi} & J \\ {\scriptstyle\alpha}\uparrow & & {\scriptstyle\alpha'}\uparrow \\ X & \xrightarrow[\sigma]{} & X' \end{array} \tag{3.15}$$

Now we can define a mapping $\sigma : X \to X'$ such that

$$\sigma : x \mapsto x' \quad \Leftrightarrow \quad \varphi\alpha\,(x) = \alpha'\,(x')\,, \tag{3.16}$$

or put another way, $\varphi\alpha\,(x) = \alpha'\sigma\,(x)$. Then the diagram (3.15) commutes. The mapping σ is clearly a bijection because $\varphi \restriction_I$ is a bijection of I and J; and $\alpha \restriction_X$ and $\alpha' \restriction_{X'}$ are bijections to I, J, respectively.
Now every element of $\mathrm{Aff}\,(E)$ has a decomposition as $a + x$ where $x \in X$ and $a \in \mathrm{Im}\,(\alpha)$: it always exists because X is a set of orbit representatives and $Q_x = \mathrm{Im}\,(\alpha) + x$. But it is also uniquely determined because if $z = a + x = b + y$,

$$a + x = b + y \Leftrightarrow y = a - b + x \Rightarrow y \in Q_x \Leftrightarrow x = y$$

since both $x, y \in X'$ are orbit representatives, and there exist $u, v \in E$ such that $\alpha\,(u) = a, \alpha\,(v) = b$ and

$$\alpha\,(u) + x = \alpha\,(v) + x \Leftrightarrow x = \alpha\,(u) - \alpha\,(v) + x$$
$$\overset{(3.10)}{\Leftrightarrow} x = L_u L_v^{-1}\,(x) \Leftrightarrow L_u\,(x) = L_v\,(x) \overset{prop.18(5)}{\Leftrightarrow} a = \alpha\,(u) = \alpha\,(v) = b.$$

Similarly in $\mathrm{Aff}(E')$, every element has a unique decomposition as $y+b$ where $y \in X'$ and $b \in \mathrm{Im}(\alpha')$. We define a mapping $f : \mathrm{Aff}(E) \to \mathrm{Aff}(E')$

$$f : a + x \mapsto \varphi(a) + \sigma(x).$$

The mapping is well defined and a bijection from the existence and uniqueness of the decomposition as shown above, the fact that $\varphi : \mathrm{Im}(\alpha) \to \mathrm{Im}(\alpha')$ is a bijection and the fact that $\sigma : X \to X'$ is a bijection of orbit representatives in $\mathrm{Aff}(E)$ and $\mathrm{Aff}(E')$.
We still need to prove that it is a quandle homomorphism. Let $a+x, b+y \in \mathrm{Aff}(E)$ where $x, y \in X$ and $a, b \in \mathrm{Im}(\alpha)$.

$$\begin{aligned} f((a+x) * (b+y)) &= f(\alpha(a+x) + (-\alpha+1)(b+y)) \\ &= f(\alpha(a) + \alpha(x) + (-\alpha+1)(b) - \alpha(y) + y) \\ &= \varphi(\alpha(a) + \alpha(x) + (-\alpha+1)(b) - \alpha(y)) + \sigma(y) \\ &= \varphi\alpha(a) + \varphi\alpha(x) + \varphi(-\alpha+1)(b) - \varphi\alpha(y) + \sigma(y) \end{aligned}$$

In the last equality we used the fact that $\varphi : \mathrm{Im}(\alpha) \to \mathrm{Im}(\alpha')$ is a group homomorphism. As for the other part of the quandle isomorphism equality, we have

$$\begin{aligned} f(a+x) * f(b+y) &= (\varphi(a) + \sigma(x)) * (\varphi(b) + \sigma(y)) \\ &= \alpha'(\varphi(a) + \sigma(x)) + (-\alpha'+1)(\varphi(b) + \sigma(y)) \\ &= \alpha'\varphi(a) + \alpha'\sigma(x) + (-\alpha'+1)\varphi(b) + (-\alpha'+1)\sigma(y) \\ &= \alpha'\varphi(a) + \alpha'\sigma(x) + (-\alpha'+1)\varphi(b) - \alpha'\sigma(y) + \sigma(y) \\ &= \varphi\alpha(a) + \varphi\alpha(x) + \varphi(-\alpha+1)(b) - \varphi\alpha(y) + \sigma(y). \end{aligned}$$

In the last equality we use the commutativity of the mappings from (3.14) and (3.16). Throughout the proof we carefully use the properties of enveloping algebras as defined and derived previously: all the elements in the expressions except for the last one are from the abelian groups $\mathrm{Im}(\alpha)$ or $\mathrm{Im}(\alpha')$, so we do not need to write the associativity brackets. The outcome of the two expressions is the same, thus we have shown f is a quandle isomorphism. Clearly $f(e) = \varphi(e) = e' \in \mathrm{Im}(\alpha')$ since φ is a group isomorphism and the proof is complete.

□

This theorem together with Example 7 on page 25 also gives us an interesting corollary regarding affine quandles and quandles constructed from essential enveloping algebras.

Corollary 20. *Let $E = (E, +, -, 0, \alpha)$ be an essential enveloping algebra, $Q = \mathrm{Aff}(A, k)$ an essential affine quandle and $\varphi : \mathrm{Im}(\alpha) \to \mathrm{Im}(1-k)$ a group isomorphism such that $\varphi(-\alpha+1)(a) = k\varphi(a)$ for every $a \in \mathrm{Im}(\alpha)$. Then $\mathrm{Aff}(E) \simeq Q$.*

Proof. As shown in Example 7 on page 25, the abelian group A with its operations and endomorphism $1-k$ is an essential enveloping algebra and $\mathrm{Aff}(A, k) = \mathrm{Aff}(A)$. So by Theorem 19 $\mathrm{Aff}(E) \simeq \mathrm{Aff}(A) = Q$.

□

3.4 Hou's Lemma and Affineness

We saw that the quandles constructed from essential enveloping algebras have a lot in common with affine quandles. If we are given an essential enveloping algebra E and an essential affine quandle $Q = \mathrm{Aff}\,(A, k)$ which satisfies a set of conditions regarding $\mathrm{Im}\,(1-k)$, the quandles $\mathrm{Aff}\,(E)$ and Q are isomorphic, therefore $\mathrm{Aff}\,(E)$ is affine.

To get a better characterization of affine quandles, we would like to drop the assumptions that Q is essential and having the appropriate affine quandle at hand. By Theorem 3, in order to prove that a quandle Q is affine, we need to prove the existence of an abelian group A and its automorphism k such that $\mathrm{Dis}\,(Q)$ and $\mathrm{LMlt}\,(Q)$ satisfy the conditions stated in the theorem. Finding the abelian group seems to be a fundamental problem in deciding whether a qiven quandle is affine or not, since the affine quandle does not uniquely determine its underlying abelian group. In fact, we already noted that two affine quandles can still be isomorphic even if their underlying abelian groups are not (see Example 8 on page 32).

Unfortunately so far we have been able to prove the characterization theorem only for finite quandles using a theorem by Xiang-Dong Hou published in [8]. It certainly leaves a lot of room for future generalization to infinite case.

Hou's Lemma 21. *Let D be a finite abelian group and $\varphi \in \mathrm{End}\,(D)$. Then there exist a finite abelian group $A \geq D$ with $|A/D| = |D/\,\mathrm{Im}\,(\varphi)\,|$ and an onto homomorphism $\bar{\varphi} : A \to D$ such that $\bar{\varphi} \restriction_D = \varphi$.*

Proposition 22. *Let E be a finite essential enveloping algebra. Then* $\mathrm{Aff}\,(E)$ *is an essential affine quandle.*

Proof. Let E be a finite essential enveloping algebra. We denote $\varphi = \alpha \restriction_{\mathrm{Im}(\alpha)}$, then $\varphi \in \mathrm{End}\,(\mathrm{Im}\,(\alpha))$ and by Hou's Lemma, there exists an abelian group $A \geq \mathrm{Im}\,(\alpha)$ and an onto homomorphism $\bar{\varphi} : A \to \mathrm{Im}\,(\alpha)$ such that $|A/\,\mathrm{Im}\,(\alpha)\,| = |\,\mathrm{Im}\,(\alpha)\,/\,\mathrm{Im}\,(\varphi)\,|$ and $\bar{\varphi} \restriction_{\mathrm{Im}(\alpha)} = \varphi = \alpha \restriction_{\mathrm{Im}(\alpha)}$. By Definition 2(3), $(1-\alpha) \restriction_{\mathrm{Im}(\alpha)} = 1-\varphi$ is an automorphism of $\mathrm{Im}\,(\alpha)$ so by Corrolary 16, $l = 1 - \bar{\varphi}$ is an automorphism of A; and $Q = \mathrm{Aff}\,(A, l)$ is an affine quandle.
We will use Corrolary 20 to show that $Q \simeq \mathrm{Aff}\,(E)$. We can see that

$$1 - l = 1 - (1 - \bar{\varphi}) = \bar{\varphi}$$

and we know that $\mathrm{Im}\,(\bar{\varphi}) = \mathrm{Im}\,(\alpha)$, so the group isomorphism between $\mathrm{Im}\,(1-l)$ and $\mathrm{Im}\,(\alpha)$ is identity. Conjugating a mapping by identity does not change the mapping, so we show that $l \restriction_{\mathrm{Im}(1-l)} = (-\alpha + 1) \restriction_{\mathrm{Im}(\alpha)}$:

$$l\,(a) = (1 - \bar{\varphi})\,(a) = (1 - \varphi)\,(a) = (-\alpha + 1)\,(a)\,.$$

From the size constraint given by Hou's Lemma and the fact that $\mathrm{Im}\,(\varphi) = \mathrm{Im}\,(\alpha^2)$, we get

$$|A| = |\,\mathrm{Im}\,(\alpha)\,| \cdot |\,\mathrm{Im}\,(\alpha)\,/\,\mathrm{Im}\,(\varphi)\,|$$

so by Proposition 10, $m\,(Q) = 1$ and Q is essential. All requirements of the Corrolary 20 are satisfied, hence $Q \simeq \mathrm{Aff}\,(E)$ and $\mathrm{Aff}\,(E)$ is affine.

$\square$

The following corollary is the piece that we were missing when we proved that every affine quandle is a direct product of its essential subquandle and a projection quandle.

Corollary 23. *Let Q be a finite affine quandle and Q' an essential subquandle of Q such that $0 \in Q'$. Then Q' is affine.*

Proof. We saw in Example 7 that Q' as a set with the restrictions of the group operations from A is an essential enveloping algebra, so by Proposition 22, $\mathrm{Aff}\,(Q')$ is an affine quandle.

$\square$

Now we proceed to state and prove the most important results of this thesis.

