An Algebraic Approach to Symmetry with Applications to Knot Theory

by

David Edward Joyce

A dissertation in mathematics

Presented to the Graduate Faculty of the University of Pennsylvania in partial fulfillment of the requirements for the degree of Doctor of Philosophy

1979

[signed]
Peter J. Freyd
Supervisor of Dissertation

[signed] Jerry L. Kazdan
Graduate Group Chairman

Preface

This edition of my dissertation differs little from the original 1979 version. This edition is typeset in LaTeX, whereas the original was typed on a typewriter and the figures were hand drawn. The page numbers and figure numbers are changed, the table of contents is expanded to include sections, a list of figures is included, and the index appears at the end instead of the front. I've corrected a few typos (and probably added others), and I added figure 4.5 that was missing from the original.

David Joyce
June, 2009

Acknowledgments

I thank my friends for their tolerance, nay, for their encouragement, of the investigation of the mathematics herein presented. I owe much to Julian Cole for many encouraging discussions and for some suggestions concerning nomenclature. I owe much more to my adviser, Peter Freyd, for his continued guidance of my mathematical maturity and for many discussions in many fields, mathematical and otherwise. I give special thanks to Janet Burns for the fine job of typing this dissertation.

Abstract

The usual algebraic construction used to study the symmetries of an object is the group of automorphisms of that object. In many geometric settings, however, one may interpret the symmetries in a more intimate manner by an algebraic structure on the object itself. Define a *quandle* to be a set equipped with two binary operations, $(x, y) \mapsto x \triangleright y$ and $(x, y) \mapsto x \triangleright^{-1} y$, which satisfies the axioms

Q1. $x \triangleright x = x$.

Q2. $(x \triangleright y) \triangleright^{-1} y = x = (x \triangleright^{-1} y) \triangleright y$.

Q3. $(x \triangleright y) \triangleright z = (x \triangleright z) \triangleright (y \triangleright z)$.

Call the map $S(y)$ sending x to $x \triangleright y$ the *symmetry* at y.

To each point y of a symmetric space there is a symmetry $S(y)$ of the space. By defining $x \triangleright y = x \triangleright^{-1} y$ to be the image of x under $S(y)$, the symmetric space becomes a quandle. Call a quandle satisfying $x \triangleright y = x \triangleright^{-1} y$ an *involutory* quandle. Loos [1] has defined a symmetric space as a manifold with an involutory quandle structure such that each point y is an isolated fixed point of $S(y)$.

The underlying set of a group G along with the operations of conjugation, $x \triangleright y = y^{-1}xy$ and $x \triangleright^{-1} y = yxy^{-1}$ form a quandle $\operatorname{Conj} G$. Moreover, the theory of conjugation may be regarded as the theory of quandles in the sense that any equation in $\triangleright$ and $\triangleright^{-1}$ holding in $\operatorname{Conj} G$ for all groups G also holds in any quandle. If the center of G is trivial, then $\operatorname{Conj} G$ determines G.

Let G be a group and $n \geq 2$. The *n-core* of G is the set

$$\{(x_1, x_2, \ldots, x_n) \in G^n \mid x_1 x_2 \ldots x_n = 1\}$$

along with the operation

$$(x_1, x_2, \ldots, x_n) \triangleright (y_1, y_2, \ldots, y_n) = (y_n^{-1} x_n y_1, y_1^{-1} x_1 y_2, \ldots, y_{n-1}^{-1} x_{n-1} y_n).$$

The n-core is an *n-quandle*, that is, each symmetry has order dividing n. The group G is simple if and only if its n-core is a simple quandle.

Let G be a noncyclic simple group and Q a nontrivial conjugacy class in H viewed as a subquandle of $\operatorname{Conj} G$. Then Q is a simple quandle.

Let Q be a quandle. The *transvection group* of Q, $\operatorname{Trans} Q$, is the automorphism group of Q generated by automorphisms of the form $S(x)S(y)^{-1}$ for x, y in Q. Suppose Q is a simple p-quandle where p is prime. Then either $\operatorname{Trans} Q$ is a simple group, or else Q is the p-core of a simple group G and $\operatorname{Trans} Q = G^p$.

Consider the category of pairs of topological spaces $(X, K), K \subseteq X$, where a map $f : (X, K) \to (Y, L)$ is a continuous map $f : X \to Y$ such that $f^{-1}(L) = K$. Let (D, O) be the closed unit disk paired with the origin O. Call a map from (D, O) to (X, K) a *noose* in X about K. The homotopy classes of nooses in X about K form the *fundamental quandle* $Q(X, K)$. The inclusion of the unit circle to the boundary of D gives a natural transfromation from $Q(X, K)$ to the fundamental group $\pi_1(X - K)$. A statement analogous to the Seifert-Van Kampen theorem for the fundamental group holds for the fundamental quandle.

Let K be an oriented knot in the 3-sphere X. Define the *knot quandle* $Q(K)$ to be the subquandle of $Q(X, K)$ consisting of nooses linking once with K. Then $Q(K)$ is a classifying invariant of tame knots, that is, if $Q(K) = Q(K')$, then K is equivalent to K'. The knot group and the Alexander invariant can be computed from $Q(K)$.

[1] Loos, O., *Symmetric Spaces*, Benjamin, New York, 1969.

Contents

List of Figures

Chapter 1

Definitions and Examples

1.1 Quandles

Let Q be a set equipped with a binary operation, and denote this operation by $(x, y) \mapsto x \triangleright y$. We use the nonsymmetric symbol $\triangleright$ here since the two variables will play different roles in the following discussion. Also, it will distinguish this binary operation from others that Q may have, in particular, addition and multiplication.

For z in Q, let $S(z)$ be the function on Q whose value at x is $x \triangleright z$. It will be more convenient for us to use the notation $xS(z) = x \triangleright z$ rather than $S(z)(x) = x \triangleright z$. For $S(z)$ to be a homomorphism, we require

$$(x \triangleright y)S(z) = xS(z) \triangleright yS(z),$$

that is,

$$(x \triangleright y) \triangleright z = (x \triangleright z) \triangleright (y \triangleright z). \tag{1}$$

When (1) holds for all x, y, z in Q, S is a function from Q to $\operatorname{End} Q$, the set of endomorphisms of Q. If $S(z)$ is also a bijection for all z, then S maps Q to $\operatorname{Aut} Q$, the group of automorphisms of Q. Any group, in particular $\operatorname{Aut} Q$, has the operation of conjugation, $f \triangleright g = g^{-1}fg$, which satisfies (1). Then $S : Q \to \operatorname{Aut} Q$ is itself a homomorphism. That is $S(y \triangleright z) = S(z)^{-1}S(y)S(z)$, equivalently, $S(z)S(y \triangleright z) = S(y)S(z)$, which is a restatement of (1). The requirement that $S(z)$ be a bijection for all z is equivalent to the existence of another binary operation

$$(x, y) \mapsto x \triangleright^{-1} y$$

that satisfies

$$x \triangleright y = z \iff x = z \triangleright^{-1} y. \tag{2}$$

An equational identity equivalent to (2) is

$$(x \triangleright y) \triangleright^{-1} y = x = (x \triangleright^{-1} y) \triangleright y. \tag{3}$$

From (1) and (2) we may derive the identities

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

In all the applications that follow, $S(z)$ will not only be an automorphism, but one which fixes z.

Definition. A *quandle* is a set Q equipped with two binary operations $(x, y) \mapsto x \triangleright y$ and $(x, y) \mapsto x \triangleright^{-1} y$ which satisfies three axioms

Q1. $$x \triangleright x = x.$$

Q2. $$(x \triangleright y) \triangleright^{-1} y = x = (x \triangleright^{-1} y) \triangleright y.$$

Q3. $$(x \triangleright y) \triangleright z = (x \triangleright z) \triangleright (y \triangleright z).$$

The map $S(z)$ is called *the symmetry at* z, and $x \triangleright z$ may be read as "x through z". The axioms taken together say that the symmetry at any point of Q is an automorphism of Q fixing that point. The *order* of a quandle is the cardinality of its underlying set. The elements of a quandle will be frequently referred to as points.

Example 1. A group G is a quandle, denoted $\operatorname{Conj} G$, with conjugation as the operation. $x \triangleright y = y^{-1}xy$, $x \triangleright^{-1} y = yxy^{-1}$. Any conjugacy class of G is a subquandle of $\operatorname{Conj} G$ as is any subset closed under conjugation. When G is Abelian, the operation becomes simply the first projection operation, $x \triangleright y = x$.

Definition. A quandle Q is said to be *Abelian* if it satisfies

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

It follows from the definition that an Abelian quandle also satisfies the identities

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

Example 2. Let T be a nonsingular linear transformation on a vector space V. Then V becomes a quandle with the operations $x \triangleright y = T(x - y) + y$ and $x \triangleright^{-1} y = T^{-1}(x - y) + y$. Moreover, V is an Abelian quandle.

It should be noted that quandles are seldom associative. In fact, the identity $(x \triangleright y) \triangleright z = x \triangleright (y \triangleright z)$ is equivalent to the identity $x \triangleright y = x$. One associativity equation which does hold for any quandle is $(x \triangleright y) \triangleright x = x \triangleright (y \triangleright x)$. To reduce the number of parentheses we use the notation $x \triangleright y \triangleright z$ for $(x \triangleright y) \triangleright z$.

By far the most interesting axiom for quandles is the distributivity axiom Q3. The first study of self-distributivity is that of Burstin and Mayer [5]. They define "distributive groups", or in modern terminology, distributive quasigroups. A *quasigroup* is a set G equipped with a binary operation $(x, y) \mapsto xy$ such that for all a, b in G there exist

unique solutions x, y to the equations $xa = b$ and $ay = b$. A quasigroup is *distributive* if it satisfies the two identities

$$\begin{aligned}(xy)z &= (xz)(yz), \text{ and}\\ x(yz) &= (xy)(xz).\end{aligned}$$

It follows that a distributive quasigroup is idempotent, $xx = x$. Hence, quandles are a generalization of distributive quasigroups. Burstin and Mayer define an "Abelian distributive group" to be one satisfying

$$(wx)(yz) = (wy)(xz).$$

This axiom goes by the names "entropy", "mediality", "surcommutativity", and "symmetry".

1.2 Involutory quandles

An important class of quandles are those in which the symmetries $S(z)$ are all involutions, $S(z)^2$ is the identity. In this case $x \triangleright z = x \triangleright^{-1} z$, which allows us to dispense with the second quandle operation. An equivalent condition is the identity

QInv. $$x \triangleright y \triangleright y = x.$$

Definition. A quandle satisfying **QInv** is called an *involutory quandle* or *2-quandle*. Alternatively, an involutory quandle may be defined as a set equipped with a binary operation $(x, y) \mapsto x \triangleright y$ which satisfies **Q1**, **Qinv**, and **Q3**. Analogously an *n-quandle* is a quandle such that for all x, y, $xS(y)^n = x$. In any quandle let $x \triangleright^n y$ denote $xS(y)^n$.

Example 1. Let G be a group. The set of involutions in G, $\operatorname{Inv} G = \{x \in G \mid x^2 = 1\}$, forms an involutory quandle with conjugation as the operation.

Example 2. Any group G has an involutory quandle structure given by $x \triangleright y = yx^{-1}y$. The underlying set of G along with this operation is called the *core* of G and is denoted $\operatorname{Core} G$. Note that $\operatorname{Core} G$, $\operatorname{Conj} G$, and $\operatorname{Inv} G$ are all distinct unless G consists of involutions only.

Example 3. Let M be a Riemannian symmetric space, that is, a connected Riemannian manifold M in which each point y is an isolated fixed point of an involutive isometry $S(y)$. In a neighborhood of y, $S(y)$ is given in terms of the exponential map $\exp : T_y \to M$ (T_y = tangent space at y) as

$$xS(y) = \exp(-\exp^{-1}(x)).$$

Since M is connected, this local involutive isometry is uniquely extendable to M. M is an involutive quandle with the operation $x \triangleright y = xS(y)$. Indeed, **Q1** holds since y is fixed by $S(y)$, and **QInv** holds since $S(y)$ is an involution. To show **Q3** it suffices to show

$S(y \triangleright z) = S(z)S(y)S(z)$. But $S(z)S(y)S(z)$ is an involutive isometry having $y \triangleright z$ as an isolated fixed point, and $S(y \triangleright z)$ is described by this property.

A more descriptive construction of $x \triangleright y$ is the following. If $x = y$, let $x \triangleright y = x$. Otherwise, pass a geodesic through x and y, and let d be the length along the geodesic from x to y. Let $x \triangleright y$ be the point on the geodesic extended through y by the same length d.

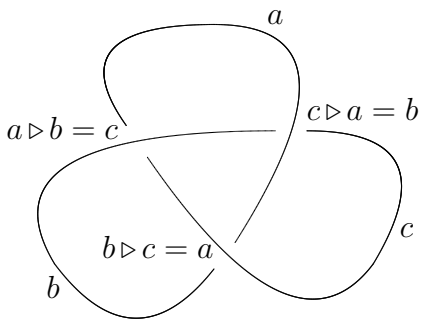
Symmetric spaces give examples of 2-quandles which are not cores of groups. Three basic two-dimensional symmetric spaces are the sphere, Euclidean plane, and hyperbolic plane. The Euclidean plane is the core of the Abelian group $\mathbf{R}^2$, but neither the sphere nor the hyperbolic plane are cores of toplogical groups.

Example 4. The involutory quandle of a knot. Consider a regular projection of a knot K, such as the trefoil knot in figure 1.1, and label the arcs $a, b, c, \ldots$, where by "arc" is meant a segment from one underpass, over whatever overpasses there may be, to the next underpass. At each underpass, read a relation on the arcs, as "a under b gives c" $a \triangleright b = c$. Let $Q(K)$ be the quandle generated by the arcs with relations given by the underpasses. For instance,

$$Q(\text{trefoil}) = (a, b, c : a \triangleright b = c, b \triangleright c = a, c \triangleright a = b)$$

which is isomorphic to $\text{Core}(\mathbf{Z}/3\mathbf{Z})$. The order of $Q(K)$ need not be equal to the number of arcs in the projection; it need not even be finite. A different regular projection of K will give the same $Q(K)$ up to isomorphism. Moreover, if K and K' are equivalent knots, then $Q(K)$ is isomorphic to $Q(K)$. Proofs and precise definitions will be supplied in Chapter 4.