Theorem 24 (Characterization of Finite Affine Quandles)**.** *Let Q be a finite quandle. Then the following statements are equivalent:*

1. *Q is affine;*
2. *there exists an essential enveloping algebra E and $m \in \mathbb{N}$ such that $Q \simeq \mathrm{Aff}\,(E) \times \mathrm{Proj}\,(m)$;*
3. *there exists an essential affine quandle $\bar{Q}$ and $m \in \mathbb{N}$ such that $Q \simeq \bar{Q} \times \mathrm{Proj}\,(m)$.*

Proof.
(1) $\Rightarrow$ (2) Let $Q = \mathrm{Aff}\,(A, k)$ be an affine quandle and $Q' = \bigcup_{x \in X'} Q_x$ an essential subquandle of Q such that $0 \in Q'$. Then by Theorem 13 we can consider a decomposition of Q such that

$$Q \simeq Q' \times \mathrm{Proj}\,(m\,(Q))\,.$$

We saw in Example 7 that $Q' \subseteq A$ is an essential enveloping algebra and the quandle $Q' = \mathrm{Aff}\,(Q')$.
(2) $\Rightarrow$ (3) The quandle we are looking for is $\bar{Q} = \mathrm{Aff}\,(E)$ since by Proposition 22 it is essential affine.
(3) $\Rightarrow$ (1) The projection quandle $\mathrm{Proj}\,(m) \simeq \mathrm{Aff}\,(\mathbb{Z}_m, id)$ is affine, and a direct product of the two affine quandles $\mathrm{Aff}\,(A, k) \times \mathrm{Proj}\,(m) = \mathrm{Aff}\,(A \times \mathbb{Z}_m, (k, id))$ is also affine.

$\square$

3.5 Isomorphisms of Affine Quandles

Before we proceed to describing the algorithm for recognizing affine quandles from their Cayley tables, we will make a small detour. Both of the following theorems are known results published in [17] and [7]. We present different formulations and proofs since they are direct corollaries of the facts we proved in the previous sections.

In the previous section we stated a condition that is both necessary and sufficient to determine whether two quandes constructed from essential enveloping algebras are isomorphic. We showed that any abelian group A with its automorphism k such that $\mathrm{Ker}\,(1-k) \subseteq \mathrm{Im}\,(1-k)$ is an essential enveloping algebra; and $\mathrm{Aff}\,(A,k) = \mathrm{Aff}\,(A)$. It means that Theorem 19 can be directly applied to essential affine quandles.

To get a full description of the situation when two quandles are isomorphic we need to generalize Theorem 19 for the case that $m\,(Q) > 1$. We achieve this in the following theorem.

Theorem 25. *Let $Q_1 = (A_1, k_1)$, $Q_2 = (A_2, k_2)$ be affine quandles. Then $Q_1 \simeq Q_2$ if and only if there is a group isomorphism $\varphi : \mathrm{Im}\,(1-k_1) \to \mathrm{Im}\,(1-k_2)$, $k_2\,(a) = k_1^{\varphi}\,(a)$ for every $a \in \mathrm{Im}\,(1-k_1)$ and $m\,(Q_1) = m\,(Q_2)$.*

Proof. Let us first suppose that there is a quandle isomorphism $f : Q_1 \to Q_2$. Then $\varphi = T_{-f(0)} \circ f : x \mapsto f\,(x) - f\,(0)$ is also a quandle isomorphism because $T_a : x \mapsto x + a \in \mathrm{Aut}\,(Q_2)$ for every $a \in Q_2$, and a composition of an automorphism with an isomorphism is an isomorphism as well. In addition to that, $\varphi\,(0) = f\,(0) - f\,(0) = 0 \in A_2$.
Let us consider an essential subquandle $Q_1' \leq Q_1$ such that $0 \in Q_1'$ and denote $Q_2' = \varphi\,(Q_1')$. We will show that Q_2' is an essential subquandle of Q_2. First we will show that for every orbit Q_x, $\varphi\,(Q_x) = Q_{\varphi(x)}$. By Proposition 5 (1), $k_i\,(Q_x) = Q_x$ so $k_i\,(\mathrm{Im}\,(1-k_i)) = \mathrm{Im}\,(1-k_i)$, so

$$Q_{k_i(x)} = \mathrm{Im}\,(1-k_i) + k_i\,(x) = k_i\,(\mathrm{Im}\,(1-k_i)) + k_i\,(x) = k_i\,(Q_x) = Q_x$$

for $i \in \{1, 2\}$, and for any $Q_x \subseteq Q_1$ we have

$$\begin{aligned} \varphi\,(Q_x) &= \{\varphi\,((1-k_1)\,(a) + k_1\,(x)) : a \in Q_1\} && (\varphi \text{ q. isomorphism}) \\ &= \{(1-k_2)\,\varphi\,(a) + k_2\varphi\,(x) : a \in Q_1\} && (\varphi\,(Q_1) = Q_2) \\ &= \{(1-k_2)\,b + k_2\varphi\,(x) : b \in Q_2\} = Q_{k_2\varphi(x)} = Q_{\varphi(x)}. \end{aligned}$$

In particular we know again by Proposition 5 (1) that $\mathrm{Im}\,(1-k_i) = Q_0 \leq Q_i$ and $\varphi\,(0) = 0$ so

$$\varphi\,(\mathrm{Im}\,(1-k_1)) = \varphi\,(Q_0) = Q_{\varphi(0)} = \mathrm{Im}\,(1-k_2)\,.$$

If we put $y = 0$ in the quandle homomorphism equation for φ, we get that that for every $x \in Q_1$,

$$\varphi\,((1-k_1)\,(x)) = (1-k_2)\,(\varphi\,(x))\,, \tag{3.17}$$

so

$$(1-k_2)\,Q_2' = (1-k_2)\,\varphi\,(Q_1') = \varphi\,(1-k_1)\,Q_1' = \varphi\,(\mathrm{Im}\,(1-k_1)) = \mathrm{Im}\,(1-k_2)$$

and

$$(1-k_2)\,Q_{\varphi(x)} = (1-k_2)\,\varphi\,(Q_x) = \varphi\,(1-k_1)\,Q_x$$

so if we have $w \in (1-k_2)\,Q_{\varphi(x)} \cap (1-k_2)\,Q_{\varphi(y)}$, then $\varphi^{-1}\,(w) \in (1-k_1)\,Q_x \cap (1-k_1)\,Q_y$; and since we assumed that Q_1' is an essential quandle, by Lemma 12

$Q_x = Q_y$, so $Q_{\varphi(x)} = Q_{\varphi(y)}$ and again by Lemma 12, $Q'_2 = \varphi(Q'_1)$ is an essential subquandle of Q_2.
By Example 7 on page 25, the essential subquandles $Q_i = \mathrm{Aff}(Q_i)$, and we know that $\varphi(0) = 0$, so by Theorem 19 there exists a group isomorphism $f : \mathrm{Im}(1-k_1) \to \mathrm{Im}(1-k_2)$ such that $fk_1(a) = k_2 f(a)$.
It remains to show that $m(Q_1) = m(Q_2)$. First we notice that $\varphi(\mathrm{Ker}(1-k_1)) = \mathrm{Ker}(1-k_2)$: we know that $\varphi(0) = 0$ so from (3.17) we can see that

$$(1-k_1)(x) = (1-k_1)(0) = 0 \Leftrightarrow (1-k_2)\varphi(x) = (1-k_2)\varphi(0) = 0.$$

We proved that φ is a bijection of both $\mathrm{Im}(1-k_1)$ to $\mathrm{Im}(1-k_2)$ and $\mathrm{Ker}(1-k_1)$ to $\mathrm{Ker}(1-k_2)$, so the mapping of the quotient groups $\mathrm{Ker}(1-k_i) / \mathrm{Im}(1-k_i) \cap \mathrm{Ker}(1-k_i)$ derived from φ must be a bijection as well. Therefore $m(Q_1) = m(Q_2)$.

Conversely, let us have two affine quandles $Q_1 = (A_1, k_1)$ and $Q_2 = (A_2, k_2)$ and the group isomorphism $\varphi : \mathrm{Im}(1-k_1) \to \mathrm{Im}(1-k_2)$ such that $\varphi k_1(a) = k_2\varphi(a)$ for every $a \in \mathrm{Im}(1-k_1)$ and $m = m(Q_1) = m(Q_2)$. For $i \in \{1,2\}$, there exist subquandles Q'_i such that

$$Q_i \simeq Q'_i \times Q_m$$

where Q'_i is an essential subquandle of Q_i and $0 \in Q'_i$. Now by Example 7, the quandles $Q'_i = \mathrm{Aff}(Q'_i)$, and by Theorem 19 is $Q'_1 \simeq Q'_2$, hence the products with the projection quandle $\mathrm{Proj}(m)$ are isomorphic as well:

$$Q'_1 \times Q_m \simeq Q'_2 \times Q_m$$

so $Q_1 \simeq Q_2$.

□

This theorem says that we do not need for the underlying abelian groups of two affine quandles to be isomorphic for the quandles to be isomorphic. In the following example we will present a quandle that is isomorphic to the quandle $Q' \leq Q$ from the Example 4 and its underlying abelian group is not $\mathbb{Z}_4 \times Z_2$ but Z_2^3.
Example 8. Let $Q'' = \mathrm{Aff}(\mathbb{Z}_2^3, l)$ where $l = \{(0,0,1) \mapsto (1,0,1), (0,1,0) \mapsto (1,0,0), (1,0,0) \mapsto (0,1,0)\}$.

x	$(0,0,0)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$
$l(x)$	$(0,0,0)$	$(1,0,1)$	$(1,0,0)$	$(0,0,1)$	$(0,1,0)$	$(1,1,1)$	$(1,1,0)$	$(0,1,1)$
$(1-l)(x)$	$(0,0,0)$	$(1,0,0)$	$(1,1,0)$	$(0,1,0)$	$(1,1,0)$	$(0,1,0)$	$(0,0,0)$	$(1,0,0)$

Table 3.2: $\mathbb{Z}_2^3$ with the endomorphisms l and $1-l$

We can see that $\mathrm{Im}(1-l) = \{(0,0,0), (1,1,0), (1,0,0), (0,1,0)\} \simeq \mathbb{Z}_2^2$. We will construct an isomorphism φ from $\mathrm{Im}(1-k) \leq Q'$ to $\mathrm{Im}(1-l)$:

$x \in \mathrm{Im}(1-k)$	$(0,0,0)$	$(2,0,0)$	$(0,1,0)$	$(2,1,0)$
$\varphi(x)$	$(0,0,0)$	$(1,1,0)$	$(1,0,0)$	$(0,1,0)$
$\varphi k(x)$	$(0,0,0)$	$(1,1,0)$	$(0,1,0)$	$(1,0,0)$

Table 3.3: Group isomorphism $\varphi : \mathrm{Im}(1-k) \to \mathrm{Im}(1-l)$

Applying l to $\varphi(x)$ means switching the first and second coordinate, so we can see that $l\varphi(x) = k\varphi(x)$ for every $x \in \operatorname{Im}(1-k)$ and, by Theorem 25, $Q'' \simeq Q'$.

Theorem 25 together with Hou's Lemma gives us the following description of finite affine quandles.

Theorem 26. *Let D be a finite abelian group, $l \in \operatorname{Aut}(D)$ and $m \in \mathbb{N}$ an arbitrary number. Then there exists an affine quandle $Q = \operatorname{Aff}(A,k)$ such that $D \leq A$, $\operatorname{Im}(1-k) = D$, $m(Q) = m$ and $k\restriction_D = l$; and it is determined uniquely up to isomorphism.*

Note 27. For clarity's sake we will consider the groups D and $D \times \mathbb{Z}_1$, and the automorphisms l and (l, id) to be the same.

Proof. First we prove the existence of such quandle. Let D and $l \in \operatorname{Aut}(D)$ be as described in the theorem, then $\alpha = 1 - l \in \operatorname{End}(D)$ and by Hou's Lemma, there exists an abelian group $B \geq D$ and an endomorphism $\bar{\alpha}$ such that $\operatorname{Im}(\bar{\alpha}) = D$ and $\bar{\alpha}\restriction_D = \alpha$. Since $1 - \bar{\alpha}\restriction_D = 1 - \alpha = l \in \operatorname{Aut}(D)$, by Corrolary 16 $1 - \bar{\alpha} \in \operatorname{Aut}(B)$. We consider the direct product $A = B \times \mathbb{Z}_m$ and $k = (1 - \bar{\alpha}, \mathrm{id})$. Then the quandle

$$Q = \operatorname{Aff}(A,k) = \operatorname{Aff}(B, 1-\bar{\alpha}) \times \operatorname{Proj}(m)$$

satisfies the conditions given by the theorem.
Now let us consider two quandles $Q_1 = \operatorname{Aff}(A_1, k_1)$ and $Q_2 = \operatorname{Aff}(A_2, k_2)$ such that for $i \in \{1,2\}$, $\operatorname{Im}(1-k_i) = D \leq A_i$, $m(Q_i) = m$ and $k_i\restriction_D = l$. Clearly the conditions of Theorem 25 are satisfied with the group isomorphism being identity, so $Q_1 \simeq Q_2$.

$\square$

Chapter 4

Recognizing Affineness

Having an underlying abelian group and its isomorphism at hand makes working with affine quandles very natural, since we can freely use the properties of abelian groups and their isomorphisms. We can very easily prove many interesting properties that affine quandles have. The reason why we made the simple definition of affine quandles seemingly more complicated by introducing enveloping algebras is that recognizing an underlying abelian group from the quandle's Cayley table is not easy. The problem is that the quandle does not determine the group uniquely; it is possible for an affine quandle to be constructed from different (non-isomorphic) abelian groups (see Example 8 on page 32), and we do not know if one of them would be the canonical choice. Nevertheless, we have found a canonical choice for an enveloping algebra.

In this chapter we will present an algorithm which has a multiplication table of a quandle Q on the input and which decides whether the quandle Q is affine. The algorithm uses the Cayley table to attempt to construct the canonical essential enveloping algebra E such that $Q \simeq \mathrm{Aff}(E) \times \mathrm{Proj}(m)$; if it is successful then Q is affine and if it is not, it decides that Q is not affine.

4.1 Supporting Lemmas

Before we proceed to the description of the algorithm we should prove several technical lemmas.

So far, whenever we have applied facts about essential enveloping algebras to essential subquandles, we always assumed that $0 \in Q'$ so that we can use $1-k$ as the unary operation α and $\mathrm{Im}(1-k) \subseteq Q'$ as the abelian group $\mathrm{Im}(\alpha)$. In this section we will show, among other things, that we can define an enveloping algebra where the unit is an arbitrary element of Q', and the resulting quandle will be the same (isomorphic).

Lemma 28. *Let Q be an affine quandle and $Q' \leq Q$ a subquandle. Then Q' is an essential subquandle if and only if $R_a(Q') = \mathrm{Im}(R_a)$ and $R_a(Q_x) \cap R_a(Q_y) = \emptyset$ for every $Q_x \neq Q_y$, $Q_x, Q_y \subseteq Q'$ for any $a \in Q$.*

Proof. By Lemma 12 it is sufficient to show that the conditions stated here are equivalent with $(1-k)\,Q' = \mathrm{Im}(1-k)$ and $(1-k)\,Q_x \cap (1-k)\,Q_y = \emptyset$ for

$Q_x, Q_y \subseteq Q'$, $Q_x \neq Q_y$. But that is clear since $R_a : x \mapsto (1-k)(x) + k(a)$, so

$$R_a(Q') = (1-k)Q' + k(a)$$
$$R_a(Q_x) = (1-k)Q_x + k(a)$$

and A is an abelian group.

□

Lemma 29. *Let Q be an affine quandle. Then for every $Q_x, Q_y \subseteq Q$ and any $a \in Q$, the following is true:*

1. $|R_a(Q_x)| = |R_a(Q_y)|$;
2. *either* $R_a(Q_x) = R_a(Q_y)$ *or* $R_a(Q_x) \cap R_a(Q_y) = \emptyset$.

Proof. Both statements come as a corollary of Proposition 5 and the fact that $R_a : x \mapsto (1-k)(x) + k(a)$, so

$$R_a(Q_x) = (1-k)Q_x + k(a)$$

□

While previous chapter's Theorem 24 gives us a description of finite affine quandles that is fairly easy to imagine, the conditions that are sufficient to determine that a given quandle is affine are not exactly algorithm-friendly. If we wanted to use it to show that a quandle is not affine, we would have to prove non-existence of an enveloping algebra satisfying certain conditions. In the following two lemmas we will introduce a set of conditions that are perhaps less transparent but algorithmically easily verifiable; it further turns out that they are not only necessary but, combined with a few others, also sufficient to determine whether a finite quandle is affine.

Lemma 30. *Let Q be an affine quandle and $Q' \leq Q$ an essential subquandle of Q, $a \in Q$ arbitrary and $S \subseteq Q'$ such that R_a is a bijection from S to $\mathrm{Im}(R_a)$. Then the following conditions are satisfied:*

1. $L_S = \{L_x : x \in S\}$ *is a set of all pairwise distinct left translations in Q*
2. $\mathrm{Dis}(Q) = \{L_x L_a^{-1} : x \in S\}$
3. *for every $x, y \in S$ and $w \in Q$*

$$L_x L_a^{-1} R_a(y) = R_a(z) \text{ where } z \in S \text{ such that } L_x L_a^{-1} L_y L_a^{-1} = L_z L_a^{-1} \quad (4.1)$$
$$R_a L_x L_a^{-1}(w) = L_{R_a(x)} L_a^{-1} R_a(w) \quad (4.2)$$

Proof. Let $a \in Q$ be arbitrary and $S \subseteq Q'$ a set such that R_a is a bijection from S to $\mathrm{Im}(R_a)$ and $L_S = \{L_x : x \in S\}$. Such a set always exists since $R_a(Q') = \mathrm{Im}(R_a)$ by Lemma 28. The mapping $R_a \restriction_S$ is injective, so

$$L_x(a) = R_a(x) \neq R_a(y) = L_y(a) \text{ for } \forall x, y \in S$$

and $L_x \neq L_y$ for every $x, y \in S$; hence $L_x \in L_S$ are pairwise distinct. In addition to that, $R_a(S) = \operatorname{Im}(R_a)$, which means that if we have $L_y \notin L_S$, there exists $x \in S$ such that $L_y(a) = R_a(y) = R_a(x) = L_x(a)$ and by equality (3.1) on page 13 we have $L_x = L_y$. So $L_S = \{L_x : x \in S\}$ is a set of all pairwise distinct left translations in Q'. By note 11, the sets of left translations in Q and Q' are the same.
From the definition of $\operatorname{Dis}(Q)$, $\{L_x L_a^{-1} : x \in S\} \subseteq \operatorname{Dis}(Q)$ and since R_a is a bijection from S to $\operatorname{Im}(R_a) = \operatorname{Im}(1-k) + k(a)$, from equation (3.2) on page 14 and the above we have

$$|\operatorname{Dis}(Q)| = |\operatorname{Im}(1-k)| = |\operatorname{Im}(R_a)| = |S|,$$

so $\operatorname{Dis}(Q) = \{L_x L_a^{-1} : x \in S\}$.
Now for equality (4.1), we have

$$L_x L_a^{-1} L_y L_a^{-1} : c \mapsto (1-k)(x+y-2a) + c,$$

so $L_x L_a^{-1} L_y L_a^{-1} = L_{x+y-a} L_a^{-1}$; and because L_S is a set of all left translations, there exists $z \in S$ such that $L_z = L_{x+y-a}$, i.e. $(1-k)(z) = (1-k)(x+y-a)$. So we can rewrite the first condition as

$$L_x L_a^{-1} R_a(y) = L_x L_a^{-1}((1-k)(y) + k(a)) = (1-k)(x-a) + (1-k)(y) + k(a)$$

$$R_a(z) = (1-k)(z) + k(a) = (1-k)(x+y-a) + k(a),$$

so the first equality stands. For the condition (4.2), we can see that for any $x \in S$ and $y \in Q$ we have

$$\begin{aligned} L_{R_a(x)} L_a^{-1} R_a(y) &= (1-k)(R_a(x) - a) + R_a(y) \\ &= (1-k)((1-k)(x) + k(a) - a) + (1-k)(y) + k(a) \\ &= (1-k)^2(x-a) + (1-k)(y) + k(a) \end{aligned}$$

and

$$R_a L_x L_a^{-1}(y) = R_a((1-k)(x-a) + y) = (1-k)((1-k)(x-a) + y) + k(a)$$

which are clearly the same since $1-k$ is a group endomorphism.

$\square$

For any quandle Q such that $\operatorname{Dis}(Q) = \{L_x L_e^{-1} : x \in Q\}$, for an arbitrary element $e \in Q$, we consider a partial algebra $\operatorname{Env}(Q, e) = (Q, +, -, R_e, e)$ where the operations are defined as follows:

- $R_e(x) + y = L_x L_e^{-1}(y)$ for every $x, y \in Q$
- $-R_e(x) = R_e(y)$ where $y \in Q$ such that $L_y L_e^{-1} = L_e L_x^{-1}$

The element $y \in Q$ such that $L_y L_e^{-1} = L_e L_x^{-1}$ always exists because $L_e L_x^{-1} \in \operatorname{Dis}(Q)$ and we assumed that $\operatorname{Dis}(Q) = \{L_x L_e^{-1} : x \in Q\}$. On the other hand, if we have $y, z \in Q$ such that $L_y L_e^{-1} = L_z L_e^{-1}$, it means that $L_y = L_z$ so $R_e(y) = L_y(e) = L_z(e) = R_e(z)$ and $-R_e(x)$ is uniquely determined.

Note that if $S \subseteq Q$ such that $\{L_x : x \in S\}$ contains all pairwise distinct left translations, and $\mathrm{Dis}(Q) = \{L_x L_e^{-1} : x \in X\}$, then actually

$$\mathrm{Dis}(Q) = \{L_x L_e^{-1} : x \in S\}.$$

This partial algebra $\mathrm{Env}(Q, e)$ resembles an enveloping algebra, and in the following lemma we will introduce conditions that are sufficient to prove that $\mathrm{Env}(Q, e)$ actually is an enveloping algebra.