Figure 1.1: The trefoil knot



A similar construction gives the (non-involutory) quandle of a knot. An orientation of the knot is used to determine the relations. As expected, the knot quandle holds more information about the knot than the involutory knot quandle.

M. Takasaki [16] defined involutory quandles under the name "kei". Takasaki's motivation derives form the net (web) theory of Thomsen [17,18]. This theory is described in the book of Blaschke and Bol [2]. A similar geometric basis underlies Moufang's [9] study of loops. Bruck [3] defined the *core* of a Moufang loop as the underlying set of the loop along with the operation $(x, y) \mapsto yx^{-1}y$ (example 2 above). See Chapter 3 more more on loop cores.

Loos discovered the intrinsic algebraic structure of symmetric spaces as explained in Loos [7,9]. Not only are Riemannian symmetric spaces determined by their algebraic structure, but so are affine symmetric spaces. This allows Loos to define a symmetric space as a differentiable involutory quandle in which every point is an isolated fixed point of the symmetry through it.

Chapter 2

Representations and the general algebraic theory of quandles

There are various ways that groups may be used to represent quandles. First of all, $\operatorname{Conj} G$, for G a group, is a quandle. Many quandles may be represented as subquandles of $\operatorname{Conj} G$ for appropriate G. Free quandles, for example, may be so represented. Secondly, homogeneous quandles may be represented as cosets $H\backslash G$ for H a subgroup of G where an automorphism of G fixing H is needed to describe the quandle operations on $H\backslash G$. Non-homogeneous quandles are representable as a union $H_1\backslash G \cup H_2\backslash G \cup \cdots$ where several automorphisms are used to describe the quandle operations. Finally, a quandle may be given by a set Q along with an action of a group G and a function $\epsilon : Q \to G$ that describes the symmetries of the points of Q. Such a construction will be called an augmented quandle. We will be able to study some varieties of quandles by means of augmented quandles.

2.1 The algebraic theory of conjugation

In this section we show that the theory of quandles may be regarded as the theory of conjugation. Consider the two binary operations of conjugation, $(x, y) \mapsto y^{-1}xy = x \triangleright y$ and $(x, y) \mapsto yxy^{-1} = x \triangleright^{-1} y$, on a group. We ask whether there are any equations involving only these two operations which hold uniformly for all groups other than those which hold in all quandles. To this end we show that free quandles may be faithfully represented as unions of conjugacy classes in free groups.

Proposition. Let A be a set and F be the free group on A. Then the free quandle on A appears as the subquandle Q of $\operatorname{Conj} F$ consisting of the conjugates of the generators of F.

Proof. We use the notation of quandles in $\operatorname{Conj} F$. Each element of Q is named as

$$a \triangleright^{e_1} b_1 \triangleright^{e_2} \cdots \triangleright^{e_n} b_n$$

where $a, b_1, \ldots, b_n \in A$ and $e_1, \ldots, e_n \in \{1, -1\}$. That is to say, the conjugates of a are of the form

$$b_n^{-e_n} \cdots b_1^{-e_1} a b_1^{e_1} \cdots b_n^{e_n}.$$

The equivalence on names is generated by two cases.

1. If $a = b_1$, then $a \triangleright^{e_1} b_1 \triangleright^{e_2} \cdots \triangleright^{e_n} b_n$ names the same element as $a \triangleright^{e_2} b_2 \triangleright^{e_3} \cdots \triangleright^{e_n} b_n$.
2. If $b_i = b_{i+1}$ and $e_i + e_{i+1} = 0$, then $a \triangleright^{e_1} b_1 \triangleright^{e_2} \cdots \triangleright^{e_n} b_n$ names the same element as $a \triangleright^{e_1} \cdots \triangleright^{e_{i-1}} b_{i-1} \triangleright^{e_{i+2}} b_{i+2} \triangleright \cdots \triangleright^{e_n} b_n$.

Now let each a in A be assigned to a point $f(a)$ in a quandle P. If f extends to Q, then we must have

$$f(a \triangleright^{e_1} b_1 \triangleright^{e_2} \cdots \triangleright^{e_n} b_n) = f(a) \triangleright^{e_1} f(b_1) \triangleright^{e_2} \cdots \triangleright^{e_n} f(b_n).$$

We must only show that this extension is well-defined. But this follows directly from the fact that in P the analogues of 1) and 2) hold for $f(a) \triangleright^{e_1} f(b_1) \triangleright^{e_2} \cdots \triangleright^{e_n} f(b_n)$. □

Corollary. any equation holding in $\operatorname{Conj} G$ for all groups G holds in all quandles.

Proof. Let E be an equation holding in $\operatorname{Conj} G$ for all groups G. In particular E holds in $\operatorname{Conj} F$ for free groups F, hence, E holds in free quandles. Whence, E holds in all quandles. □

2.2 Automorphism groups of quandles

Let Q be a quandle. We define three automorphism groups for A. First, there is the group consisting of all automorphisms, the *full automorphism group of* Q, $\operatorname{Aut} Q$. Second, there is the subgroup of $\operatorname{Aut} Q$, generated by all the symmetries of Q, called the *inner automorphism group of* Q, $\operatorname{Inn} Q$. Third, there is the subgroup of $\operatorname{Inn} Q$ generated by automorphisms of the form $S(x)S(y)^{-1}$ for $x, y \in Q$, called the *transvection group of* Q, $\operatorname{Trans} Q$. $\operatorname{Inn} Q$ is a normal subgroup of $\operatorname{Aut} Q$, and $\operatorname{Trans} Q$ is normal in both $\operatorname{Inn} Q$ and $\operatorname{Aut} Q$. The quotient group $\operatorname{Inn} Q / \operatorname{Trans} Q$ is a cyclic group. The elements of $\operatorname{Trans} Q$ are the automorphisms of the form $S(x_1)^{e_1} \cdots S(x_n)^{e_n}$ such that $e_1 + \cdots + e_n = 0$.

To illustrate these groups let Q be $\mathbf{R}^2$ with $x \triangleright y = 2y - z$ consered as a quandle in the category of topological spaces. Then $\operatorname{Aut} Q$ consists of the continuous automorphisms of $\mathbf{R}^2$, that is, the affine transformations. $\operatorname{Inn} Q$ includes symmetries at points and translations. $\operatorname{Trans} Q$ includes only translations.

2.3 Representation of quandles as conjugacy classes

Two points x and y of a quandle Q are said to be *behaviorally equivalent* if $z \triangleright x = z \triangleright y$ for all z in Q. An equivalent condition is that $S : Q \to \operatorname{Inn} Q$ identifies x and y. Behavioral equivalence is a congruence relation, $\equiv_b$, on the quandle, and $Q / \equiv_b$ is isomorphic to the

image $S(Q)$ as a subquandle of $\operatorname{Conj}\operatorname{Inn} Q$. The elements of Q are behaviorally distinct if and only if S is an injection, in which case Q is isomorphic to a union of conjugacy classes in $\operatorname{Inn} Q$.

Even if the points of a quandle are not all behaviorally distinct, the quandle may be isomorphic to a union of conjugacy classes of some group. For instance, any quandle satisfying $x \triangleright y = x$ may be embedded in $\operatorname{Conj}(\prod_I \mathbf{Z}_2)$ for sufficiently large I. There is a universal group in which to represent a quandle as a subset closed under conjugation. As noted in example 1 of Chapter 1, every group G may be considered to be a quandle $\operatorname{Conj} G$, with conjugation as the quandle operation. Adjointly, every quandle Q gives rise to a group $\operatorname{Adconj} Q$, generated by the elements of Q modulo the relations of conjugation. Precisely, $\operatorname{Adconj} Q$ has the presentation

$$(\overline{x}, \text{for } x \in Q : \overline{x \triangleright y} = \overline{y}^{-1}\overline{x}\,\overline{y}, \text{for } x, y \in Q\}.$$

The map $\eta : Q \to \operatorname{Conj}\operatorname{Adconj} Q$ sending x to $\overline{x}$ is a quandle homomorphism whose image is a union of conjugacy classes of $\operatorname{Adconj} Q$. The map η has the following universal property: for any quandle homomorphism $h : Q \to \operatorname{Conj} G$, G a group, there exists a unique group homomorphism $H : \operatorname{Adconj} Q \to G$ such that $h = H \circ \eta$. Thus, if any $h : Q \to \operatorname{Conj} G$ is monic, then η is monic.

But η need not be injective in general. Consider the 2-quandle of three elements given in the table in figure 2.1. Since $b \triangleright a = b$, $\overline{a}$ commutes with $\overline{b}$. But $a \triangleright b = c$, so $\overline{b}^{-1}\overline{a}\overline{b} = \overline{c}$. Therefore, $\overline{a} = \overline{c}$, and η is not injective.

Figure 2.1: A singular 2-quandle

$\triangleright$	a	b	c
a	a	c	a
b	b	b	b
c	c	a	c

Later, when we consider the quandle associated to a knot, the non-injectivity of η will be important. For example, the quandles associated to the square and granny knots are distinct, but the Adconj groups of these quandles (which are the knot groups) are isomorphic, and for each, η is not injective.

2.4 Representation of quandles as cosets

Let s be an automorphism on a group G. We may define a quandle operation on G by $x \triangleright y = s(xy^{-1})y$. Verification is straightforward. Let H be a subgroup of G whose elements are fixed by s. Then $H\backslash G$ inherits this quandle structure

$$Hx \triangleright Hy = Hs(xy^{-1})y.$$

Denote this quandle as $(H\backslash G; s)$. G acts on the right on $(H\backslash G; s)$ by $(Hx, y) \mapsto Hxy$, and the action is by quandle automorphisms. Since G acts transitively on $H\backslash G$, it follows that $(H\backslash G; s)$ is a *homogeneous* quandle, that is, there is a quandle automorphism sending any point to any other point of the quandle.

We are mainly interested in the case when s is an inner automorphism of G, $s(x) = z^{-1}xz$ for some fixed element z of G. Then $x \triangleright y = z^{-1}xy^{-1}zy$. When H contains z, the operation of $(H\backslash G; z) = (H\backslash g; s)$ is

$$Hx \triangleright Hy = Hxy^{-1}zy.$$

Proposition. Every homogeneous quandle is representable as $(H\backslash G; z)$.

Proof. Let Q be a homogeneous quandle and $G = \operatorname{Aut} Q$. Fix $p \in Q$. Let $z = S(p)$, symmetry at p, and let s be conjugation by z in G. Then $e : (G; s) \to Q$, evaluation at p, defined by sending the element x to its value at p, is a quandle homomorphism. Indeed, $e(x \triangleright y) = e(z^{-1}xy^{-1}zy) = p\,xy^{-1}zy = (p\,xy^{-1} \triangleright p)y = p\,xy^{-1}y \triangleright py = e(x) \triangleright e(y)$. Since Q is homogeneous, e is surjective. Let H be the stability subgroup of p, $H = \{x \in G \mid px = p\}$. Then e factors through $(H\backslash g; z)$ since $p = pH$. Moreover, $(H\backslash G; z) \to Q$ is injective, for if $pHx = pHy$, then $pxy^{-1} = p$, $xy^{-1} \in H$, and so $Hx = Hy$. Thus, Q is isomorphic to $(H\backslash G; z)$. □

Some adjustments are needed to represent non-homogeneous quandles. Given a group G, elements $z_1, z_2, \ldots$ of G, and subgroups $H_1, H_2, \ldots$ of G such that for each index i, H_i is contained in the centralizer of z_i, we form a quandle $(H_1, H_2, \ldots \backslash G; z_1, z_1, \ldots)$ as the disjoint union of $H_1\backslash G, H_2\backslash G, \ldots$ with the quandle operation

$$H_ix \triangleright H_jy = H_ixy^{-1}z_jy.$$

□

Proposition. Every quandle is representable as $(H_1, H_2, \ldots \backslash G; z_1, z_1, \ldots)$.

Proof. Let Q be a quandle and $G = \operatorname{Aut} Q$. Let $Q_1, Q_2, \ldots$ be the orbits of the action of G on Q. For each index i choose $p_i \in Q_i$, let $z_i = S(p_I)$, and let H_i be the stability subgroup of p_i. Then for each i, H_i is contained in the centralizer of z_i, and so we have a quandle $P = (H_1, H_2, \ldots \backslash G; z_1, z_1, \ldots)$ as described above. Define $e : P \to Q$ by $H_ix \mapsto p_ix$. As in the proof of the previous propsition, e may be shown to be an isomorphism. □

In the case of involutory quandles, the automorphism s of G must be an involution on G while the elements $z, z_1, z_2, \ldots$ of g must be involutions in G.

2.5 Algebraic connectivity

We say that a quandle Q is *algebraically connected* (or just *connected* when there will be no confusion with topological connectivity) if the inner automorphism group $\operatorname{Inn} Q$ acts

transitively on Q. In other words, Q is connected if and only if for each pair a, b in Q there are $a_1, a_2, \ldots, a_n$ in Q and $e_1, e_2, \ldots, e_n \in \{1, -1\}$ such that

$$a \triangleright^{e_1} a_1 \triangleright^{e_2} \cdots \triangleright^{e_n} a_n = b.$$

Let Q be a quandle and q a point of Q. The *q-fibre* of a map $g : Q \to Q''$ is the subquandle $Q' = \{p \in Q \,|\, g(p) = g(q)\}$ of Q. Suppose that Q'' is a quotient of Q, that is, Q'' is given by a congruence on Q. In general the q-fibre does not determine Q''; just consider quandles whose operation is the first projection.

Proposition. Let Q be an algebraically connected quandle and q a point of Q. Then every quotient of Q is determined by its q-fibre. Consequently, every congruence on Q is determined by any one of its congruence classes.

Proof. Let Q'' be a quotent of Q with q-fibre Q'. Let $a, b \in Q$. By the connectivity of Q there is an inner automorphism x such that $ax = q$. Since homomorphisms respect inner automorphisms, it follows that $g(a) = g(b)$ if and only if $g(ax) = g(bx)$. Hence, $g(a) = g(b)$ if and only if $\exists x \in \operatorname{Inn} Q$ such that $ax = q$ and $bx \in Q'$. Thus, Q' determines Q''. □

2.6 The transvection group

As defined above, the transvection group $\operatorname{Trans} Q$ of a quandle Q is the subgroup of $\operatorname{Inn} Q$ generated by automorphisms of the form $S(x)S(y)^{-1}$. $\operatorname{Trans} Q$ is a normal subgroup of $\operatorname{Inn} Q$ with cyclic quotient. Alternatively, we may define a *transvection* on Q as an automorphism of Q of the form $S(x_1)^{e_1} \cdots S(x_n)^{e_n}$ with $x_i \in Q$, $e_i \in \mathbf{Z}$, $i = 1, \ldots, n$, such that $e_1 + \cdots + e_n = 0$. Then $\operatorname{Trans} Q$ is the group of transvections on Q.

Some the the properties of Q are reflected in $\operatorname{Trans} Q$.

Proposition. A quandle is Abelian if and only if its transvection group is Abelian.

Proof. Let Q be a quandle with transvection group T. By definition, Q is Abelian if and only if

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

Equivalently,

$$S(x)S(z)^{-1}S(y) = S(y)S(z)^{-1}S(x).$$

On the other hand, T is Abelian if and only if

$$S(x)S(z)^{-1}S(y)S(t)^{-1} = S(y)S(t)^{-1}S(x)S(z)^{-1}.$$

By setting $t = z$ we find that if T is Abelian then Q is Abelian. From Q Abelian follows

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

which implies that T is Abelian. □

2.7 n-Cores

The core of a group has the property that all its symmetries are involutions. In this section we define an n-core of a group wherein the n-th power of each symmetry is the identity. This agrees with the usual core in the case $n = 2$.

Let G be a group and n a positive integer. The wreath product $G \wr \mathbf{Z}_n$ consists of $n+1$-tuples $(x_0, \ldots, x_{n-1}, k)$ with $x_i \in G, k \in \mathbf{Z}_n$. The index i is to take values in $\mathbf{Z}_n$. Multiplication in $G \wr \mathbf{Z}_n$ is given by

$$(x_0, \ldots, x_{n-1}, k) \cdot (y_0, \ldots, y_{n-1}, l) = (x_0 y_k, x_1 y_{k+1}, \ldots, x_{n-1} y_{k-1}, k + l).$$

Let Q be the conjugacy class of $(1, \ldots, 1, 1)$ in $G \wr \mathbf{Z}_n$. Then

$$Q = \{x_0, \ldots, x_{n-1}, 1) \,|\, x_0 \cdots x_{n-1} = 1\}$$

and the quandle operation on Q is given by

$$(x_0, \ldots, x_{n-1}, 1) \triangleright (y_0, \ldots, y_{n-1}, 1) = (y_{n-1}^{-1} x_{n-1} y_0, y_)^{-1} x_0 y_1, \ldots, 1).$$

This quandle is called the *n-core of G*. The 2-core of G is isomorphic to the core of G.

2.8 Examples of simple quandles

A quandle is said to be *simple* if its only quotients are itself and the one-point quandle. We will show in this section that n-cores of noncyclic simple groups are simple. In fact, a noncyclic group is simple if and only if its n-core is simple. Also, nontrivial conjugacy classes of simple groups are simple. We proceed with some lemmas.

Lemma 1. Let H be a group with commutator H'. An element x in H lies in H' if and only if there exist $x_1, x_2, \ldots, x_k$ in H such that $x = x_1 x_2 \ldots x_k$ and $x_k \ldots x_2 x_1 = 1$. □

Lemma 2. Let H be a perfect group, $H = H'$. Then the n-core Q of H as a subset of $G = H \wr \mathbf{Z}_n$ generates G.

Proof. Let $b = (\mathbf{1}, 1) = (1, \ldots, 1, 1) \in Q$. Let $x \in H$. By lemma 1, $x = x_1 \ldots x_k, x_k \ldots x_1 = 1$. Then

$$\begin{aligned} & (x_1, x_1^{-1}, 1, \ldots, 1) b^{-1} (x_2, x_2^{-1} 1, \ldots, 1) b^{-1} \ldots (x_k, x_k^{-1}, 1, \ldots, 1) b^{-1} \\ = \; & (x_1 x_2 \cdots x_k, x_1^{-1} x_2^{-1} \cdots x_k^{-1}, 1, \ldots, 1, 0) \\ = \; & (x, 1, \ldots, 1, 0). \end{aligned}$$

Since b and each $(x_i, x_i^{-1}, 1, \ldots, 1)$ lie in Q, so $(x, 1, \ldots, 1, 0)$ is a member of the subgroup generated by Q. The rest follows easily. □

Lemma 3. If the center of a nontrivial group H is trivial, then the center of $H \wr \mathbf{Z}_n$ is trivial. □

Lemma 4. Let G be a group with trivial center, and let Q be a conjugacy class that generates G. Then $G \cong \operatorname{Inn} Q$, and $G' \cong \operatorname{Trans} Q$.

Proof. For each $x \in G$ let $S(x)$ be conjugation by x, and regard $S(x)$ as an automorphism of Q. Then S is a group homomorphism $S : G \to \operatorname{Aut} Q$. Note that $S(x) = 1$ if and only if for all q in Q, $x^{-1}qx = q$. Since Q generates G, $S(x) = 1$ if and only if $x \in Z(G)$. Therefore, S is injective. The image of S is $\operatorname{Inn} Q$. Hence, S is an isomorphism $G \cong \operatorname{Inn} Q$.

We show next that $S(G') = \operatorname{Trans} Q$. Let $p, q \in Q$. Then $[S(p), S(q)] = S(p)^{-1}S(p \triangleright q) \in \operatorname{Trans} Q$. $\operatorname{Trans} Q$ is a normal subgroup of $\operatorname{Inn} Q$, so $S(G') = (\operatorname{Inn} Q)' \subseteq \operatorname{Trans} Q$. Since Q is a conjugacy class in G, there is an x in G such that $x^{-1}px = q$. Therefore, $S(p)^{-1}S(q) = [x, S(q)] \in (\operatorname{Inn} Q)'$. Thus, $\operatorname{Trans} Q \subseteq S(G')$. □

Lemma 5. Under the hypotheses of lemma 4 the following statements are equivalent.

(1) Q is a simple quandle.

(2) G' is the smallest nontrivial normal subgroup of G.

(3) G' is a minimal nontrivial normal subgroup of G.

Proof. (1) $\Longrightarrow$ (2). Let N be a normal subgroup of $\operatorname{Inn} Q$. Define an equivalence relation on Q by

$$p \equiv q \iff \exists n \in N \text{ such that } pn = q.$$

We show that $\equiv$ is an congruence. Assume $p \equiv q$, $pn = q$. For r in Q we have $q \triangleright r = pn \triangleright r = (p \triangleright r)m$ where $m = S(r)^{-1}nS(r) \in N$. Hence, $q \triangleright r \equiv p \triangleright r$. Also $r \triangleright q = r \triangleright pn = (r \triangleright p)m^{-1}n$ where $m^{-1}n \in N$. Hence, $r \triangleright q = r \triangleright p$. Therefore, $\equiv$ is a congruence. By the simplicity of Q we have only two cases.

Case 1. $\equiv$ is equality. Let $n \in N$. For all q in Q, $qn = q$, so $n^{-1}S(q)n = S(q)$. From the hypotheses of the lemma it follows that $n = 1$. Thus, $N = 1$.

Case 2. $\equiv$ relates all points of Q. For p, q in Q there is an n in N such that $pn = q$. Then $n^{-1}S(p)n = S(q)$. Therefore, $S(p)S(q)^{-1} \in N$. Hence, $\operatorname{Trans} Q \subseteq N$.

Now (2) follows from the conclusions of lemma 4.

(2) $\Longrightarrow$ (3). Clear.

(3) $\Longrightarrow$ (1). Assume (3). Let $\equiv$ be a congruence on Q. Conjugation by elements of Q respects $\equiv$, that is, $p \equiv q$ implies $p \triangleright r \equiv q \triangleright r$. Since Q generates G, conjugation by elements of G respects $\equiv$. Let

$$N = \{x \in G' \mid ps(x) \equiv p \text{ for all } p \in Q\}.$$

Then N is a normal subgroup of G contained in G'. By (3), either $N = 1$ or $N = G'$. Assume $\equiv$ is not equality. Then $\exists q, r \in Q$ such that $q \equiv r$ but $q \neq r$. It follows that $1 \neq qr^{-1} \in N$. Hence, $N = G'$. Now let q, r be arbitrary in Q. $\exists x \in G'$ such that $x^{-1}qx = r$. Therefore, $q \equiv qS(x) = p$. Thus, if $\equiv$ is not equality, then $\equiv$ relates any two elements. □

Lemma 6. Let H be a noncyclic simple group and $G = H \wr \mathbf{Z}_n$, $n \geq 2$. Then $K = \{(x_0, \ldots, x_{n-1}, 0) \in G\}$ is a minimal nontrivial normal subgroup of G.

Proof. Let $(x_0, \ldots, x_{n-1}, 0)$ be a nontrivial element of K. We will show the smallest normal subgroup N containing this element is K. For some i, $x_i \neq 1$, say $i = 0$. There is an element w of G such that $[x_0, w] = z \neq 1$. Then $[(x_0, \ldots, x_{n-1}, 0), (w, 1, \ldots, 1)] = (z, 1, \ldots, 1, 0)$ lies in N. As $z \neq 1$ and H is simple, it follows that $(y, 1, \ldots, 1, 0) \in N$ for all y in H. Now

$$(y, 1, \ldots, 1, 0) \triangleright (1, \ldots, 1, k) = (1, \ldots, y, \ldots, 1, 0)$$

also lies in N for all y in H and k in $\mathbf{Z}_n$. Hence $N = K$. □

Theorem 1. Let H be a noncyclic group and Q be the n-core of H ($n \geq 2$). Then Q is simple if and only if H is simple, in which case $\operatorname{Inn} Q \cong G = H \wr \mathbf{Z}_n$ and

$$\operatorname{Trans} Q \cong G' = \{(x_0, \ldots, x_n, 0) \in G\} \cong H^n.$$

Proof. Assume H is simple. According to lemma 2, Q generates G, and by lemma 3 $z(G) = 1$. Since the hypotheses of lemma 4 hold, we have $G \cong \operatorname{Inn} Q$, and $G' \cong \operatorname{Trans} Q$. Lemma 6 says $K = \{(x_0, \ldots, x_{n-1}, Q) \in T\}$ is a minimal nontrivial normal subgroup of G. Hence, $G' = K$. Finally, we conclude from lemma 5 that Q is simple.

Any normal subgroup N of H gives a quandle congruence on Q defined by

$$(\mathbf{x}, 1) \equiv (\mathbf{y}, 1) \iff x_i y_i^{-1} \in N \text{ for } i = 0, \ldots n-1.$$

Moreover, if $N \neq 1$, then $\equiv$ is not equality. Hence, the simplicity of Q assures that of H. □

The n-core of a noncyclic simple group retains, therefore, more information about the group than just its simplicity. It can, in fact, be reconstructed from its n-core.

Remark. The 4-core of the cyclic simple group $\mathbf{Z}_2$ is not a simple quandle.

Corollary. The core (2-core) of a group is simple if and only if the group is simple.

Proof. The only groups not covered by the theorem are cyclic groups for which the statement is easily verified. □

There are two other ways that simple quandles derive from simple groups besides n-cores. We will show that any nontrivial conjugacy class in a simple group is a simple quandle. The following lemma is a direct consequence of lemmas 4 and 5.

Lemma 7. Under the hypotheses of lemma 4, if G' is a simple group, then Q is a simple quandle. □

Theorem 2. Let H be a noncyclic simple group and Q a nontrivial conjugacy class in H. Then Q is a simple quandle. Also, $\operatorname{Inn} Q = \operatorname{Trans} Q \cong H$.

Proof. Q generates H, and $z(H) = 1$. So by lemma 4, $\operatorname{Inn} Q = \operatorname{Trans} Q \cong H$. By lemma 7, Q is a simple quandle. □

Theorem 3. Let H be a noncyclic simple group, p a prime integer, and s an outer automorphism of G of order p. Let G be the semidirect product $H \ltimes \mathbf{Z}_p$, $(x,y)\cdot(y,l) = (xs^{-k}(y), k+l)$. Then Q is a simple quandle, $\operatorname{Inn} Q \cong G$, and $\operatorname{Trans} Q \cong H$.

Proof. First we show that Q generates G. Let (Q) be the subgroup generated by Q. (Q) is normal in G. $(1,1) \in (Q)$, so $(1,k) \in (Q)$ for all k in $\mathbf{Z}_p$. Also, $(1,1) \triangleright (y,0) = (y^{-1}s^{-1}(y), 1) \in (Q)$. Since $s \neq 1$, $\exists y \in H$ such that $1 \neq (y^{-1}s^{-1}(y),1) \in (Q)$. Also $(y^{-1}s^{-1}(y),0) \in (Q)$. Hence $(Q) \cap H \neq 1$. Therefore, $(Q) \cap H = H$. It follows that $(Q) = G$.

Next we show $Z(G) = 1$. Suppose $(a,k) \in Z(G)$. Then $zs^{-k}(y) = yz$ for all y in H. Thus, $s^k = S(z^{-1})$. If p divides k, then $1 = s^k = S(z^{-1})$, which gives $(z,k) = (1,0)$. Otherwise, $(p,k) = 1$. Then for some m, $km \equiv 1 \bmod p$, so $s = s^{km} = S(z^{-m})$. in contradiction to the hypothesis that s is not an inner automorphism. This, $Z(G)$ is trivial.