Lemma 31. *Let Q be a medial quandle and $e \in Q$ arbitrary. Let $S \subseteq Q$ be any set such that $R_e : S \to \mathrm{Im}(R_e)$ is a bijection and the following conditions are satisfied:*

1. $R_e(Q_x) \cap R_e(Q_y) = \emptyset$ *for every $Q_x, Q_y \in Q$ such that $Q_x \neq Q_y$*
2. $\mathrm{Dis}(Q) = \{L_x L_e^{-1} : x \in S\}$ *and* $|Q_x| = |\mathrm{Dis}(Q)|$ *for every $Q_x \subseteq Q$*
3. *for every $x, y \in S$ and $w \in Q$*

$$L_x L_e^{-1} R_e(y) = R_e(z) \text{ where } z \in S \text{ such that } L_x L_e^{-1} L_y L_e^{-1} = L_z L_e^{-1} \quad (4.3)$$
$$R_e L_x L_e^{-1}(w) = L_{R_e(x)} L_e^{-1} R_e(w) \quad (4.4)$$

Then $\mathrm{Env}(Q, e) = (Q, +, -, R_e, e)$ *is an essential enveloping algebra and* $\mathrm{Aff}(\mathrm{Env}(Q, e)) = Q$*. If Q is finite, it is affine.*

Proof. First we will prove that $\mathrm{Im}(R_e)$ with the operations defined as above is an abelian group. By Proposition 2 (3), since Q is medial, $\mathrm{Dis}(Q)$ is an abelian group. We consider a mapping $\varphi : \mathrm{Dis}(Q) \to \mathrm{Im}(R_e)$,

$$\varphi : L_x L_e^{-1} \mapsto L_x(e) = R_e(x) \quad \text{for every } x \in S,$$

and we show that it is a group isomorphism. It is onto because $R_e(S) = \mathrm{Im}(R_e)$. Because $R_e \restriction_S$ is injective, $L_x(e) \neq L_y(e)$ for every $x, y \in S$, so the mappings L_x, $x \in S$ are pairwise distinct and $|\mathrm{Dis}(Q)| = |S|$. For every orbit Q_a we have $|Q_a| = |\mathrm{Dis}(Q)|$, which means that $L_x L_e^{-1}(a) \neq L_y L_e^{-1}(a)$ for every $x \neq y \in S$ and every $a \in Q$. In particular, $L_x L_e^{-1} \neq L_y L_e^{-1}$ implies $L_x(e) = L_x L_e^{-1}(e) \neq L_y L_e^{-1}(e) = L_y(e)$, thus φ is injective.
So φ is a bijection and we need to confirm that it is also a group homomorphism. The unit satisfies the homomorphism condition by idempotency of Q: $\varphi(id) = R_e(e) = e$. For the inverse, we can find $y \in S$ such that $(L_x L_e^{-1})^{-1} = L_y L_e^{-1}$ and

$$\varphi\left(\left(L_x L_e^{-1}\right)^{-1}\right) = \varphi\left(L_y L_e^{-1}\right) = R_e(y) = -R_e(x).$$

As for the addition, we need to see if for every $x, y \in S$ the following is true:

$$\varphi\left(L_x L_e^{-1} L_y L_e^{-1}\right) = R_e(x) + R_e(y).$$

But by assumption, $L_x L_e^{-1} L_y L_e^{-1} = L_z L_e^{-1}$ for some $z \in S$ and

$$\varphi\left(L_z L_e^{-1}\right) = R_e(z) \overset{(4.3)}{=} L_x L_e^{-1}(R_e(y)) = R_e(x) + R_e(y),$$

so $\mathrm{Im}\,(R_e)$ is an abelian group. We can also see that the addition on Q satisfies the partial associativity condition since we can find $z \in S$ such that $L_x L_e^{-1} L_y L_e^{-1} = L_z L_e^{-1}$, and for any $w \in Q$:

$$\begin{aligned}(R_e(x) + R_e(y)) + w &= \left(L_x L_e^{-1}(R_e(y))\right) + w \\ &= R_e(z) + w && \text{(from (4.3))} \\ &= L_z L_e^{-1}(w) \\ &= L_x L_e^{-1} L_y L_e^{-1}(w)\end{aligned}$$

and

$$R_e(x) + (R_e(y) + w) = R_e(x) + L_y L_e^{-1}(w) = L_x L_e^{-1} L_y L_e^{-1}(w).$$

As for the unit, we know that $R_e(e) = e$, so for every $x \in Q$

$$e + x = R_e(e) + x = L_e L_e^{-1}(x) = x$$

and if we have $R_e(a) + x = L_a L_e^{-1}(x) = x$, then $L_a L_e^{-1} = L_e L_e^{-1} = \mathrm{id}$ and $R_e(a) = e$, since we showed above that $L_x L_e^{-1}(w) = L_y L_e^{-1}(w)$ implies $L_x L_e^{-1} = L_y L_e^{-1}$.

For E to be an essential enveloping algebra, it remains to check that the property (3) of the mapping R_e from Definition 2, since we assumed that $R_e(Q_x) \cap R_e(Q_y) = \emptyset$ for $Q_x \neq Q_y$. The enveloping algebra homomorphism equation written in the language of translations is

$$R_e\left(L_x L_e^{-1}(y)\right) = L_{R_e(x)} L_e^{-1}(R_e(y))$$

but that is exactly what we assumed in equality (4.4). Clearly $R_e(\mathrm{Im}\,(R_e)) \subseteq \mathrm{Im}\,(R_e)$, so $R_e \restriction_{\mathrm{Im}(R_e)}$ and $(-R_e + 1) \restriction_{\mathrm{Im}(R_e)}$ are group endomorphisms. We need to show that $(-R_e + 1) \restriction_{\mathrm{Im}(R_e)}$ is also a permutation. For $y \in S$ such that $-R_e(x) = R_e(y)$, we have

$$-R_e(x) + x = R_e(y) + x = L_y L_e^{-1}(x) = L_e L_x^{-1}(x) = L_e(x), \tag{4.5}$$

so $-R_e + 1 = L_e$ is a permutation on Q: hence $(-R_e + 1) \restriction_{\mathrm{Im}(R_e)} = L_e \restriction_{\mathrm{Im}(R_e)}$ is injective. Since $\mathrm{Im}\,(R_e) = \{L_x(e) : x \in S\} = \{L_x L_e^{-1}(e) : x \in S\}$ is an orbit of $\mathrm{Dis}\,(Q)$, by Proposition 1 it is also an orbit of $\mathrm{LMlt}\,(Q)$; and $L_e^{-1} \in \mathrm{LMlt}\,(Q)$, which means $L_e^{-1}(\mathrm{Im}\,(R_e)) \subseteq \mathrm{Im}\,(R_e)$. But $L_e \restriction_{\mathrm{Im}(R_e)}$ is a group endomorphism, so $L_e(\mathrm{Im}\,(R_e)) \subseteq \mathrm{Im}\,(R_e)$, hence $L_e(\mathrm{Im}\,(R_e)) = \mathrm{Im}\,(R_e)$, $L_e \restriction_{\mathrm{Im}(R_e)}$ is a group automorphism and $\mathrm{Env}\,(Q, e)$ is an essential enveloping algebra.

The last thing we need to show is that $\mathrm{Aff}\,(E) = Q$; i.e., for every $x, y \in Q$

$$x * y = R_e(x) + (-R_e + 1)(y)$$

where $*$ is the quandle operation in Q. Using the operations of the enveloping algebra, we can rewrite it as

$$x * y = L_x(y) = L_x L_e^{-1}(L_e(y)) = R_e(x) + L_e(y),$$

and because we showed in equation (4.5) that $-R_e(x) + 1 = L_e(x)$, the quandles are equal; and if Q is finite, then it is affine by Proposition 22.

□

Note 32. In affine quandles, we have $1-k=R_0$ and $k=L_0$, so the quandle operation is exactly the same as in $\operatorname{Aff}(\operatorname{Env}(Q,e))$:

$$x * y = R_0(x) * L_0(y).$$

Notice that the equalities in condition (3) in lemmas 30 and 31 are the same. In addition to that, condition (1) from Lemma 31 stands for any essential subquandle, and $|\operatorname{Dis}(Q)| = |Q_x|$ is true for any affine quandle by equality (3.4). This observation gives us the following corollary.

Corollary 33. *Let Q be an affine quandle and $Q' \leq Q$ an essential subquandle of Q. Then $Q' = \operatorname{Aff}(\operatorname{Env}(Q',e))$ for $e \in Q'$ arbitrary. If Q is finite, then Q' is affine.*

Proof. We will show that any essential subquandle of Q satisfies the conditions given in Lemma 31. Any affine quandle is medial by Proposition 2, and so is its subquandle Q'. Let $e \in Q'$ be arbitrary and $S \subseteq Q'$ such that $R_e : S \to \operatorname{Im}(R_e)$ is a bijection. By Lemma 28, $R_e(Q_x) \cap R_e(Q_y) = \emptyset$ for any $e \in Q'$ and $Q_x, Q_y \subseteq Q'$ such that $Q_x \neq Q_y$. By Lemma 30, $\operatorname{Dis}(Q) = \{L_x L_e^{-1} : x \in S\}$ and the equations (4.3) and (4.4) of Lemma 31 stand. Hence $Q' = \operatorname{Aff}(\operatorname{Env}(Q',e))$ and if Q is finite, Q' is affine.

□

This is the piece we have been missing while describing the essential subquandles of affine quandles. Now we know that any way we choose the orbits that constitute the essential subquandle, the partial algebra $\operatorname{Env}(Q',e)$ is an essential enveloping algebra for any $e \in Q'$; and if Q' is finite, it is affine. In the light of this corollary, the following lemma is not surprising: we will show that every two essential subquandles of an affine quandle are isomorphic.

Lemma 34. *Let Q be a finite affine quandle, X a set of orbit representatives and $X', X'' \subseteq X$ such that $Q' = \bigcup_{x \in X'} Q_x$ and $Q'' = \bigcup_{x \in X''} Q_x$ are essential subquandles of Q. Then for any $e \in Q$ and L_S a set of all pairwise distinct left translations on Q*

1. *there exists an injective mapping $\lambda : X' \hookrightarrow Q''$ such that $R_e(x) = R_e(\lambda(x))$ and $\lambda(X')$ is a set of orbit representatives in Q'';*
2. *the mapping $\sigma : Q' \to Q''$ such that $\sigma : L_a L_e^{-1}(x) \mapsto L_a L_e^{-1}(\lambda(x))$, $L_a \in L_S$ is a quandle isomorphism for any such λ and $R_e(\sigma(x)) = R_e(x)$ for every $x \in Q'$.*

Proof. Let $Q = \operatorname{Aff}(A,k)$. Since Q' and Q'' are its essential subquandles, by definition $(1-k)X'$ and $(1-k)X''$ are transversals of $\operatorname{Im}(1-k)/\operatorname{Im}(1-k)^2$. It means that there is a bijection $\rho : X' \to X''$ such that $(1-k)(x-\rho(x)) \in \operatorname{Im}(1-k)^2$; i.e., there exists $a_x \in \operatorname{Im}(1-k)$ such that $(1-k)(a_x) = (1-k)(x-\rho(x))$ for every $x \in X'$. We define $\lambda : X' \to Q''$ such that

$$\lambda : x \mapsto \rho(x) + a_x.$$

Clearly this is the mapping we are looking for: it is injective and $\lambda(X')$ is a set of orbit representatives in Q'' because $\rho(X') = X''$ is a bijection and $\lambda(x) = \rho(x) + a_x \in Q_{\rho(x)}$, so $Q_{\rho(x)} = Q_{\lambda(x)}$, and

$$\begin{aligned} R_e(\lambda(x)) &= (1-k)(\rho(x) + a_x) + k(e) \\ &= (1-k)(\rho(x)) + (1-k)(x - \rho(x)) + k(e) \\ &= (1-k)(x) + k(e) = R_e(x). \end{aligned}$$

Let us now consider mappings $\gamma : X' \hookrightarrow Q''$ such that $R_e(x) = R_e(\gamma(x))$ and $\gamma(X')$ is a set of orbit representatives in Q'', and σ such that

$$\sigma : L_a L_e^{-1}(x) \mapsto L_a L_e^{-1}(\gamma(x)) \quad \text{where } L_a \in L_S, x \in X'.$$

By Lemma 30 we know that $\mathrm{Dis}(Q) = \{L_a L_e^{-1} : L_a \in L_S\}$, $Q_x = \{L_a L_e^{-1}(x) : L_a \in L_S\}$ where $L_a L_e^{-1}(x)$ are pairwise distinct and in affine quandles by (3.1) on page 13 $L_a \neq L_b$ implies $L_a(x) \neq L_b(x)$ for every $x \in Q$. So for every $z \in Q'$ there exist a unique $x \in X'$ and $L_a \in L_S$ such that $z \in Q_x$ and $L_a L_e^{-1}(x) = z$, and similarly for every $w \in Q''$ there exist a unique $x \in X'$ and $L_a \in L_S$ such that $w = L_a L_e^{-1}(\gamma(x))$. From this we can see that σ as defined above is a bijection from Q' to Q''. It remains to check whether σ is a quandle homomorphism. We assumed that $R_e(\gamma(x)) = R_e(x)$ which means

$$(1-k)(x) + k(e) = (1-k)(\gamma(x)) + k(e) \Leftrightarrow (1-k)(\gamma(x)) = (1-k)(x). \tag{4.6}$$

For every $x, y \in X'$ and $L_a, L_b \in L_S$, we have

$$\begin{aligned} L_a L_e^{-1}(x) * L_b L_e^{-1}(y) &= (1-k)((1-k)(a-e) + x) + k((1-k)(b-e) + y) \\ &= (1-k)((1-k)(a-e) + k(b-e) + x) + k(y) \\ &= (1-k)((1-k)(a) + k(b) - e + x) - (1-k)(y) + y \\ &= (1-k)((1-k)(a) + k(b) + x - y - e) + y \\ &= L_c L_e^{-1}(y) \end{aligned}$$

where $L_c \in L_S$ and $(1-k)(c) = (1-k)((1-k)(a) + k(b) + x - y)$. So

$$\begin{aligned} \sigma\left(L_a L_e^{-1}(x) * L_b L_e^{-1}(y)\right) &= \sigma\left(L_c L_e^{-1}(y)\right) \\ &= L_c L_e^{-1}(\gamma(y)) \\ &= (1-k)(c-e) + \gamma(y) \\ &= (1-k)((1-k)(a) + k(b) + x - y - e) + \gamma(y) \\ &\overset{(4.6)}{=} (1-k)((1-k)(a) + k(b) + x - \gamma(y) - e) + \gamma(y) \\ &= (1-k)((1-k)(a) + k(b) + x - e) + k(\gamma(y)) \end{aligned}$$

while on the other hand we have

$$\begin{aligned} \sigma\left(L_a L_e^{-1}(x)\right) * \sigma\left(L_b L_e^{-1}(y)\right) &= L_a L_e^{-1}(\gamma(x)) * L_b L_e^{-1}(\gamma(y)) \\ &= (1-k)((1-k)(a-e) + \gamma(x)) \\ &\quad + k((1-k)(b-e) + \gamma(y)) \\ &\overset{(4.6)}{=} (1-k)((1-k)(a-e) + k(b-e) + x) + k(\gamma(y)) \\ &= (1-k)((1-k)(a) + k(b) + x - e) + k(\gamma(y)) \end{aligned}$$

In both calculations we used equality (4.6) and the fact that k and $1-k$ commute by equation (2.1) on page 11. Hence σ is a quandle isomorphism and by equality (4.6),

$$\begin{aligned}R_eL_aL_e^{-1}(\gamma(x)) &= (1-k)((1-k)(a-e)+\gamma(x))+k(e)\\ &= (1-k)((1-k)(a-e)+x)+k(e) = R_eL_aL_e^{-1}(x)\end{aligned}$$

so $R_e(\sigma(x)) = R_e(x)$.

$\square$

Not only we showed that any two essential subquandles of Q are isomorphic, we showed exactly what the isomorphism looks like. That turns very naturally into an algorithm: deciding whether two quandles are isomorphic is much more difficult than to decide if a specific mapping is a quandle isomorphism. In the next lemma we prove another predictable property of essential subquandles.

Lemma 35. *Let Q be an affine quandle. Then Q is a union of $m(Q)$ disjoint essential subquandles.*

Proof. Let I a transversal of $\mathrm{Im}(1-k)/\mathrm{Im}(1-k)^2$ and X set of orbit representatives of Q such that $(1-k)X = I$. For every $a \in I$ we consider the set $X_a \subseteq X$ such that $(1-k)(x) = a$ for every $x \in X_a$. Now

$x \neq y \in X_a \Leftrightarrow x-y \in \mathrm{Ker}(1-k)$ and $x \notin Q_y \Leftrightarrow x-y \in \mathrm{Ker}(1-k) \setminus \mathrm{Im}(1-k)$

so for every $a \in I$, we have

$$|X_a| = |\,\mathrm{Ker}(1-k)/\mathrm{Im}(1-k) \cap \mathrm{Ker}(1-k)\,| = m(Q)$$

and $X = \bigcup_{a\in I} X_a$ is a set of orbit representatives of Q. Let us consider X^i, $i < m(Q)$ such that $|X^i \cap X_a| = 1$ for every $a \in I$ and the sets X^i are pairwise disjoint. Such sets always exist because $|X_a| = m(Q)$ for every $a \in I$ and the sets X_a are pairwise disjoint. For every $i < m(Q)$, the quandle

$$Q^i = \bigcup_{x\in X^i} Q_x$$

is an essential subquandle of Q because from the definition of X^i, there is exactly one $x \in X^i$ such that $(1-k)(x) = a$ for every $a \in I$, so X^i is an essential set. The quandles Q^i are pairwise disjoint because X^i, X^j are pairwise disjoint subsets of the set of orbit representatives, and

$$Q = \bigcup_{x\in X} Q_x = \bigcup_{i<m(Q)} \bigcup_{x\in X^i} Q_x = \bigcup_{i<m} Q^i$$

$\square$

The last lemma in this section is useful for determining when a finite quandle can be written as a direct product of its affine subquandle and a projection quandle of size m.

Lemma 36. *Let Q be a finite quandle and $Q' \leq Q$ affine such that* $\mathrm{Dis}(Q) = \mathrm{Dis}(Q')$ *and* $|Q| = m \cdot |Q'|$. *Let there be a set of pairwise disjoint subquandles* $Q^1, \ldots, Q^{m-1}$ *such that* $Q = Q' \dot\cup \dot\bigcup_{i=1}^{m} Q^i$ *and for every* $i < m$ *there exists a quandle isomorphism* $\sigma_i : Q' \to Q^i$ *such that* $R_e(x) = R_e(\sigma_i(x))$ *for every* $x \in Q'$ *and* $e \in Q$ *arbitrary. Then* $Q \simeq Q' \times \mathrm{Proj}(m)$.

Proof. Let $\sigma_i : Q' \to Q^i$ be the quandle isomorphisms, $\mathrm{Proj}(m) = \mathrm{Aff}(\mathbb{Z}_m, id)$ and $\sigma_0 : Q' \to Q'$, $\sigma_0 = \mathrm{id}$. We consider a mapping $\sigma : Q' \times \mathrm{Proj}(m) \to Q$ such that

$$\sigma : (x, i) \mapsto \sigma_i(x)$$

This mapping clearly is a bijection since each σ_i is a bijection, $\mathrm{Im}(\sigma_i)$ are pairwise disjoint, and $Q = Q' \cup \bigcup_{i \leq m} \mathrm{Im}(\sigma_i)$. We need to see if it is also a quandle homomorphism:

$$\begin{gathered} \sigma((x * y, j)) = \sigma_j(x * y) = \sigma_j(x) * \sigma_j(y) \\ \sigma((x, i)) * \sigma((y, j)) = \sigma_i(x) * \sigma_j(y) \end{gathered}$$

We need to show that $L_{\sigma_i(x)} = L_{\sigma_j(x)}$ for every $i, j \leq m$ and $x \in Q'$. We assumed that $\mathrm{Dis}(Q) = \mathrm{Dis}(Q')$ and $L_x(e) = L_{\sigma_i(x)}(e)$ for every σ_i. Since Q' is affine, by Lemma 30 there exists a set $S \subseteq Q'$ and $e \in Q'$ such that $\mathrm{Dis}(Q') = \{L_x L_e^{-1} : x \in S\}$ where L_x, L_y for $x, y \in S$ are pairwise distinct, and by equation (3.1) on page 13, $L_x \neq L_y$ implies $L_x(e) \neq L_y(e)$. So if $L_x(e) = L_{\sigma_i(x)}(e)$ and $L_x \neq L_{\sigma_i(x)}$, we get that $L_{\sigma_i(x)} L_e^{-1} \notin \mathrm{Dis}(Q)$ which is a contradiction. So $L_{\sigma_i(x)} = L_x$ for each $x \in Q'$ and σ_i.

□

4.2 Algorithm for Recognizing Affine Quandles

Let us now assume that we are given a Cayley table of a finite quandle Q. The values in the row corresponding to an element $x \in Q$ are the values of the quandle automorphism L_x; the values in the column corresponding to x are the values of the mapping R_x.

The algorithm has four parts. In the main part, we first test some basic properties of the quandle. Then we use three other algorithms that first try to create a setup for a decomposition by Theorem 13, a set $Q' \subseteq Q$ and $m = |Q|/|Q'|$, then test if Q' is an affine quandle and finally, if $Q \simeq Q' \times \mathrm{Proj}(m)$.

First, we state one more definition. Let Q be a medial quandle and $e \in Q$ arbitrary. We call the ordered set $(X, \{Q_x : x \in X\}, X', Q', S)$ an *essential configuration* in Q if X is a set of orbit representatives of $\mathrm{Dis}(Q)$ in Q, $\{Q_x : x \in X\}$ a set of orbits and

- $|Q_x| = |\mathrm{Dis}(Q)|$ and $|R_e(Q_x)| = |R_e(Q_y)|$ for $\forall x, y \in X$;
- $X' \subseteq X$ such that for every $x, y \in X'$, $R_e(Q_x) \cap R_e(Q_y) = \emptyset$;
- $Q' = \bigcup_{x \in X'} Q_x$ such that $R_e(Q') = \mathrm{Im}(R_e)$;

- $S \subseteq Q'$ such that $R_e : S \to \mathrm{Im}(R_e)$ is a bijection and $\mathrm{Dis}(Q) = \{L_x L_e^{-1} : x \in S\}$.