We have shown that Q and G satisfy the hypotheses of lemma 4. Hence, $G \cong \operatorname{Inn} Q$, and $G' \cong \operatorname{Trans} Q$.

Clearly, $G' = H \ltimes 0 \cong H$, so by lemma 7, Q is simple. □

2.9 Classification of simple p-quandles

In this section we examine the problem of classifying simple quandles. In the case of p-quandles, p a prime integer, we solve the problem in terms of simple groups. Throughout this section let Q be a simple quandle and $G = \operatorname{Inn} Q$.

Lemma 1. Either $S : Q \to G$ is injective or the order of Q is less than three.

Proof. The behavioral equivalence on Q is either equality or else relates any two elements of Q. In the former case S is injective. In the latter case Q satisfies the identity $x \triangleright y = x$. But the only simple quandles satisfying $x \triangleright y = x$ have fewer than three elements. □

Assume for the rest of this section that the order of Q is greater than two. Since the set of connected components of Q is a quotient of Q, it follows that Q is algebraically connected. Also, $S(Q)$ is a conjugacy class in G since it is closed under conjugation and generates G.

Lemma 2. The center of G is trivial.

Proof.

$$\begin{aligned} z \in Z(G) &\iff \forall q \in Q, zS(q) = S(q)z \\ &\iff \forall q \in Q, S(qz) = S(q) \\ &\iff \forall q \in Q, qz = q. \end{aligned}$$

But the only automorphism fixing all the points of Q is 1. Therefore, $Z(G) = 1$. □

By lemma 4 of section 2.9 we have $\operatorname{Trans} Q = G'$. Hence, G/G' is a cyclic group. Moreover, if Q is an n-quandle, then the order of G/G' divides n. Since $S(Q) \cong Q$ is

a simple quandle, by lemma 5 of section 2.9 it follows that G' is the smallest nontrivial normal subgroup of G.

At this point we must break the classification into cases. If $G' = G$, then G is a simple group, and Q is isomorphic to the nontrivial conjugacy class $S(Q)$ in the simple group G. For the rest of this section we assume $G' \neq G$. We will also assume that Q is a p-quandle, p a prime integer. Then $G/G' \cong \mathbf{Z}_p$.

Fix q_0 in Q. Let $x_0 = S(q_0) \in G$, and let s be conjugation by x_0 as an automorphism of G'. Then $x_0 \neq 1$, $x_o^p = 1$, $s \neq 1$, $s^p = 1$. Let K be the semidirect product $G' \ltimes \mathbf{Z}_p$ where

$$(x, k)(y, l) = (xs^{-k}(y), k + l).$$

There is an isomorphism $f : K \to G$, $f(x, k) = xx_0^k$. In particular, $f(1, 1) = x_0$, and $f^{-1}(S(Q))$ is the conjugacy class in K of $(1, 1)$.

Suppose G' is a simple group. From the fact that $Z(G') = 1$ it follows that s is not an inner automorphism of G'. Thus, Q is isomorphic to the conjugacy class of $(1, y)$ in $k = G' \ltimes \mathbf{Z}_p$ where G' is a simple group and $G' \ltimes \mathbf{Z}_p$ is constructed from an outer automorphism of G' of order p. This is the situation encountered in theorem 3 of section 2.8.

We have yet to consider the case where G' is not simple.

Lemma 3. Let H be a group with a smallest nontrivial normal subgroup T such that $[H : T] = p$ is prime. Assume T is not simple. Then T is isomorphic to N^p for some simple group N.

Proof. Let N be a nontrivial proper normal subgroup of T. Fix x in $H - T$. Let s be conjugation by x as an automorphism of T. Then $s^p(N) = N$ since $x^p \in T$. More generally, $s^{p+i}(N) = s^i(N)$ for any integer i. Since p is prime and N is not normal in N, we have p distinct conjugates of N, namely,

$$N, s(N), \ldots, s^{p-1}(N).$$

Claim. For $k = 0, 1, \ldots, p - 2$, there exist nontrivial proper normal subgroups N_k of T such that $0 \neq |i - j| \leq k$ implies $s^i(N_k) \cap s^j(N_k) = 1$.

Define $N_0 = N$. Inductively define N_{k+1} $(k+1 \leq p-1)$ as follows. The group

$$N_k \cap s^{k+1}(N_k) \cap \cdots \cap s^{(k+1)(p-1)}(N_k)$$

is normal in G since $k+1$ is relatively prime to p, and, being strictly contained in T, is, therefore, trivial. Let l be least such that

$$N_k \cap s^{k+1}(N_k) \cap \cdots \cap s^{(k+1)l}(N_k) = 1.$$

Then

$$N_{k+1} = N_k \cap s^{k+1}(N_k) \cap \cdots \cap s^{(k+1)(l-1)}(N_k)$$

satisfies the requirements of the claim.

We may assume $N = N_{p-1}$. That is, the p conjugates of N,

$$N, s(N), \ldots, s^{p-1}(N),$$

have pairwise trivial intersection and generate T. Hence

$$T = N \times s(N) \times \cdots \times s^{p-1}(N) \cong N^p.$$

Also, N is simple. Indeed, if M is a proper normal subgroup of N, then $M \times s(M) \times \cdots \times s^{p-1}(M)$ is normal in H and strictly contained in T and, therefore, is trivial as is M. □

Theorem 1. Let Q be a simple p-quandle, p a prime, and let $G = \operatorname{Inn} Q$. As noted above, $G' = \operatorname{Trans} Q$. Assume G' is not a simple group. Then G is a wreath product of a simple group N with $\mathbf{Z}_p$, $G' \cong N^p$, and Q is isomorphic to the p-core of N.

Proof. By lemma 3, $G' \cong N^p$ where N is a simple group. As noted above G is isomorphic to $G' \ltimes \mathbf{Z}_p$. Therefore, $G = G' \ltimes \mathbf{Z}_p = N \wr \mathbf{Z}_p$. Also, Q is isomorphic to the conjugacy class of $(1, 1)$ in $G' \ltimes \mathbf{Z}_p$ and, therefore, to the p-core of N. □

Scholium. simple p-quandles of order greater than two arise in three ways:

1. a nontrivial conjugacy class in a simple group,
2. the conjugacy class of $(1, 1)$ in $H \ltimes \mathbf{Z}_p$ where H is a simple group and $H \ltimes \mathbf{Z}_p$ is constructed from an outer automorphism of H,
3. the p-core of a simple group.

The three cases are distinguished by the structure of the inner automorphism group of the quandle.

2.10 Augmented quandles

Let G be a group acting on a quandle Q by quandle automorphisms. That is, for $x, y \in G$ and $p, q \in Q$ we have

$$\begin{aligned} q(xy) &= (qx)y, \text{ and} \\ (p \triangleright q)x &= px \triangleright py. \end{aligned}$$

Assume that G contains representatives of the symmetries of Q, that is, there is a function $\epsilon : Q \to G$ satisfying

$$p\epsilon(q) = p \triangleright q.$$

In particular, we have

AQ1. $$p\epsilon(p) = p, \text{ for } p \in Q.$$

Assume further that ϵ satisfies the coherency condition

AQ2. $$\epsilon(px) = x^{-1}\epsilon(p)x, \text{ for } p \in Q, x \in G.$$

Then we have a group action on Q, $Q \times G \to Q$, and a function $\epsilon : Q \to G$ which satisfy **AQ1** and **AQ2**.

Conversely, given a group action of G on a set Q, $Q \times G \to Q$, and a function $\epsilon : Q \to G$ satisfying **AQ1** and **AQ2**, we can define quandle operations on Q as $x \triangleright y = x\epsilon(y)$ and $x \triangleright^{-1} y = x\epsilon(y)^{-1}$ so that the action of G on Q is by quandle automorphisms.

Definition. An *augmented quandle* (Q, G) consists of a set Q and a group G equipped with a right action on the set Q and a function $\epsilon : Q \to G$ called the *augmentation map* which satisfy **AQ1** and **AQ2**.

With the operations mentioned above Q is a quandle, and the augmentation map is a quandle homomorphism $\epsilon : Q \to \operatorname{Conj} G$.

A *morphism of augmented quandles* from (Q, G) to $P, H)$ consists of a group homomorphism $g : G \to H$ and a function $f : Q \to P$ such that the diagram

$$\begin{array}{ccccc} Q \times G & \longrightarrow & Q & \xrightarrow{\epsilon} & G \\ {\scriptstyle f\times g}\downarrow & & {\scriptstyle f}\downarrow & & {\scriptstyle g}\downarrow \\ P \times H & \longrightarrow & P & \xrightarrow{\epsilon} & H \end{array}$$

commutes. It follows that f is a quandle homomorphism.

Examples. Fix a quandle Q. Two examples of augmented quandles with underlying quandle Q are $(Q, \operatorname{Aut} Q)$ and $(Q, \operatorname{Inn} Q)$. the augmentation in each case is the function that has been denoted S. The action is the natural one. In the category of augmentations of Q, $(Q, \operatorname{Aut} Q)$ is the terminator. That is, for each augmentation (Q, G), there is a unique homomorphism $f : G \to \operatorname{Aut} Q$ such that

$$\begin{array}{ccccc} Q \times G & \longrightarrow & Q & \xrightarrow{\epsilon} & G \\ {\scriptstyle 1\times f}\downarrow & & {\scriptstyle 1}\downarrow & & {\scriptstyle f}\downarrow \\ Q \times \operatorname{Aut} Q & \longrightarrow & Q & \xrightarrow{S} & \operatorname{Aut} Q \end{array}$$

commutes. The map f is readily defined from $Q \times G \to Q$.

Another example of an augmentation of Q is $(Q, \operatorname{Adconj} Q)$, (see section 2.3). The function representing symmetries of Q is $\eta : Q \to \operatorname{Adconj} Q$, while the group action is defined by

$$z(\overline{y}_1^{e_1} \cdots \overline{y}_n^{e_n}) = z \triangleright^{e_1} y_1 \triangleright^{e_2} \cdots \triangleright^{e_n} y_n,$$

where $z \in Q$ and $\overline{y}_1^{e_1} \cdots \overline{y}_n^{e_n}$ is an arbitrary element of $\operatorname{Adconj} Q$, $y_i \in Q$, $e_i \in \{-1, 1\}$ for $i = 1, \ldots n$. To show that this is a well-defined group action, it suffices to note that

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

The axiom **AQ1** clearly holds. Since $\eta(Q)$ generates $\operatorname{Adconj} Q$, **AQ2** reduces to the fact that $\eta : Q \to \operatorname{Conj}\operatorname{Adconj} Q$ is a quandle homomorphism as noted in section 2.3.

In the category of augmentations of Q, $(Q, \operatorname{Adconj} Q)$ is the coterminator. That is, for each (Q, G) there is a unique group homomorphism $f : \operatorname{Adconj} Q \to G$ such that

$$\begin{array}{ccccc} Q \times \operatorname{Adconj} Q & \longrightarrow & Q & \xrightarrow{\eta} & \operatorname{Adconj} G \\ {\scriptstyle 1\times f}\downarrow & & {\scriptstyle 1}\downarrow & & {\scriptstyle f}\downarrow \\ Q \times G & \longrightarrow & Q & \xrightarrow{\epsilon} & G \end{array}$$

commutes. According to the right square, f must be the map $H : \operatorname{Adconj} Q \to G$ described in section 2.3. To show the commutativity of the left square it suffices to show $z\overline{y} = zf(\overline{y})$ for y, z in Q, since such $\overline{y}$ generate $\operatorname{Adconj} Q$. But $z\overline{y} = z \triangleright y = z\epsilon(y) = zf(\overline{y})$.

We consider now constructions in the category $\mathcal{AQ}$ of augmented quandles. Products, equalizers, and limits in general are of the usual sort. For instance, the product of (Q, G) and (P, H) has as its augmentation group $G \times H$ and has as its underlying quandle $Q \times P$. However, it will take more work to describe colimits.

Let U be the forgetful functor from $\mathcal{AQ}$ to the category of groups, $U(Q, G) = G$. U has both a left adjoint T and a right adjoint V. That U has a left adjoint T is automatic and uninteresting. $T(G) = (\emptyset, G)$. On the other hand, the existence of a right adjoint V is unexpected. Let G be a group. Then $V(G) = (\operatorname{Conj} G, G)$ where G acts on $\operatorname{Conj} G$ by conjugation and the function $\epsilon : \operatorname{Conj} G \to G$ is the identity. We show that $(\operatorname{Conj} G, G)$ satisfies the appropriate universal property. Let (G, H) be an augmented quandle and $f : H \to G$ a group homomorphism. We must show there exists a unique function $g : Q \to \operatorname{Conj} G$ such that

$$\begin{array}{ccccc} Q \times H & \longrightarrow & Q & \xrightarrow{\epsilon} & H \\ {\scriptstyle g\times f}\downarrow & & {\scriptstyle g}\downarrow & & {\scriptstyle f}\downarrow \\ \operatorname{Conj} G \times G & \longrightarrow & \operatorname{Conj} G & \longrightarrow & G \end{array}$$

commutes. Since $\operatorname{Conj} G \to G$ is the identity, the function g must be $f \circ \epsilon$. The commutativity of the left square states

$$(*) \qquad g(qx) = g(q) \cdot f(x)$$

for $q \in Q$, $x \in H$. Here, $g(q) \cdot f(x)$ denotes conjugation of $g(q)$ by $f(x)$, so equals $f(x)^{-1}g(q)f(x)$ where the multiplication occurs in G. Then $(*)$ is equivalent to

$$\begin{aligned} f \circ \epsilon(qx) &= f(x)^{-1}(f \circ \epsilon)(q)f(x) \\ &= f(x^{-1}\epsilon(q)x), \end{aligned}$$

and this follows from axiom **AQ2** for (Q, H).

The existence of a right adjoint for U simplifies the construction of colimits in $\mathcal{AQ}$. If (Q, G) is the colimit, $\varprojlim(Q_i, G_i)$, then G is the colimit, $\varprojlim G_i$, in the category of groups.

Unfortunately, the forgetful functor from $\mathcal{AQ}$ to the category of quandles has no right adjoint. We need another construction of augmented quandles to describe their colimits.