Clearly, for any affine quandle Q, there is an essential configuration where X' is an essential set and Q' is as essential subquandle by Lemma 30. For every Q_x, Q_y, $|R_e(Q_x)| = |R_e(Q_y)|$ by Lemma 29 and $|Q_x| = |\mathrm{Dis}(Q)|$ by equation (3.4).

We can now proceed to the main part of the algorithm.

Algorithm 1 Main Algorithm

Input: quandle Q
Output: decides whether Q is affine

$\mathrm{Dis}(Q) \leftarrow \langle L_x L_y^{-1} \ : \ x, y \in Q \rangle$
if $\mathrm{Dis}(Q)$ not commutative **then**
    return Q NOT affine ▷ equality (3.2) and $\mathrm{Im}(1-k)$ abelian
end if
pick $e \in Q$ arbitrary, $Q_e \leftarrow \{f(e) \ : \ f \in \mathrm{Dis}(Q)\}$
if $|Q_e| = |Q|$ **then**
    return Q affine ▷ Proposition 2(3)
end if
if $|Q_e| \neq |\mathrm{Dis}(Q)|$ **then**
    return Q NOT affine ▷ equality (3.4)
end if
if `ConstructEssConfig`$(Q, \mathrm{Dis}(Q), e, Q_e) =$ "FAIL" **then**
    return Q NOT affine
else
    $(X, \{Q_x : x \in X\}, X', Q', S) \leftarrow$ `ConstructEssConfig`$(Q, \mathrm{Dis}(Q), e, Q_e)$
    $m \leftarrow |Q|/|Q'|$
end if
if `IsEssConfigAffine`$(Q, \mathrm{Dis}(Q), (X, \{Q_x : x \in X\}, X', Q', S))$ **then**
    if `IsDirectlyDecomposable`$(Q, \mathrm{Dis}(Q), (X, \{Q_x : x \in X\}, X', Q', S))$ **then**
        return Q affine
    else
        return Q NOT affine
    end if
else
    return Q NOT affine
end if

The first step is to find the group $\mathrm{Dis}(Q) = \langle L_x L_y^{-1} \ : \ x, y \in Q \rangle$ and check whether it is abelian. By equality (3.2) on page 14, for the affine quandle $Q = (A, k)$, $\mathrm{Dis}(Q) \simeq \mathrm{Im}(1-k)$; so if $\mathrm{Dis}(Q)$ is not abelian, Q is not affine. Next we set e to be an arbitrary element of Q and we find the orbit of $\mathrm{Dis}(Q)$ which contains e, $Q_e = \{f(e) \ : \ f \in \mathrm{Dis}(Q)\}$.
By Proposition 2(3), $\mathrm{Dis}(Q)$ is abelian if and only if Q is medial. So if $Q_e = Q$, then Q is connected and medial, therefore by Proposition 2 (2) it is affine.
By equation (3.4) on page 14, we know that if $|Q_e| \neq |\mathrm{Dis}(Q)|$, Q is not affine.

It remains to check three things: if it is possible to construct an essential configuration in Q, if Q' is affine and if Q is isomorphic to $Q' \times \operatorname{Proj}(m)$ where $m = |Q|/|Q'|$. If Q is affine, then we can always find an essential configuration in Q, Q' is an essential subquandle therefore affine by Corollary 33 and by Theorem 13, $Q \simeq Q' \times \operatorname{Proj}(m)$ where $m = |Q|/|Q'|$. So if no essential configuration exists, Q' is not affine or $Q \not\simeq Q' \times \operatorname{Proj}(m)$, then the algorithm rejects Q as not affine. If Q' is affine and $Q \simeq Q' \times \operatorname{Proj}(m)$, then Q is affine by Theorem 24.

For affine quandles, the following algorithm constructs an essential configuration. If it finds out that Q is not affine, it returns "FAIL".

Algorithm 2 `ConstructEssConfig`

Input: a quandle Q, $\operatorname{Dis}(Q)$ abelian, $e \in Q$, Q_e
Output: essential configuration $(X, \{Q_x : x \in X\}, X', Q', S)$ if exists, otherwise "FAIL"

$S \leftarrow \{e\}$
for all $a \in Q_e$ **do**
  if $R_e(a) \notin R_e(S)$ **then**
    $S \leftarrow S \cup \{a\}$
  end if
end for
$A \leftarrow Q \setminus Q_e$, $X \leftarrow \{e\}$, $X' \leftarrow \{e\}$, $Q' \leftarrow Q_e$, $N \leftarrow \emptyset$, $q \leftarrow |Q_e|$, $a \leftarrow |S|$
repeat
  pick $x \in A$, $Q_x \leftarrow \{f(x) \ : \ f \in \operatorname{Dis}(Q)\}$
  if $|Q_x| \neq q$ or $|R_e(Q_x)| \neq a$ **then**
    return FAIL ▷ equality (3.4) or Lemma 29
  end if
  $X \leftarrow X \cup \{x\}$, $A \leftarrow A \setminus Q_x$
  if $R_e(x) \notin R_e(S)$ **then** ▷ $R_e(Q_x) \neq R_e(Q_y)$ for $\forall y \in X'$
    $X' \leftarrow X' \cup \{x\}$, $Q' \leftarrow Q' \cup Q_x$
    for all $a \in Q_x$ **do**
      if $R_e(a) \notin R_e(N)$ **then**
        $N \leftarrow N \cup \{a\}$
      end if
    end for
    if $R_e(N) \cap R_e(S) = \emptyset$ **then**
      $S \leftarrow S \cup N$, $N \leftarrow \emptyset$
    else
      return FAIL ▷ Lemma 28
    end if
  end if
until $A = \emptyset$
if $|\operatorname{Dis}(Q)| \neq |S|$ or $|Q'| \nmid |Q|$ **then**
  return FAIL
else
  return $(X, \{Q_x : x \in X\}, X', Q', S)$
end if

If we find Q_x, Q_y such that $|R_e(Q_x)| \neq |R_e(Q_y)|$, or $R_e(Q_x) \neq R_e(Q_y)$ and $R_e(Q_x) \cap R_e(Q_y) \neq \emptyset$, we know that Q is not affine by Lemma 29.
We defined the set S so that for every $x, y \in S$,

$$L_x(e) = R_e(x) \neq R_e(y) = L_e(y),$$

so L_x for $x \in S$ are pairwise distinct; and we know from the definition of $\mathrm{Dis}(Q)$ that $\{L_a L_e^{-1} : a \in S\} \subseteq \mathrm{Dis}(Q)$. Hence if $|\mathrm{Dis}(Q)| = |S|$, the two sets must be equal and

$$\mathrm{Dis}(Q) = \{L_a L_e^{-1} \ : \ a \in S\}.$$

On the other hand, if $|\mathrm{Dis}(Q)| > |S|$ or $|Q'| \nmid |Q|$, we know that Q is not affine: if Q is affine, then Q' is an essential subquandle of Q by Lemma 28. We have $S \subseteq Q'$ such that $R_e : S \to \mathrm{Im}(R_e)$ is a bijection so by Lemma 30, the left translations in $L_S = \{L_x : x \in S\}$ are pairwise distinct and $\mathrm{Dis}(Q) = \{L_x L_e^{-1} : x \in S\}$, so it must be true that $|S| = |\mathrm{Dis}(Q)|$. By Theorem 13, $Q \simeq Q' \times \mathrm{Proj}(m(Q))$, so $|Q| = |Q'| \cdot m(Q)$.

We continue with checking whether Q' is affine.

Algorithm 3 `IsEssConfigAffine`

Input: a quandle Q, $\mathrm{Dis}(Q)$ and $(X, \{Q_x : x \in X\}, X', Q', S)$ essential configuration in Q
Output: decides if Q' is affine

1: **if** $|Q'| = |Q_x|$ **then**
2:     **return** TRUE $\triangleright$ Proposition 2(3)
3: **end if**
4: **for all** $x, y \in S$ **do**
5:     find $z \in S$ such that $L_z L_e^{-1} = L_x L_e^{-1} L_y L_e^{-1}$
6:     **if** $L_x L_e^{-1}(R_e(y)) \neq R_e(z)$ **then** $\triangleright$ equation (4.3)
7:         **return** FALSE
8:     **end if**
9: **end for**
10: **for all** $x \in S$, $y \in Q'$ **do**
11:     **if** $R_e(L_x L_e^{-1}(y)) \neq L_{R_e(x)} L_e^{-1}(R_e(y))$ **then** $\triangleright$ equation (4.4)
12:         **return** FALSE
13:     **end if**
14: **end for**
15: **return** TRUE

If $|Q'| = |Q_x|$ then Q' is connected and medial, therefore affine by Proposition 2.
We have an essential configuration $(X, \{Q_x : x \in X\}, X', Q', S)$ in Q. Since $S \subseteq Q'$ and $\mathrm{Dis}(Q') = \{L_x L_e^{-1} : x \in S\}$, clearly $\mathrm{Dis}(Q') = \mathrm{Dis}(Q)$. To show that Q' is affine by Lemma 31, it remains to check if the equations (4.3) and (4.4) stand. That is done in the two for-cycles on lines 4 to 14. If they pass, by Lemma 31 Q' is affine because it is finite.
On the other hand, if Q' is affine then the equalities (4.3) and (4.4) must stand by Lemma 30 because they are the same as the equalities (4.1) and (4.2). So if

any of the conditions above are not satisfied, then Q' is not affine.

In the last part of the algorithm, we have $(X, \{Q_x : x \in X\}, X', Q', S)$, an essential configuration in Q, where Q' is affine and $m = |Q|/|Q'|$; and we decide whether $Q \simeq Q' \times \mathrm{Proj}\,(m)$.

Algorithm 4 `IsDirectlyDecomposable`

Input: a quandle Q, $\mathrm{Dis}\,(Q)$ and $(X, \{Q_x : x \in X\}, X', Q', S)$ essential configuration in Q where Q' is affine, $m = |Q|/|Q'|$
Output: decides if $Q \simeq Q' \times \mathrm{Proj}\,(m)$

$A \leftarrow Q \setminus Q'$
for $i = 1 \rightarrow m-1$ **do**
    if $R_e\,(A) = \mathrm{Im}\,(R_e)$ **then** $\quad \triangleright\ \exists Q^i \subseteq A$ such that $R_e\,(Q^i) = \mathrm{Im}\,(R_e)$
        $Q^i \leftarrow \emptyset$
        repeat
            find $x \in A ::\ R_e\,(x) \notin R_e\,(Q^i)$ $\quad \triangleright\ R_e\,(Q_x) \neq R_e\,(Q_y)\,, \forall Q_y \subseteq Q^i$
            if $R_e\,(Q_x) \cap R_e\,(Q^i) = \emptyset$ **then**
                $Q^i \leftarrow Q^i \cup Q_x$
                $A \leftarrow A \setminus Q_x$
            else
                return FALSE $\quad \triangleright$ Lemma 29
            end if
        until $R_e\,(Q^i) = \mathrm{Im}\,(R_e)$
        $B \leftarrow Q^i$
        for all $x \in X'$ **do**
            if $\exists y \in B$ such that $R_e\,(x) = R_e\,(y)$ **then**
                $\lambda_i\,(x) = y$
                $B \leftarrow B \setminus Q_y$
            else
                return FALSE $\quad \triangleright$ Lemma 34(1)
            end if
        end for
        for all $x \in X'$ and $a \in S$ **do**
            if $R_e L_a L_e^{-1}\,(x) \neq R_e L_a L_e^{-1}\,(\lambda_i\,(x))$ **then**
                $Q \not\simeq Q' \times \mathrm{Proj}\,(m)$
            end if
            for all $y \in X'$ and $b \in S$ **do**
                find $z \in X'$, $c \in S ::\ L_a L_e^{-1}\,(x) * L_b L_e^{-1}\,(y) = L_c L_e^{-1}\,(z)$
                if $L_c L_e^{-1}\,(\lambda_i\,(z)) \neq L_a L_e^{-1}\,(\lambda_i\,(x)) * L_b L_e^{-1}\,(\lambda_i\,(y))$ **then**
                    return FALSE $\quad \triangleright$ Lemma 34(2)
                end if
            end for
        end for
    else
        return FALSE $\quad \triangleright$ Lemma 35
    end if
end for
return TRUE $\quad \triangleright$ Lemma 36

The main for-cycle has $m-1$ iterations. In a successful i-th iteration we first find $Q^i \subseteq A$ as a union of orbits such that $R_e(Q_x) \cap R_e(Q_y) = \emptyset$ and $R_e(Q^i) = \mathrm{Im}(R_e)$, where $A = Q \setminus \{Q' \cup \bigcup_{j<i} Q^j\}$.

If we find Q_x, Q_y such that $R_e(Q_x) \neq R_e(Q_y)$ and $R_e(x) \cap R_e(y) \neq \emptyset$, we know that Q is not affine by Lemma 29 and therefore cannot be isomorphic to the affine quandle $Q' \times \mathrm{Proj}(m)$.

At this point if we have Q^i such that $R_e(Q_x) \cap R_e(Q_y) = \emptyset$ for every $Q_x \neq Q_y$ and $R_e(Q^i) = \mathrm{Im}(R_e)$, we know that $|Q^i| = |Q'|$ and the number of orbits in each set is the same because we assumed $|Q_x| = |Q_y|$ and $|R_e(Q_x)| = |R_e(Q_y)|$ for every $Q_x, Q_y \subseteq Q$.

Next, we define $\lambda_i : X' \hookrightarrow Q^i$ such that $R_e(x) = R_e(\lambda_i(x))$ and $\mathrm{Im}(\lambda_i)$ is a set of orbit representatives in Q'. We put $B = Q^i$ and for each $x \in X'$, we find $y \in B$ such that $R_e(x) = R_e(y)$ and take the orbit Q_y out of B. This ensures that $Q_{\lambda_i(x)} \neq Q_{\lambda_i(y)}$ for $x \neq y \in X'$; and if we are successful, then $\mathrm{Im}(\lambda_i)$ is a set of orbit representatives in Q^i, because the number of orbits in Q' and Q^i is the same as stated above. Clearly if such mapping λ_i exists, this procedure will find it.

The last step is to check whether the mapping

$$\sigma_i : L_a L_e^{-1}(x) \mapsto L_a L_e^{-1}(\lambda_i(x)) \text{ for } x \in X', a \in S$$

is a quandle homomorphism satisfying $R_e(\sigma_i(x)) = R_e(x)$ for every $x \in X'$. This mapping is a bijection of orbits $Q_x \mapsto Q_{\lambda_i(x)}$ because each orbit is the same size as $\mathrm{Dis}(Q) = \{L_a L_e^{-1} : a \in S\}$, the orbits are pairwise distinct and X', $\lambda_i(X')$ are orbit representatives of Q', Q^i, respectively. Hence if it is a quandle homomorphism, $Q^i \simeq Q'$.
If Q is affine both Q' and Q^i are essential subquandles of Q by Lemma 28. So if either the mapping λ_i does not exist, or the mapping σ_i is not a quandle isomorphism such that $R_e(\sigma_i(x)) = R_e(x)$ for every $x \in X'$, we would get a contradiction with Lemma 34 so we can state that $Q \not\simeq Q' \times \mathrm{Proj}(m)$.

In the end, if we found isomorphisms $\sigma_i : Q' \to Q^i$ such that $R_e(\sigma_i(x)) = R_e(x)$ for every Q^i, then by Lemma 36 $Q \simeq Q' \times \mathrm{Proj}(m)$.
If in the beginning of i-th iteration, $i < m$, we find out that $R_e(A) \neq \mathrm{Im}(R_e)$, we know that Q is not affine. This is because in Lemma 35 we showed that every affine quandle is a disjoint union of its affine subquandles and we choose the orbits that we add to Q^i in a way that if the essential subquandle exists, the algorithm will find it. So if $R_e(A) \subsetneq \mathrm{Im}(R_e)$, then Q cannot be written as a disjoint union of subquandles Q^i such that for every Q^i, $R_e(Q^i) = \mathrm{Im}(R_e)$ and $R_e(Q_x) \cap R_e(Q_y)$ for every $Q_x \neq Q_y \subseteq Q^i$.

4.3 Example

Again we will look at the quandle Q from Example 1 on page 16. This time we will rename the elements and ignore everything except for the Cayley table of the quandle; this will demonstrate how the algorithm works.

$(0,0,0)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$
a	b	c	d	e	f	g	h
$(2,0,0)$	$(2,0,1)$	$(2,1,0)$	$(2,1,1)$	$(3,0,0)$	$(3,0,1)$	$(3,1,0)$	$(3,1,1)$
i	j	k	l	m	n	o	p

Table 4.1: Renaming the elements of Q

The quandle Cayley table appears like this:

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
a	a	b	k	l	g	h	m	n	i	j	c	d	o	p	e	f
b	a	b	k	l	g	h	m	n	i	j	c	d	o	p	e	f
c	i	j	c	d	o	p	e	f	a	b	k	l	g	h	m	n
d	i	j	c	d	o	p	e	f	a	b	k	l	g	h	m	n
e	c	d	i	j	e	f	o	p	k	l	a	b	m	n	g	h
f	c	d	i	j	e	f	o	p	k	l	a	b	m	n	g	h
g	k	l	a	b	m	n	g	h	c	d	i	j	e	f	o	p
h	k	l	a	b	m	n	g	h	c	d	i	j	e	f	o	p
i	a	b	k	l	g	h	m	n	i	j	c	d	o	p	e	f
j	a	b	k	l	g	h	m	n	i	j	c	d	o	p	e	f
k	i	j	c	d	o	p	e	f	a	b	k	l	g	h	m	n
l	i	j	c	d	o	p	e	f	a	b	k	l	g	h	m	n
m	c	d	i	j	e	f	o	p	k	l	a	b	m	n	g	h
n	c	d	i	j	e	f	o	p	k	l	a	b	m	n	g	h
o	k	l	a	b	m	n	g	h	c	d	i	j	e	f	o	p
p	k	l	a	b	m	n	g	h	c	d	i	j	e	f	o	p

First we find $\mathrm{Dis}\,(Q)$. At first glance we can see that

$$\mathrm{Dis}\,(Q) = \langle L_aL_c^{-1}, L_aL_e^{-1}, L_aL_g^{-1}, L_cL_e^{-1}, L_cL_g^{-1}, L_eL_g^{-1}\rangle.$$

These mappings are quandle automorphisms and can be written as permutations of Q:

$$\begin{aligned}
L_aL_c^{-1} &= (ai)\,(bj)\,(ck)\,(dl)\,(em)\,(fn)\,(go)\,(hp)\\
L_aL_e^{-1} &= (ac)\,(bd)\,(eg)\,(fh)\,(ik)\,(jl)\,(mo)\,(np)\\
L_aL_g^{-1} &= (ak)\,(bl)\,(ci)\,(dj)\,(eo)\,(fp)\,(gm)\,(hn)\\
L_cL_e^{-1} &= (ak)\,(bl)\,(ci)\,(dj)\,(eo)\,(fp)\,(gm)\,(hn)\\
L_cL_g^{-1} &= (ac)\,(bd)\,(eg)\,(fh)\,(ik)\,(jl)\,(mo)\,(np)\\
L_eL_g^{-1} &= (ai)\,(bj)\,(ck)\,(dl)\,(em)\,(fn)\,(go)\,(hp)\,.
\end{aligned}$$

So we can see that the generators of $\mathrm{Dis}\,(Q)$ are $L_aL_c^{-1}, L_aL_e^{-1}, L_aL_g^{-1}$ and it is easy to confirm that

$$\begin{aligned}
L_aL_c^{-1}L_aL_e^{-1} &= L_aL_e^{-1}L_aL_c^{-1} = L_aL_g^{-1}\\
L_aL_g^{-1}L_aL_e^{-1} &= L_aL_e^{-1}L_aL_g^{-1} = L_aL_c^{-1}\\
L_aL_c^{-1}L_aL_g^{-1} &= L_aL_g^{-1}L_aL_c^{-1} = L_aL_e^{-1}
\end{aligned}$$

so $\mathrm{Dis}(Q) = \{\mathrm{id}, L_a L_c^{-1}, L_a L_e^{-1}, L_a L_g^{-1}\} \simeq \mathbb{Z}_2^2$ is an abelian group. We will choose the unit to be e. We find

$$Q_e = \{e, L_a L_c^{-1}(e), L_a L_e^{-1}(e), L_a L_g^{-1}(e)\} = \{e, g, m, o\}$$

and clearly $|Q_e| < |Q|$ so Q is not connected.

Now we use Algorithm 2 to construct an essential configuration. At this moment, $S = \{e\}$. We iterate through the values of $R_e(Q_e)$ and if we find $a \in Q_e$ such that $R_e(a) \notin R_e(S)$, we add a to S. After this step, we have $S = \{e, m\}$, and we set $q = 4, a = 2$.

Next we define sets $A = Q \setminus Q_e$, $X = \{e\}$, $X' = \{e\}$, $Q' = Q_e$ and $N = \emptyset$. In each step of the for-cycle, we take $x \in A$ and find the orbit Q_x, add x to the set X and take Q_x out of A. We test if $R_e(S)$ contains $R_e(x)$ and if it does not, we iterate through Q_x and add to the set N all elements of Q_x such that their R_e-values are pairwise distinct. If at the end $R_e(S) \cap R_e(N) = \emptyset$, we set $S = S \cup N$ and $N = \emptyset$, otherwise we reject the quandle as not affine. The next list represents the progress of the algorithm:

1. $X = \{e\}$, $X' = \{e\}$, $Q' = Q_e$ and $S = \{e, g\}$
2. $X = \{e, a\}$, $X' = \{e, a\}$, $Q' = Q_e \cup Q_a$ and $S = \{e, g, a, c\}$
3. $X = \{e, a, b\}$, $X' = \{e, a\}$, $Q' = Q_e \cup Q_a$ and $S = \{e, g, a, c\}$
4. $X = \{e, a, b, f\}$, $X' = \{e, a\}$, $Q' = Q_e \cup Q_a$ and $S = \{e, g, a, c\}$

where the orbits and their values in R_e are the following:

$$\begin{aligned} Q_a &= \{a, c, i, k\}, \quad R_e(Q_a) = \{g, o\} \\ Q_b &= \{b, d, j, l\}, \quad R_e(Q_b) = \{g, o\} \\ Q_f &= \{f, h, n, p\}, \quad R_e(Q_f) = \{e, m\} \end{aligned} \tag{4.7}$$

For all the orbits, $|Q_x| = 4$ and $|R_e(Q_x)| = 2$. Clearly in steps 3. and 4., $R_e(b) = g \in R_e(S)$ and $R_e(f) = e \in R_e(S)$, so we do not add any more elements to S, X' and Q'.