Let (Q, G) be an augmented quandle and $f : G \to H$ a group homomorphism. Then $Q \times H$ is a right H-set with action $(q, x)y = (q, xy)$ for q in Q and x, y in H. Define an H-set congruence on $Q \times H$ by $(q, y) \equiv (p, z)$ if and only if $yz^{-1} = f(x)$ and $p = qx$ for some $x \in G$. Let $q \otimes y$ denote the congruence class of (q, y), and let $Q \otimes_G H$, or more simply $Q \otimes H$, denote the set of congruence classes. We have

$$\begin{aligned} (q \otimes y)z &= q \otimes yz, \text{ and} \\ q \otimes f(x) &= qx \otimes 1. \end{aligned}$$

Define $\epsilon : Q \otimes H \to H$ by $\epsilon(q \otimes x) = x^{-1}(f \circ \epsilon)(q)x$. ϵ is well-defined since axiom **AQ2** holds for (Q, G). Then $(Q \otimes H, H)$ is an augmented quandle, as can be directly verified. We also have a function $i : Q \to Q \otimes H$ given by $q \mapsto q \otimes 1$, which along with f gives a map $(i, f) : (Q, G) \to (Q \otimes H, H)$ of augmented quandles.

Proposition. Let (Q, G) be an augmented quandle and $f : G \to H$ a group homomorphism. Then $(i, f) : (Q, G) \to (Q \otimes H, H)$ satisfies the following universal property. For each map of the form $(g, h \circ f) : (Q, G) \to (P, K)$, there exists a unique map of the form $(k, h) : (Q \otimes H, H) \to (P, K)$ such that $(g, h \circ f) = (k, h) \circ (i, f)$. Otherwise said, in the category of augmented quandles

$$\begin{array}{ccc} (\emptyset, G) & \longrightarrow & (Q, G) \\ {\scriptstyle (1,f)}\downarrow & & \downarrow{\scriptstyle (i,f)} \\ (\emptyset, H) & \longrightarrow & (Q \otimes H, H) \end{array}$$

is a pushout diagram.

Proof. Let $(g, h \circ f) : (Q, G) \to (P, K)$ be given. Denote the required function $Q \otimes H \to P$ by k. There are four requirements on k. In order that k be well-defined we need

1) $$k(q \otimes f(x)y) = k(qx \otimes y), \text{ for } q \in Q, x \in G, y \in H.$$

In order that (k, h) be a map in $\mathcal{AQ}$ we need

2) $$(\epsilon \circ k)(q \otimes y) = (h \circ \epsilon)_(q \otimes y), \text{ for } q \in Q, y \in H,$$

and

3) $$k(q \otimes yz) = k(q \otimes y)h(z), \text{ for } q \in Q, y, z \in H.$$

And so that $(q, h \circ f) = (k, h) \circ (i, f)$ we need

4) $$g(q) = k(q \otimes 1), \text{ for } q \in Q.$$

Together, 3) and 4) show that k must be defined as $k(q \otimes y) = g(q)h(y)$, giving the uniqueness of k. With this definition of k, 1) states

$$g(q)h(f(x)y) = g(qx)h(y).$$

This reduces to

$$g(q)(h \circ f)(x) = g(qx),$$

which holds since $(g, h \circ f)$ is a map in $\mathcal{AQ}$.

Finally, 2) states that

$$\epsilon(g(q)h(y)) = (h \circ \epsilon)(q \otimes y).$$

But

$$\begin{aligned} \epsilon(g(q)h(y) &= h(y)^{-1}(\epsilon \circ g)(q)h(y) \\ &= h(y)^{-1}(h \circ f \circ \epsilon)(q)h(y) \\ &= h(y^{-1}(f \circ \epsilon)(q)y) \\ &= (h \circ \epsilon)(q \otimes y). \end{aligned}$$

□

We will denote the function k in the proposition by g in spite of the confusion it may cause. In this notation $(g, h \circ f) = (g, h) \circ (i, f)$. In the case that $H = K$ and h is the identity function, $1 : H \to H$, we have $(g, f) = (g, 1) \circ (i, f)$. Note also that when $H = G$ and f is the identity, $1 : G \to G$, then the augmented quandle $(Q \otimes_G G, G)$ is the original augmented quandle (Q, G). Hence, $Q \otimes_G G = Q$.

We now consider an arbitrary colimit $(Q, G) = \varprojlim(Q_j, G_j)$ in the category $\mathcal{AQ}$. As noted above G is the colimit, $\varprojlim G_j$, in the category of groups. By the preceding proposition, for each j, $(Q_j, G_j) \to (Q, G)$ factors uniquely through $(Q_j, G_j) \to (P_j, G)$ where P_j denotes $Q_j \otimes_{G_j} G$. Consequently, $(Q, G) \cong \varprojlim(P_j, G)$. This reduces the construction of colimits to the case where a single group G acts on all the sets P_j, and all maps $(P_j, G) \to (P_k, G)$ are of the form $(f, 1)$.

In this case let $P = \varprojlim P_j$ in the category of sets. Then P has a unique right G-action determined by the G-actions on the P_j, so we might just as well have taken this colimit in the category of G-sets. There is also a function $\epsilon : P \to G$ determined by the functions $\epsilon : P_j \to G$. It may be directly verified that with this action and ϵ that (P, G) is an augmented quandle. By the definition of P there is a unique function $(f, 1) : (P, G) \to (Q, G)$ determined by the maps $(P_j, G) \to (Q, G)$. Also the function $(f, 1)$ satisfies the commutativity conditions to be a map in $\mathcal{AQ}$ since all the maps $(P_j, G) \to (Q, G)$ satisfy these conditions. Furthermore, all the maps $(P_j, G) \to (P, G)$ lie in $\mathcal{AQ}$, so $(P, G) = \varprojlim(P_j, G)$.

We summarize these results.

Theorem. A colimit, $\varprojlim(Q_j, G_j)$ in $\mathcal{AQ}$ is isomorphic to $\varprojlim(Q_j \otimes_{G_j} G, G)$ where $G = \varprojlim G_j$ in the category of groups. It is also isomorphic to $(\varprojlim Q_j \otimes_{G_j} G, G)$ with $\varprojlim Q_j \otimes_{G_j} G$ taken in the category of sets. □

2.11 Quotients of augmented quandles described by normal subgroups of the augmentation group

Let (Q, G) be an augmented quandle and N be a normal subgroup of G. Let $\overline{G}$ denote the quotient group G/N with elements denoted by $\overline{x}$ for x in G. Let $\overline{Q}$ and Q/N denote the quandle $Q \otimes_G \overline{G}$. The elements of $\overline{Q}$ are equivalence classes $\overline{q}$ of elements of Q where $\overline{q} = \{qn \in Q \mid n \in N\}$. The action $\overline{Q} \times \overline{G} \to \overline{Q}$ is given by $\overline{q}\,\overline{x} = \overline{qx}$ and the augmentation $\overline{\epsilon} : \overline{Q} \to \overline{Q}$ is given by $\overline{\epsilon}(\overline{q}) = \overline{\epsilon(q)}$.

Let (Q, G) be an augmented quandle. In order that the quandle Q be Abelian we need

$$(p \triangleright q) \triangleright (r \triangleright s) = (p \triangleright r) \triangleright (q \triangleright s).$$

Equivalently, $\epsilon(q)\epsilon(r\epsilon(s)) = \epsilon(r)(\epsilon(p)\epsilon(s))$. That is, every element in G of the form

$$(*) \qquad \epsilon(q)\epsilon(s)^{-1}\epsilon(r)\epsilon(q)^{-1}\epsilon(s)\epsilon(r)^{-1}$$

equal 1. Let N be the normal subgroup of G generated by such elements. Then the quotient $(\overline{Q}, \overline{G})$ of (Q, G) is assured to be Abelian. It is evident that $(\overline{Q}, \overline{G})$ has the universal property that each map $(Q, G) \to (P, H)$ factors uniquely through $(Q, G) \to (\overline{Q}, \overline{G})$ whenever p is an Abelian quandle.

Proposition 1. Let (Q, G) be an augmented quandle such that $\epsilon(Q)$ generates G. Let N and $(\overline{Q}, \overline{G})$ be defined as above. Then $\overline{Q}$ is the Abelianization of the quandle Q.

Proof. Let P be an Abelian quandle and $f : Q \to P$ be a quandle homomorphism. We must show that $\overline{f} : \overline{Q} \to P$ given by $\overline{f}(\overline{q}) = f(q)$ is well defined, that is, $f(qn) = f(q)$ for $n \in N$. If n is of the form $(*)$, then $f(qn) = f(q)$ since P is Abelian. Since G is generated by $\epsilon(Q)$ we may assume n is of the form $\epsilon(p)^{-1}n'\epsilon(p)$ where $f(q'n') = f(q')$ for all q' in Q. Then

$$\begin{aligned} f(qn) &= f((q \triangleright^{-1} p)n' \triangleright p) \\ &= f((q \triangleright^{-1} p)n') \triangleright f(p) \\ &= f(q \triangleright^{-1} p) \triangleright f(p) \\ &= f(q). \end{aligned}$$

Thus, $\overline{f}$ is well-defined on $\overline{Q}$. □

Corollary 1. Let A be a set and G the group generated by A modulo relations $ab^{-1}c = cb^{-1}a$ for conjugates a, b, c of the generators of G. Then the free Abelian quandle on A consists of the conjugates of the generators of G. □

What has been done here for Abelian quandles can be done for many other varieties of quandles. The method works for any variety defined by equations of the form

$$p \triangleright^{e_1} \varphi_1 \triangleright^{e_2} \cdots \triangleright^{e_m} \varphi_m = p \triangleright^{f_1} \psi_1 \triangleright^{f_2} \cdots \triangleright^{f_n} \psi_n$$

where the φ_i and ψ_j are expressions not involving p. For example, the identity for n-quandles, $p \triangleright^n q = p$, is of this form.

Proposition 2. Let (Q, G) be an augmented quandle such that $\epsilon(Q)$ generates G, and N be a positive integer. Let N_n be the normal subgroup of G generated by $\epsilon(q)^n$ for q in Q. Then Q/N_n is the largest quotient of Q which is an n-quandle □

Corollary 2. Let A be a set and $G = (a, a \in A : a^n = 1, a \in A)$. The free n-quandle on A consists of the conjugates of the generators of G.

Corollary 3. The free involutory quandle on two points is isomorphic to $\mathrm{Core}\,\mathbf{Z}$ with generators 0 and 1.

Proof. Let $A = \{a, b\}$ and $G = (a, b : a^2 = b^2 = 1)$. Let Q be the quandle of conjugates of a and b in G. Let $x = ab$. Then $G = (a, x : a^2 = 1, axa = x^{-1})$. Each element of G is uniquely represented as $a^e x^k$ with $k \in \mathbf{Z}$ and $e \in \{0, 1\}$. The conjugates of a and b are those elements of the form ax^k, $k \in \mathbf{Z}$. $Q = \{ax^k \,|\, k \in \mathbf{Z}\}$. Verification that $ax^n \triangleright ax^m = ax^{2n-m}$ yields an isomorphism of quandles $f : Q \to \mathrm{Core}\,\mathbf{Z}$, $f(ax^n) = n$. Also, $f(a) = 0$, $f(b) = 1$. □

Proposition 3. The free Abelian involutory quandle on $n + 1$ generators appears as

$$A = \{(k_1, \ldots, k_n) \in \mathbf{Z}^n \,|\, \text{at most one } k_i \text{ is odd}\}$$

as a subquandle of $\mathrm{Core}\,\mathbf{Z}^n$ with generators $e_0 = (0, \ldots, 0)$, $e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, 0, \ldots, 0)$, $\ldots$, $e_n = (0, \ldots, 0, 1)$.

Proof. Let G be the group presented as

$$(a_o, ..., a_n : a_i^2 = 1, a_i a_j a_k = a_k a_j a_i, \text{ all } i, j, k),$$

and let Q include the conjugates of the generators of G. Then Q is the free Abelian involutory quandle on $a_0, \ldots, a_n$. As A is an Abelian quandle, there is a unique map $h : Q \to A$ such that $h(a_i) = e_i$, $i = 0, \ldots, n$. We will show h is an isomorphism. Let $t_j = a_o a_j$, $j = 0, \ldots, n$. Then $t_j t_k = t_k t_j$. The conjugates of a_i are of the form $a_i \triangleright a_{j_1} \triangleright \cdots \triangleright a_{j_r} = a_i \triangleright a_{j_1} \cdots a_{j_r}$, and r may be taken to be even since $a_i \triangleright a_i = a_i$. Then $a_i \triangleright a_{j_1} \cdots a_{j_r} = a_i \triangleright t_{j_1}^{-1} t_{j_2} \cdots t_{j_{r-1}}^{-1} t_{j_r}$. Thus, Q consists of elements of the form $a_i \triangleright t_1^{k_1} \cdots t_n^{k_n}$ with $k_i \in \mathbf{Z}$, $i = 1, \ldots, n$. Now $h(a_i \triangleright t_1^{k_1} \cdots t_n^{k_n} = e_i + 2k_1(e_1 - e_0) + 2k_2(e_2 - e_0) + \cdots + 2k_n(e_n - e_0) = e_i + (2k_1, \ldots, 2k_n)$. Clearly, h is surjective and injective. □

Alternatively, we may describe the free Abelian involutory quandle on $n+1$ generators as

$$B = \{(k_0, \ldots, k_n) \in \mathbf{Z}^{n+1} \,|\, \text{exactly one } k_i \text{ is odd}\}$$

as a subquandle of $\mathrm{Core}\,\mathbf{Z}^{n+1}$.

Chapter 3

Involutory quandles

3.1 Involutory quandles and geodesics

The fact that symmetric spaces are involutory quandles and that their structure is determined by distance along geodesics suggests that involutory quandles in general be determined by some kind of geodesic. Consider, for example, the *integral line quandle*, $L = \operatorname{Core} \mathbf{Z}$. Interpret L as the integral points on a line. Then for $m, n \in L$, $m \triangleright n$ is found by moving along the line from m through n the same distance beyond n as m is beyond n.

The suggestion may be formalized as follows. Define an *involutory quandle with geodesics* as a set Q of *points* with a collection of functions, called *geodesics*, $g : L \to Q$, where L is the integral line quandle $\operatorname{Core} \mathbf{Z}$, satisfying three axioms

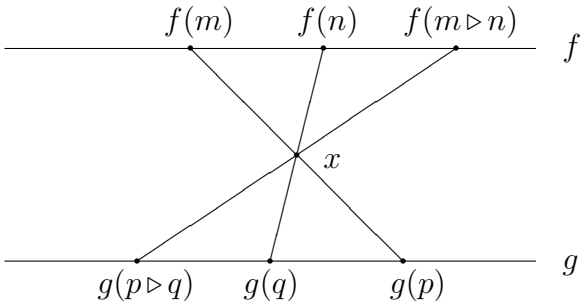
> **QG1.** Every pair of points lies in the image of some geodesic.
>
> **QG2.** Whenever a pair of points x, y lie in the image of two geodesics, $f(m) = x$, $f(n) = y$, $g(m') = x$, $g(n') = y$, it is the case that $f(m \triangleright n) = g(m' \triangleright n')$. We denote this point $f(m \triangleright n)$ as $x \triangleright y$.
>
> **QG3.** A geodesic reflected through a point is a geodesic; precisely, if x is a point and f a geodesic, then there exists a geodesic g such that for all $m, n \in L$, there exist $p, q \in L$ such that $f(m) \triangleright x = g(p)$, $f(n) \triangleright x = g(q)$, and $f(m \triangleright n) \triangleright x = g(p \triangleright q)$. See figure 3.

It is easily seen that an "involutory quandle with geodesics" is an "involutory quandle". The operation $\triangleright$ is as defined in **QG2**.

Proposition. Every involutory quandle is representable as an involutory quandle with geodesics.

Proof. Recall corollary 3, section 2.11, which states that L is the free involutory quandle on two points. Let Q be the given quandle. For each pair of points x, y in Q there is a unique quandle map $f : L \to Q$ such that $f(0) = x$ and $f(1) = y$. Take all such maps

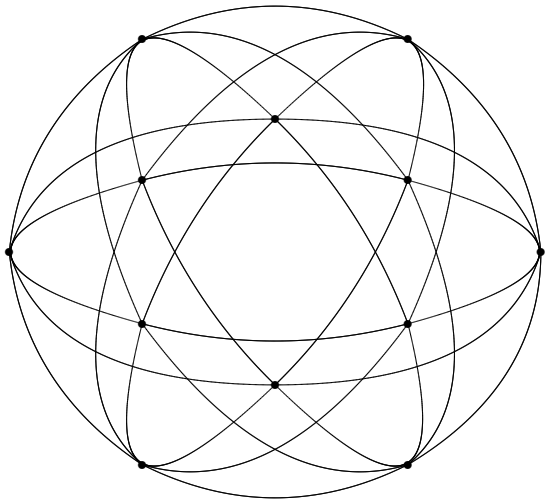
Figure 3.1: **QG3**



as geodesics. Clearly, **QG1** holds. For points x, y, if f is a geodesic such that $f(m) = x$ and $f(n) = y$, then $f(m \triangleright n) = x \triangleright y$, hence, **QG2** holds. Finally, given a geodesic f and a point x, the geodesic g required for **QG3** is that such that $g(0) = f(0) \triangleright x$ and $g(1) = f(1) \triangleright x$.

Example. Figure 3.2 displays a 2-quandle by means of geodesics. Note that some pairs of points of the quandle lie on distinct geodesics. This particular example is algebraically connected but does not have behaviorally distinct elements.

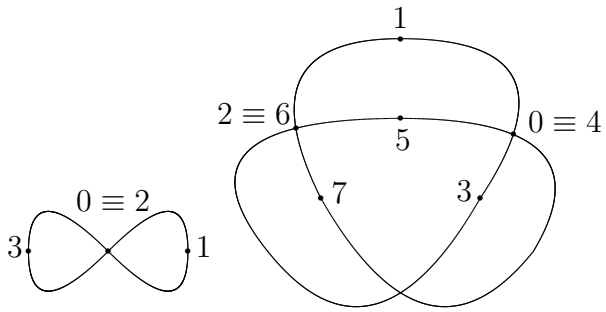
Figure 3.2: Geodesics



3.2 Involutory quandles generated by two points

At this point it is appropriate to classify the involutory quandles generated by two points. They will all be quotients of the free involutory quandle on two points, $L = \operatorname{Core} \mathbf{Z}$.

Figure 3.3: Singular quandles $Cs(4)$ and $CS(8)$



$Cs(4)$ $\qquad$ $Cs(8)$

Proposition. Any involutory quandle generated by two points is isomorphic to one of the following

i). $L = \operatorname{Core} \mathbf{Z}$.

ii). $C(n) = \operatorname{Core} \mathbf{Z}_n$, the *(nonsingular) cyclic quandle of order* n.

iii). $Cs(4n)$, the quotient of $C(4n)$ given by the congruence $2k \equiv 2k + 2n$ for all $k \in \mathbf{Z}_n$, the *singular cyclic quandle of order* $3n$.

Remark. Figure 3.3 illustrates $Cs(4)$ and $Cs(8)$.

Proof. It is straightforwad to check that the list induces only quotient quandles of L. Assume now that Q is the proper quotient of L, $Q = L/\equiv$. Let d be the least difference between any two distinct equivalent points of L. $d = |m - n| \neq 0$, $m \equiv n$. By using a translation by $-m$ on L, which is an isomorphism of L, we may assume $m = 0$. $d = |n| \neq 0$. Now $-n = n \triangleright 0 \equiv 0 \triangleright 0 = 0$, so $0 \equiv d$. For all k, $k = -k \triangleright 0 \equiv -k \triangleright d = k + 2d$. Therefore, Q is a quotient of $C(2d) = \operatorname{Core} \mathbf{Z}_{2d}$. Note that for all k, $2k = 0 \triangleright k \equiv d \triangleright k = 2k - d$. Similarly,

$$(*) \qquad 2k - d \equiv 2k \equiv 2k + d.$$

We consider two cases depending on the parity of d.

Case 1. d is odd. We show $p \equiv p + d$ for all p. If p is even, $p = 2k$, then $(*)$ implies $p \equiv p + d$. If p is odd, $p = 2k - d$, then $(*)$ implies $p \equiv 2k \equiv p + d$. Therefore, Q is a quotient of $C(d) = \operatorname{Core} \mathbf{Z}_d$. By the minimality of d, $Q = C(d)$.

Case 2. d is even. Let $d = 2c$. We see from $(*)$ that Q is a quotient of $Cs(4c)$. Assume that Q is a proper quotient of $Cs(4c)$. Let p be the least nonnegative integer congruent to an element in Q from which it is distinct in $Cs(4c)$. Reflection through $p-1$ shows that $p-2$ has the same property unless $p = 0$ or $p = 1$. However, p cannot be 0, as the elements equivalent to 0 in $Cs(4c)$ are already the minimal distance d apart. Thus, $p = 1$. Then there is some q, $1 < q \leq 2n$ such that $1 \equiv q$. We have $1 \equiv 2d+1$ in $Cs(4c)$, so by the minimality of d, $q = d+1$, and $1 \equiv d+1$. For all k, $2k-1 = 1 \triangleright k \equiv (d+1) \triangleright k = 2k-1-d$. Coupled with $(*)$ we now have $Q = C(d) = \operatorname{Core} \mathbf{Z}_d$. □

It may be asked why other axioms were not included in the definition of "quandle" in order to eliminate the singular cyclic quandles as examples of quandles. There are two responses to this question. One is that the axioms could not remain equational without adding more operations. The other is these singular examples occur as the involutory quandles associated to certain links (as defined in chapter 4).

3.3 Group cores

In this section we will examine some more properties of the core of a group. We have already demonstrated (in section 2.8) the equisimplicity of a group and its core. In fact, if the core is simple, then the core determines the group. Bruck in [3] has shown, however, that different groups may have isomorphic cores. In particular, a nilpotent group of class two all of whose elements have odd finite order h has a core isomorphic to that of an Abelian group. Nonetheless, we have the following proposition.

Proposition 1. If the cores of two finitely generated Abelian groups are isomorphic, then the groups themselves are isomorphic.

Proof. Let $f : \operatorname{Core} G \to \operatorname{Core} H$ be an isomorphism between the cores of the finitely generated Abelian groups G and H. By composing f with the translation by $-f(0)$ in H (translation, $y \mapsto y - f(0)$, is a quandle isomorphism of $\operatorname{Core} H$), we may assume that $f(0) = 0$. Then $f(-x) = -f(x)$ and $f(2x) = 2f(x)$. Moreover,

$$(*) \qquad f(x + 2y) = f(x) + 2f(y).$$

The bijection f restricts to an isomorphism from $2G = \{2x \mid x \in G\}$ onto $2H$. Using the structure theorem for finitely generated Abelian groups, we conclude that

$$G \cong \mathbf{Z}^r \oplus (\mathbf{Z}_{2^{m_1}} \oplus \cdots \oplus \mathbf{Z}_{2^{m_k}}) \oplus \operatorname{Odd} G$$

where $1 \leq m_1 \leq \cdots \leq m_k$, and $\operatorname{Odd} G$ is the subgroup of G of elements of odd order. Similarly,

$$H \cong \mathbf{Z}^s \oplus (\mathbf{Z}_{2^{n_1}} \oplus \cdots \oplus \mathbf{Z}_{2^{n_l}}) \oplus \operatorname{Odd} H.$$

Now, $2G \cong 2\mathbf{Z}^r \oplus (2\mathbf{Z}_{2^{m_1}} \oplus \cdots \oplus 2\mathbf{Z}_{2^{m_k}}) \oplus \operatorname{Odd} G$, and we have a similar isomorphism for $2H$. Since $2G \cong 2H$, we have $\operatorname{Odd} G \cong \operatorname{Odd} H$, $r = s$, and beginning at the first $m_i > 1$ and the first $n_j > 1$, the sequence $m_1, m_2, \ldots, m_k$ is the same as $n_1, n_2, \ldots, n_l$. We only

have to show there are the same number of ones occurring in the sequence $m_1, \ldots, m_k$ as in the sequence $n_1, \ldots, n_l$. Using $(*)$ we see f induces a bijection form $G/2G$ onto $H/2H$. But $G/2G \cong \mathbf{Z}_2^r \oplus \mathbf{Z}_2^k$ and $H/2H \cong \mathbf{Z}_2^s \oplus \mathbf{Z}_2^l$. Since $r = s$ and $G/2G$ has the same cardinality as $H/2H$, we have $k = l$. Hence $G \cong H$. □

The next proposition interprets the Abelianness of a group core. Distributivity will be considered in section 3.4.

Proposition 2. A group G is nilpotent of class at most 2, that is, its commutator G' is contained in its center Z, if and only if its core is Abelian.

Proof. First note that for group cores, $x \triangleright y = z$ if and only if $xw \triangleright yw = zw$. Core G is Abelian when the identity $(w \triangleright x) \triangleright (y \triangleright z) = (w \triangleright y) \triangleright (x \triangleright z)$. Multiplying this equation by z^{-1} on the right yields

$$(wz^{-1} \triangleright xz^{-1}) \triangleright (yz^{-1} \triangleright 1) = (wz^{-1} \triangleright yz^{-1}) \triangleright (xz^{-1} \triangleright 1).$$

Thus, the group core is Abelian if and only if it satisfies

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

that is, $y^{-1}w^{-1}wx^{-1}y^{-1} = x^{-1}y^{-1}wy^{-1}x^{-1}$, which may be rewritten as

$$(*) \qquad w[x, y] = [x^{-1}, y^{-1}]w.$$

Assume Core G is Abelian. then for $w = 1$, $[x, y] = [x^{-1}, y^{-1}]$, and so, generally

$$w[x, y] = [x, y]w.$$

Hence, $G' \subseteq Z$.

Now assume $G' \subseteq Z$. In order to show $(*)$, it suffices to show $[x, y] = [x^{-1}, y^{-1}]$. But

$$[x^{-1}, y^{-1}] = xyx^{-1}y^{-1} = yx[x, y]x^{-1}y^{-1} = [x, y]yxx^{-1}y^{-1} = [x, y].$$

□

Proposition 2 generalizes Soublin's result [15] page 101, which, in the nomenclature of quandles, states that for any group G of exponent 3, Core G is Abelian if and only if G is nilpotent of class at most 2.

3.4 Distributive quandles

A property of quandles which is weaker than Abelianness is *distributivity*, satisfaction of

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

For each x in a distributive quandle, the map

$$P(x) : y \mapsto x \triangleright y$$

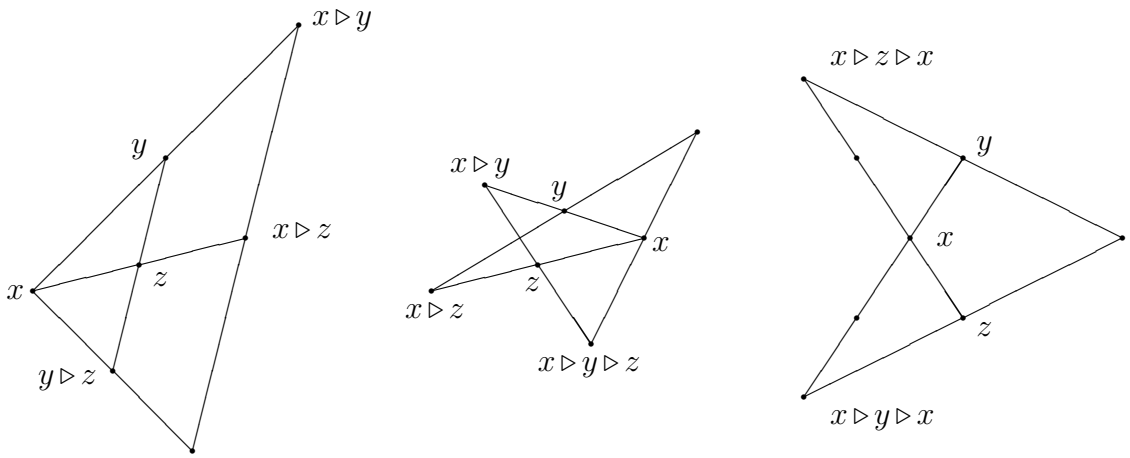
is a quandle homomorphism, called the *projection from* x. Projections need not be either injective or surjective.