All the conditions regarding the size of Q are satisfied: $|\mathrm{Dis}(Q)| = 4 = |S|$ and we can put $m = |Q|/|Q'| = 2$ and

$$\mathrm{Dis}(Q) = \{L_g L_e^{-1}, L_a L_e^{-1}, L_c L_e^{-1}, \mathrm{id}\},$$

so we have an essential configuration.

We use Algorithm 3 to check if Q' is affine. It has two orbits so it is not connected. We can see that when we compose any two mappings of $\mathrm{Dis}(Q)$, we get the third non-trivial one. So in the first iteration cycle we check

- $L_a L_e^{-1} R_e(c) = R_e(g) = m$
- $L_a L_e^{-1} R_e(g) = R_e(c) = o$
- $L_c L_e^{-1} R_e(g) = R_e(a) = g$

- $L_c L_e^{-1} R_e(a) = R_e(g) = m$
- $L_g L_e^{-1} R_e(a) = R_e(c) = o$
- $L_g L_e^{-1} R_e(c) = R_e(a) = g$

and in the second cycle, we check for every $x \in S$ and $y \in Q'$ that $R_e L_x L_e^{-1}(y) = L_{R_e(x)} L_e^{-1} R_e(y)$. The algorithm will go element by element to check if the equalities stand. But if we have a closer look, we can see that it is quite easy to compare the mappings $R_e L_x L_e^{-1} = L_{R_e(x)} L_e^{-1} R_e$. We can see that R_e works in the following way:

$$\begin{aligned} R_e(\{a, i\}) &\mapsto g \\ R_e(\{c, k\}) &\mapsto o \\ R_e(\{e, m\}) &\mapsto e \\ R_e(\{g, o\}) &\mapsto m \end{aligned}$$

and from the permutation form of the mappings in $\mathrm{Dis}(Q)$ we can see that both $L_a L_e^{-1}$ and $L_c L_e^{-1}$ switch the elements of the sets $R_e^{-1}(g)$, $R_e^{-1}(o)$ and $R_e^{-1}(e)$, $R_e^{-1}(m)$, so

$$R_e L_a L_e^{-1} = R_e L_c L_e^{-1} = (og)(em) \circ R_e$$

and the mapping $L_g L_e^{-1}$ only permutes the elements in each of the sets $R_e^{-1}(x)$, $x \in S$, so $R_e L_g L_e^{-1} = R_e$. On the other hand,

$$L_g L_e^{-1} R_e = (ai)(ck)(em)(go) \circ R_e = (og)(em) \circ R_e$$

because the remaining elements of Q' never show up on the outcome of R_e, so we can leave them out.

- $R_e L_a L_e^{-1} = (og)(em) \circ R_e = L_g L_e^{-1} R_e = L_{R_e(a)} L_e^{-1} R_e$
- $R_e L_c L_e^{-1} = (og)(em) \circ R_e = L_g L_e^{-1} R_e = L_o L_e^{-1} R_e = L_{R_e(c)} L_e^{-1} R_e$
- $R_e L_g L_e^{-1} = R_e = L_e L_e^{-1} R_e = L_m L_e^{-1} R_e = L_{R_e(g)} L_e^{-1} R_e$
- $R_e L_e L_e^{-1} = R_e = L_{R_e(e)} L_e^{-1} R_e$

So we can see that the mappings satisfy the equalities required by the algorithm and therefore Q' is affine.

Now we get to the last part, Algorithm 4: checking whether $Q \simeq Q' \times \mathrm{Proj}(2)$. Since $m = 2$, the cycle will do only one iteration.

Certainly $Q^1 = Q_b \cup Q_f$, $R_e(Q_b) \cap R_e(Q_f) = \emptyset$, as we saw in equation (4.7). The mapping λ_1 can be defined as

$$\lambda_1(e) = f, \quad \lambda_1(a) = b$$

where

$$R_e(f) = e = R_e(e), \quad R_e(b) = g = R_e(a).$$

Now we check if

$$\sigma_1 : L_a L_e^{-1}(x) \mapsto L_a L_e^{-1}(\lambda_1(x)), \ \ x \in X', a \in S$$

is a quandle homomorphism such that $R_e(\sigma(x)) = R_e(x)$ for every $x \in Q'$.
We will go through one iteration of the cycle for $a \in X'$ and $g \in S$. First we check that

$$R_e L_g L_e^{-1}(a) = R_e L_g L_e^{-1}(b) = g$$

so we can proceed to the inner for-cycle: we iterate through X' and S and verify the homomorphism equation. In each iteration we calculate the product in Q' and then apply σ_1, and see if we get the same result as when we apply σ_1 on the elements first and then multiply.

$$\begin{gathered}
L_g L_e^{-1}(a) * L_e L_e^{-1}(a) = i * a = a = L_e L_e^{-1}(a) \\
L_g L_e^{-1}(a) * L_a L_e^{-1}(a) = i * c = k = L_c L_e^{-1}(a) \\
L_g L_e^{-1}(a) * L_g L_e^{-1}(a) = i * i = i = L_g L_e^{-1}(a) \\
L_g L_e^{-1}(a) * L_c L_e^{-1}(a) = i * k = c = L_a L_e^{-1}(a) \\
L_g L_e^{-1}(a) * L_e L_e^{-1}(e) = i * e = g = L_a L_e^{-1}(e) \\
L_g L_e^{-1}(a) * L_a L_e^{-1}(e) = i * g = m = L_g L_e^{-1}(e) \\
L_g L_e^{-1}(a) * L_g L_e^{-1}(e) = i * m = o = L_c L_e^{-1}(e) \\
L_g L_e^{-1}(a) * L_c L_e^{-1}(e) = i * o = e = L_e L_e^{-1}(e)
\end{gathered}$$

Applying σ_1 on the result means applying λ_1 on the argument of the mappings; i.e., switching a for b and e for f. And now in Q^1:

$$\begin{gathered}
L_g L_e^{-1}(b) * L_e L_e^{-1}(b) = j * b = b = L_e L_e^{-1}(b) \\
L_g L_e^{-1}(b) * L_a L_e^{-1}(b) = j * d = l = L_c L_e^{-1}(b) \\
L_g L_e^{-1}(b) * L_g L_e^{-1}(b) = j * j = j = L_g L_e^{-1}(b) \\
L_g L_e^{-1}(b) * L_c L_e^{-1}(b) = j * l = d = L_a L_e^{-1}(b) \\
L_g L_e^{-1}(b) * L_e L_e^{-1}(f) = j * f = h = L_a L_e^{-1}(f) \\
L_g L_e^{-1}(b) * L_a L_e^{-1}(f) = j * h = n = L_g L_e^{-1}(f) \\
L_g L_e^{-1}(b) * L_g L_e^{-1}(f) = j * n = p = L_c L_e^{-1}(f) \\
L_g L_e^{-1}(b) * L_c L_e^{-1}(f) = j * p = f = L_e L_e^{-1}(f)
\end{gathered}$$

and we can see that the results are the same as in the first case.

The other iterations would verify that the same equalities stand for the remaining elements of X' and S; and it is needless to say that we would confirm that σ_1 is a quandle homomorphism such that $R_e(\sigma_1(x)) = R_e(x)$ for every $x \in Q'$.

So all the conditions are satisfied; $Q \simeq Q' \times \mathrm{Proj}(2)$ so Q is affine.

Bibliography

[1] Colin C. Adams. *The Knot Book*. American Mathematical Society, 2004.

[2] J. W. Alexander. Topological invariants of knots and links. *Transactions of the American Mathematical Society*, 30(2):275–306, 1928.

[3] J. W. Alexander and G. B. Briggs. On types of knotted curves. *The Annals of Mathematics*, 28(1/4):562–586, 1926-1927.

[4] P. Freyd, D. Yetter, J. Hoste, W. B. R. Lickorish, Millett K., and A. Ocneanu. A new polynomial invariant of knots and links. *Bulletin of the American Mathematical Society*, 12(2):239–246, 1985.

[5] C. McA. Gordon and J. Luecke. Knots are determined by their complements. *Journal of the American Mathematical Society*, 2(2):371–415, 1989.

[6] Christopher J. Hillar and Darren L. Rhea. Automorphisms of finite abelian groups. *The American Mathematical Monthly*, 114(10):917–923, 2007.

[7] Xiang-Dong Hou. Automorphism groups of Alexander quandles. *Journal of Algebra*, 344(1):373–385, 2011.

[8] Xiang-Dong Hou. Finite modules over $\mathbb{Z}[t, t^{-1}]$. *J. Knot Theory Ramificarions*, 21(8), 2012.

[9] Alexander Hulpke, David Stanovský, and Petr Vojtěchovský. Connected Quandles and Transitive Groups. *preprint*, 2013.

[10] Ayumu Inoue. Quandle homomorphisms of knot quandles to Alexander quandles. *J. Knot Theory Ramifications*, 10(6):813–821, 2001.

[11] Vaughan Jones. A polynomial invariant of knots via Von Neumann algebras. *Bulletin of the American Mathematical Society*, 12(1):103–111, 1985.

[12] David Joyce. A classifying invariant of knots, the knot quandle. *Journal of Pure and Applied Algebra*, 23(1):37–65, 1982.

[13] Vassily Manturov. *Knot Theory*. CRC Press, 2004.

[14] Vladimir S. Matveev. Distributive grupoids in knot theory. *Matematicheskii Sbornik*, 119(161)(1(9)):78–88, 1982.

[15] Gabriel Murillo and Sam Nelson. Alexander quandles of order 16. *J. Knot Theory Ramifications*, 17(3):273–278, 2008.

[16] Gabriel Murillo, Sam Nelson, and Anthony Thompson. Matrices and finite Alexander quandles. *J. Knot Theory Ramifications*, 16(6):769–778, 2007.

[17] Sam Nelson. Classification of finite Alexander quandles. *Proceedings of the Spring Topology and Dynamical Systems Conference*, 27(1):245–258, 2003.

[18] Jozef H. Przytycki and Pawel Traczyk. Invariants of links of Conway type. *Kobe Journal of Mathematics*, 4(2):115139, 1988.

[19] Kurt Reidemeister. Elementare Begrndung der Knotentheorie. *Abhandlungen aus dem Mathematischen Seminar der Universitt Hamburg*, 5(1):24–32, 1927.

[20] Masahico Saito. Small connected quandles and their knot colorings. `http://shell.cas.usf.edu/~saito/QuandleColor/`.