Lemma 1. For an involutory quandle, distributivity is equivalent to satisfaction of either (1) or (2).

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

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

Figure 3.4: Distributivity



QDist (1) (2)

Proof. (1) $\implies$ (2).

$$\begin{aligned}
(x \triangleright y) \triangleright x \triangleright z &= (x \triangleright y) \triangleright z \triangleright x \triangleright (x \triangleright y) && \text{by (1)} \\
&= (x \triangleright y \triangleright z) \triangleright x \triangleright y \triangleright x \triangleright y \\
&= (x \triangleright z \triangleright y \triangleright x) \triangleright x \triangleright y \triangleright x \triangleright y && \text{by (1)} \\
&= x \triangleright z \triangleright x \triangleright y.
\end{aligned}$$

(2) $\implies$ **QDist**.

$$\begin{aligned}
(x \triangleright y) \triangleright (x \triangleright z) &= x \triangleright y \triangleright x \triangleright (z \triangleright x) \triangleright x \\
&= x \triangleright (z \triangleright x) \triangleright x \triangleright y \triangleright z && \text{by (2)} \\
&= x \triangleright (y \triangleright z).
\end{aligned}$$

QDist $\implies$ (1).

$$\begin{aligned} x \triangleright z \triangleright y &= x \triangleright (y \triangleright z) \triangleright z \\ &= (x \triangleright y) \triangleright (x \triangleright z) \triangleright z \qquad \text{by } \mathbf{QDist} \\ &= x \triangleright y \triangleright z \triangleright x. \end{aligned}$$

□

Proposition 1. The core of a group is distributive if and only if every element of the group commutes with each of its conjugates.

Proof. Simplify the distributivity condition **QDist** by multiplying on the right by z^{-1}.

$$xz^{-1} \triangleright (yz^{-1} \triangleright 1) = (xz^{-1} \triangleright yz^{-1}) \triangleright (xz^{-1} \triangleright 1).$$

This yields the identity involving two variables

$$u \triangleright (v \triangleright 1) = (u \triangleright v) \triangleright (u \triangleright 1),$$

which reduces to the identity

$$u(v^{-1}uv) = (v^{-1}uv)u.$$

□

Groups in which conjugate elements commute have been studied by Burnside and others. If such a group is generated by two elements, then its commutator is contained in its center, and so its core is Abelian. This suggests that a distributive 2-quandle generated by three points is Abelian.

Proposition 2. The free distributive 2-quandle on three points appears as

$$Q = \{(m, n) \in \mathbf{Z} \times \mathbf{Z} \,|\, \text{at most one of } m \text{ and } n \text{ is odd}\}$$

as a subquandle of Core($\mathbf{Z} \times \mathbf{Z}$) with $(0, 0)$, $(1, 0)$, and $(0, 1)$ as generators.

Proof. Let D be a distributive 2-quandle and $f(0, 0)$, $f(1, 0)$, $f(0, 1)$ three points of D. We extend f to all of Q. Since Core $\mathbf{Z}$ is the free 2-quandle on two points, we can extend f uniquely to $\mathbf{Z} \times 0$ and $0 \times \mathbf{Z}$. Inductively define $f(2m, n)$ as $f(2m-1, -n) \triangleright f(2m-1, 0)$ for positive integers m, and $f(2m, n)$ as $f(2m+2, -n) \triangleright f(2m+1, 0)$ for negative integers m. For $n = 0$ this agrees with the previous definition of $f(2m, 0)$. We show

$$f(2m, n) \triangleright f(p, 0) = f(2p - 2m, -n) \tag{1}$$

by induction on $d = |2m - p|$. (1) holds for $d = 0$. It suffices to prove (1) for $2m > p$ by symmetry at $f(p, 0)$. (1) holds for $d = 1$ by definition of $f(2p - 2m, -n)$. Assume (1) holds for $d - 1$ and $d - 2$. Then

$$\begin{aligned} f(2m, n) \triangleright f(p, 0) &= f(2m - 2, -n) \triangleright f(2m - 1, 0) \triangleright f(p, 0) \\ &= (f(2m - 2, -n) \triangleright f(p, 0)) \triangleright (f(2m - 1, 0) \triangleright f(p, 0)) \\ &= f(2p - 2m + 2, n) \triangleright f(2p - 2m + 1, 0) \\ &= f(2p - 2m, -n). \end{aligned}$$

Analogously, we may define $f'(m, 2n)$ where $f'(0, q) = f(0, q)$ and $f'(p, 0) = f(p, 0)$ so that

$$f'(m, 2n) \triangleright f'(0, q) = f'(-m, 2q - 2n). \tag{1'}$$

From distributivity, we have the identity of lemma 1,

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

Taking $x = f(0, 0)$, $z = f(0, n)$, and $y = f(m, 0)$, we find that $f'(2m, 2n) = f(2m, 2n)$. Thus, we may eliminate the primes. We have defined f on all of Q. It remains to show that f is a homomorphism. We will show

$$f(2m, n) \triangleright f(0, q) = f(-2m, 2q - n). \tag{2}$$

Now, (2) holds for $q = 0$, and by reflection through $(0, 0)$, it suffices to show (2) for $q > 0$. Assume for a moment that (2) holds for $q = 1$. Then by induction on $q > 1$, we have

$$\begin{aligned} f(2m, n) \triangleright f(0, q) &= f(2m, n) \triangleright (f(0, q - 2) \triangleright f(0, q - 1)) \\ &= f(2m, n) \triangleright f(0, q - 1) \triangleright f(0, q - 2) \triangleright f(0, q - 1) \\ &= f(-2m, 2q - n). \end{aligned}$$

Thus, it suffices to show (2) for $q = 1$:

$$f(2m, n) \triangleright f(0, 1) = f(-2m, 2 - n). \tag{3}$$

By a similar induction it suffices to show (3) holds for $n = 0$ and $n = 1$. The $n = 0$ case is a special case of (1'), and the $n = 1$ case follows from projecting $f(m, 0)$, $f(0, 0)$, and $f(-m, 0)$ from $f(0, -1)$. Thus, (2) holds. Similarly, we have

$$f(m, 2n) \triangleright f(p, 0) = f(2p - m, -2n)). \tag{2'}$$

Finally, we show for (x, y) in Q that

$$f(x, y) \triangleright f(2p, q) = f(4p - x, 2q - y)). \tag{4}$$

$$\begin{aligned} f(x, y) \triangleright f(2p, q) &= f(x, y) \triangleright (f(0, -q) \triangleright f(p, 0)) \\ &= f(x, y) \triangleright f(p, 0) \triangleright f(0, -q) \triangleright f(p, 0) \\ &= f(2p - x, -y) \triangleright f(0, -q) \triangleright f(p, 0) \\ &= f(x - 2p, y - 2q) \triangleright f(p, 0) \\ &= f(4p - x, 2q - y). \end{aligned}$$

Along with (4') we have shown that f is a homomorphism. □

As a corollary, we have that any distributive 2-quandle generated by three points is Abelian.

Soublin [15] constructs a nonAbelian distributive quandle M_{81} of order 81. It is the smallest nonAbelian distributive quandle satisfying $x \triangleright y = y \triangleright x$.

3.5 Involutions

A natural occurrence of involutory quandles is that of the set of involutions in a group G. More generally, for n a positive integer

$$Q_n(G) = \{x \in G \mid x^n = 1\}$$

is an n-quandle with conjugation as the quandle operation. Q_n is a functor: (groups) $\to$ (n-quandles). Adjoint to Q_n is the functor AdQ_n : (n-quandles) $\to$ (groups). For an n-quandle Q, $AdQ_n(Q)$ is a group presented as

$$AdQ_n(Q) = (\overline{p},\ \text{for } p \in Q : \overline{p}^n = 1, \overline{p \triangleright q} = \overline{q}^{-1}\overline{p}\,\overline{q},\ \text{for } p, q \in Q).$$

The degree to which AdQ_n relates n quandles to groups may be seen in part by the following proposition.

Proposition. For an n-quandle Q, the order of the group $AdQ_n(Q)$ is no greater than n raised to the order of Q. $|AdQ_n(Q)| \leq n^{|Q|}$.

Lemma. Let the elements of an n-quandle Q be well ordered. Than any element of $AdQ_n(Q)$ may be written as a finite product of the generators in nondecreasing order.

Proof. The proposition follows directly from the lemma. We prove the lemma by a double induction.

Let $z = \overline{x}_1 \cdots \overline{x}_m$ be an element of $G = AdQ_n(Q)$, each x_i in Q, not necessarily distinct. By induction on m, the length of the product, we may assume that a product of length less than m may be written with the x_i's in nondecreasing order. So we may assume $x_1 \preceq x_2 \preceq \cdots \preceq x_{m-1}$. By transfinite induction on x_m, we may assume that products of length m whose first $m-1$ terms are in order and whose n-th term is less than x_m may be written in nondecreasing order. We show now that z may be rewritten in order without increasing its length. If $x_{m-1} \preceq x_m$, then Z is already in order.

Otherwise, $x_{m-1} \succ x_m$. Let $y = x_m \triangleright^{-1} x_{m-1}$. Then $\overline{x}_{m-1}\overline{x}_m = \overline{y}\,\overline{x}_{m-1}$, and so $z = \overline{x}_1 \cdots \overline{x}_{n-2}\overline{y}\,\overline{x}_{n-1}$. By the first induction we may write $\overline{x}_1 \cdots \overline{x}_{n-2}\overline{y}$ in nondecreasing order as $\overline{y}_1 \cdots \overline{y}_{n-1}$, so $z = \overline{y}_1 \cdots \overline{y}_{n-1}\overline{x}_{n-1}$. By the second induction, using the fact that $x_{n-1} \prec x_n$, we may write z in nondecreasing order. □

The bound of $2^{|Q|}$ is achieved for finite 2-quandles satisfying $x \triangleright y = x$. Since $AdQ_n(Q)$ maps onto $\operatorname{Inn} Q$, we have as a corollary that $|\operatorname{Inn} Q| \leq n^{|Q|}$.

3.6 Moufang loop cores

The functor Core : (groups) $\to$ (2-quandles) may be extended from groups to Moufang loops. Recall that a *loop* is a set G equipped with a binary operation (usually written multiplicatively) with an identity element 1, $x1 = 1x = x$, such that for all a, b in G there are unique solutions to the equations $xa = b$ and $ay = b$. Thus, a loop is a

quasigroup with an identity element. A loop has *the inverse property* when it has an operation $x \mapsto x^{-1}$ satisfying $(xy^{-1})y = x$ and $y(y^{-1}x) = x$. Such loops also satisfy $x^{-1}x = xx^{-1} = 1$, $(x^{-1})^{-1} = x$, $(xy)^{-1} = y^{-1}x^{-1}$, and $x^{-1}(xy) = y = (yx)x^{-1}$.

A loop is a *Moufang loop* if it satisfies

$$(xy)(zx) = (x(yz))x. \tag{1}$$

Moufang loops have the inverse property, and they satisfy the identities

$$((xy)z)y = x(y(zy)), \text{ and} \tag{2}$$

$$x(y(xz)) = ((xy)x)z. \tag{3}$$

Although a Moufang loop need not be a group, for it need not be associative, any subloop generated by two elements is a group. Also, if x, y, z are three elements of a Moufang loop which *associate*, that is, $(xy)z = x(yz)$, then the subloop which they generate is a group.

For a discussion of Moufang loops and proofs of the above statements see chapter vii of Bruck's book [3]. A basic problem of Moufang loops (and of loops and quasigroups in general) is to determine when two loops are isotopic. An *isotopy* of two quasigroups G, H consists of three bijections $f, g, h : G \to H$ such that for all x, y in G

$$f(x)g(y) = h(xy).$$

Bruck defined the *core* of a Moufang loop as the underlying set of the loop along with the binary operation $(x, y) \mapsto yx^{-1}y$ (which we denote $x \triangleright y$) in order to have a property of Moufang loops invariant under isotopy. If two Moufang loops are isotopic, then their cores are isomorphic. Work on cores of loops more inclusive than Moufang loops may be found in Robinson [12] and Burn [4].

Proposition 1. The core of a Moufang loop is a 2-quandle.

Proof. Axioms **Q1** and **QInv** hold since they only involve two variables, and they hold in the case of a group. To show axiom **Q3** first observe that $xz \triangleright yz = (x \triangleright y)z$. Indeed,

$$\begin{aligned} xz \triangleright yz &= (yz)(xz)^{-1}(yz) \\ &= (yz)(z^{-1}x^{-1})(yz) \\ &= ((yz)z^{-1})(x^{-1}(yz)) \qquad \text{by (1)} \\ &= y(x^{-1}(yz)) \\ &= (yx^{-1}y)z \qquad \text{by (3)} \\ &= (x \triangleright y)z. \end{aligned}$$

Similarly, $zx \triangleright zy = z(x \triangleright y)$. Also $(x \triangleright y)^{-1} = x^{-1} \triangleright y^{-1}$. Hence,

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

□

A Moufang loop is *commutative* if $xy = yx$. We will write commutative Moufang loops additively. We have from (2) the identity

$$((x + y) + z) + y = x + (y + (z + y)),$$

which is equivalent to

$$(x + y) + z = ((2z + z) + x) - y. \tag{4}$$

Proposition 2. The core of a commutative Moufang loop is distributive.

Proof. $x \triangleright y = 2y - x$. $2(x \triangleright y) = 2x \triangleright 2y$.

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

□

Proposition 3. The core of a Moufang loop is distributive if and only if every element commutes with each of its conjugates.

Proof. The proof is identical to that of proposition 1 in section 3.4. □

Proposition 4. The core of a commutative Moufang loop G is Abelian if and only if G is a group.

Proof. The proof that the core of an Abelian group is an Abelian quandle is direct.

Let G be a commutative Moufang loop with an Abelian core. Abelianness gives

$$(4z - 2y) - (2x - w) = (4z - 2x) - (2y - w).$$

Setting $z = 0$ and negating x and y, we find

$$(w + 2x) + 2y = (w + 2y + 2x).$$

Since the subloop generated by w, $2x$ and $2y$ is associative, w, $2x$, and $2y$ associate in any order. Note

$$\begin{aligned}(w + x) + 2y &= ((2x + 2y) + w) - x \qquad \text{by (4)} \\ &= ((2y + w) + 2x) - x \\ &= (2y + w) + x.\end{aligned}$$

Hence, w, x, and $2y$ associate. Finally,

$$\begin{aligned}(w + y) + x &= ((2y + x) + w) - y \qquad \text{by (4)} \\ &= ((x + w) + 2y) - y \\ &= (x + w) + y.\end{aligned}$$

Thus, G is associative. □

3.7 Distributive 2-quandles with midpoints

Definition. Let Q be a 2-quandle. A *midpoint* between two points x and y of Q is a point m such that $x \triangleright m = y$ (and so $y \triangleright m = x$). Q is said to *have midpoints* if there is a midpoint between any two of its points.

If Q is a finite 2-quandle with midpoints, then midpoints are unique. Midpoints need not be unique in the infinite case. Consider, for example, $Q = \mathrm{Core}\,\mathbf{R}/\mathbf{Z}$. Between 0 and $\frac{1}{2}$ lie the midpoints $\frac{1}{4}$ and $\frac{3}{4}$.

The assumption that a commutative Moufang loop is 2-divisible, that is, for each element x there exists an element y such that $2y = x$, implies that its core has midpoints.

Proposition. Let Q be a distributive 2-quandle with midpoints and 0 be a fixed element of Q. Then Q has the structure of a 2-divisible commutative Moufang loop, $L(Q)$, by taking $x + y = 0 \triangleright m$ where m is any midpoint between x and y.

Lemma. Let Q be a distributive 2-quandle with midpoints. Let $x, y \in Q$. Then any two midpoints between x and y are behaviorally equivalent.

Proof of lemma. Let m be a midpoint between x and y. Let z be a point of Q. We show that $z \triangleright m$ depends only on z, x, and y, not on m. Take n to be a midpoint between z and y. Using a variant of the identity (1) in lemma 1, section 3.4, we have

$$\begin{aligned} z \triangleright m &= z \triangleright n \triangleright m \triangleright z \triangleright n \\ &= y \triangleright m \triangleright z \triangleright n \\ &= x \triangleright z \triangleright n. \end{aligned}$$

The last expression does not depend on m. □

Proof of proposition. Addition is well-defined by the lemma. Clearly, addition is commutative, and 0 is an additive identity. To show that $L(Q)$ is a loop, we must show that for all $x, y \in Q$, there is a unique z in Q such that $x + z = y$. Let m be a midpoint between 0 and y, and set $z = x \triangleright m$. Then $x + z = y$. Conversely, if $x + z = y$, and m is a midpoint between x and z, then m is a midpoint between 0 and y, and by the lemma, $z = x \triangleright m$

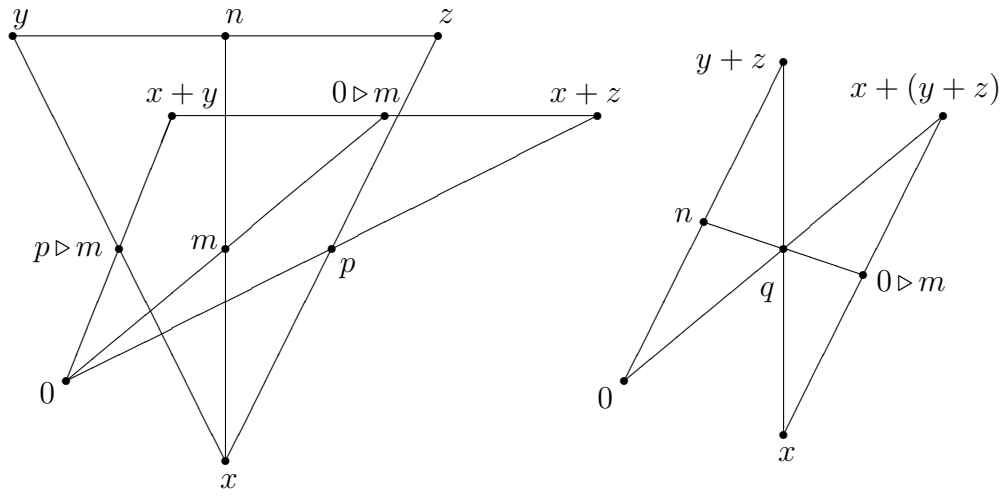
Next we show the Moufang identity for commutative loops:

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

Let n be a midpint between y and z, m a midpoint between x and n, and p a midpoint between x and z. As shown in figure 3.5, by projecting p, m, and $p \triangleright m$ from x, we conclude that $p \triangleright m$ is a midpoint between x and y. Projecting p, m, and $p \triangleright m$ from 0, we find $0 \triangleright m$ is a midpoint between $x + y$ and $x + z$. Hence, $0 \triangleright (0 \triangleright m) = (x + y) + (x + z)$. Now take q to be a midpoint between $0 \triangleright m$ and n. Then $x \triangleright q = n \triangleright m \triangleright q$, which by lemma 1, section 3.4, equals $n \triangleright q \triangleright m \triangleright n$. So

$$\begin{aligned} x \triangleright q &= n \triangleright q \triangleright m \triangleright n \\ &= 0 \triangleright m \triangleright m \triangleright n \\ &= 0 \triangleright n = y \triangleright z. \end{aligned}$$

Figure 3.5: Midpoints



Therefore, q is a midpoint between x and $y + z$. As indicated in figure 3.5, we find that $0 \triangleright m$ is a midpoint between x and $x + (y + z)$ by reflecting 0, n, and $y + z$ through q. Hence, $0 \triangleright m$ also equals $x + (x + (y + z))$.

Thus, $L(Q)$ is a Moufang loop. Finally, $L(Q)$ is 2-divisible, since if m is a midpoint between 0 and x, then $x = 2m$. □

The functors Core and L are inverse to each other, so we have an isomorphism of categories; the category of 2-divisible commutative Moufang loops is isomorphic to the category of pointed distributive 2-quandles with midpoints. By proposition 4 of section 3.6, this isomorphism restricts to an isomorphism from the category of 2-disvisible Abelian groups to the category of pointed Abelian 2-quandles with midpoints.

Chapter 4

Algebraic topology and knots

4.1 The fundamental quandle of a pair of spaces.

Consider the category $\mathcal{P}'$ of pairs of topological spaces (X, K), K a subspace of X, where a map $f : (X, K) \to (Y, L)$ in $\mathcal{P}'$ is given by a continuous map $f : X \to Y$ such that $f^{-1}(L) = K$. Two maps $f, g : (X, K) \to (Y, L)$ in $\mathcal{P}'$ are said to be *homotopic*, written $f \sim g$, if there is a map $h : (X \times I, K \times I) \to (Y, L)$ in $\mathcal{P}'$, where I is the unit interval, such that $h(x, 0) = f(x)$ and $h(x, 1) = g(x)$ for all x in X. This concept of homotopy in $\mathcal{P}'$ yields a category $[\mathcal{P}']$ of pairs of topological spaces where the maps are homotopy classes of maps in $\mathcal{P}'$.

For our purposes we must consider pointed spaces. Let $\mathcal{P}$ be the category whose objects are pairs of spaces (X, K) along with a distinguished point $*$ in $X - K$, called the *basepoint*, and whose maps between pairs preserve the basepoint. If (X, K) is such a pointed pair, let $X \wedge I$ be the quotient $(X \times I)/(\{*\} \times I)$ of $X \times I$. Two maps $f, g : (X, K) \to (Y, L)$ in $\mathcal{P}$ are *homotopic*, written $f \sim g$, if there is a map $h : (X \wedge I, K \times I) \to (Y, L)$ in $\mathcal{P}$ such that $h(x, 0) = f(x)$ and $h(x, 1) = g(x)$ for all x in X. Let $[\mathcal{P}]$ be the resulting homotopy category for $\mathcal{P}$.

One object of $[\mathcal{P}]$ is the circle $S = (S^1, \emptyset)$ where S^1 is the unit circle in the complex plane with the basepoint at 1. S is a cogroup in $[\mathcal{P}]$, that is, S has a group structure in $[\mathcal{P}^{\mathrm{op}}]$. Since we will be dealing with this cogroup in some detail, let us describe this structure explicitly. We need a comultiplication $\mu : S \to S \vee S$, a coinversion $\sigma : S \to S$, and a coidentity $S \to (1, \emptyset)$. There is only one map $S \to (1, \emptyset)$ so it is the coidentity. Define σ by $\sigma(z) = z^{-1}$. Represent $S \vee S$ as $S \times \{1, 2\}$ with the points $(1, 1)$ and $(1, 2)$ identified. Then define μ by

$$\mu(e^{it}) = \begin{cases} (e^{2it}, 1) & \text{for } 0 \leq t \leq \pi \\ (e^{2it}, 2) & \text{for } \pi \leq t \leq 2\pi. \end{cases}$$

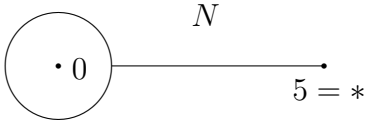
With these definitions S becomes a cogroup. The homotopy classes of maps from S to any object (X, K) form a group $\pi(X, K)$ which is just the fundamental group of $X - K$, $\pi_1(X - K)$.

A map $\alpha : S \to (X, K)$ is called a *loop* in $X - K$. If α and β are two loops, we let $\alpha^{-1} = \sigma\alpha$ and $\alpha\beta = \mu(\alpha \vee \beta)$. Then $\alpha\alpha^{-1} \sim 1$ and $(\alpha\beta)\gamma \sim \alpha(\beta\gamma)$.

Unfortunately, $\pi(X, K)$ gives only partial information about the way that K is situated in X, no more than the circumstantial information concerning $X - K$. For instance, when K is a knot in 3-space X, $\pi(X, K)$ is the knot group, and although the knot group distinguishes many knots, it fails to distinguish the square knot from the granny knot. We will replace the pair $S = (S^1, \emptyset)$ by a pair where the subspace forms an integral part of the whole. In doing so, we will not have a cogroup, but only a coquandle.

Let N be the object $(X, 0)$ in $\mathcal{P}$ where X is the subspace of the complex numbers consisting of the union of the closed unit disk $\{z \in \mathbf{C} \,|\, |z| \leq 1\}$ and the "rope" $\{z \in \mathbf{C} \,|\, z \text{ real and } 1 \leq z \leq 5\}$, where 0 denotes $\{0 \in \mathbf{C}\}$, and the basepoint $*$ of X is 5.

Figure 4.1: The noose N



We will show that N is a coquandle, but not directly. Instead, we will show that S and N together form a co-augmented-quandle. This entails the construction of two maps in $\mathcal{P}$, $a : N \to N \vee S$ and $d : S \to N$ so that in $[\mathcal{P}]^{\text{op}}$ the two axioms **AQ1** and **AQ2**, as stated in section 2.10, are satisfied. Once this is done, S and N will represent a contravariant functor from $[\mathcal{P}]$ to the category of augmented quandles which will extend the fundamental group functor.

Let $d : S \to N$ wrap the circle around the disk of N by way of the rope of N.

$$d(e^{it}) = \begin{cases} 5 - 8t/\pi & \text{for } 0 \leq t \leq \pi/2, \\ e^{2i(t-\pi/2)} & \text{for } \pi/2 \leq t \leq 3\pi/2, \\ 8t/\pi - 11 & \text{for } 3\pi/2 \leq t \leq 2\pi. \end{cases}$$

The map d may be interpreted as the boundary of N. Let the map $a : N \to N \vee S$ place the disk of N onto the disk of $N \vee S$, then stretch the rope of N along the rope of $N \vee S$ to the basepoint and around the circle of $N \vee S$.

$$a(z) = \begin{cases} z \in N & \text{if } |z| \leq 1, \\ 2z - 1 \in N & \text{if } 1 \leq z \leq 3, \\ e^{i(z-3)\pi} \in S & \text{if } 3 \leq z \leq 5. \end{cases}$$

In order to show that a gives a group action, we must show that the diagram

$$\begin{array}{ccc} N & \xrightarrow{a} & N \vee S \\ {\scriptstyle a}\downarrow & & \downarrow{\scriptstyle a \vee 1} \\ N \vee S & \xrightarrow{1 \vee \mu} & N \vee S \vee S \end{array}$$

commutes up to homotopy. Both maps $f = a(a \vee 1)$ and $g = a(1 \vee \mu)$ place the disk of N onto the disk of $N \vee S \vee S$ then stretch the rope of N along the rope of $N \vee S \vee S$ and around each circle of $N \vee S \vee S$. Restricted to the disk of N, f equals g. They only differ with regard to the rate that they stretch the rope. A homotopy $h : N \times I \to N \vee S \vee S$ between f and g is

$$h(z,t) = \begin{cases} f(z) & \text{if } |z| \leq 1, \\ f((z-1)(1-t/2)+1) & \text{if } 1 \leq z \leq 3, \\ f(z-t) & \text{if } 3 \leq z \leq 4, \\ f(5-(5-z)(1+t)) & \text{if } 4 \leq z \leq 5. \end{cases}$$

In order to show **AQ1** holds we must show that the diagram

$$\begin{array}{ccccc} N & \xrightarrow{a} & N \vee S & \xrightarrow{1 \vee d} & N \vee N \\ & \searrow^{1} & & & \downarrow \delta \\ & & & & N \end{array}$$

commutes up to homotopy. Represent $N \vee N$ as $N \times \{1,2\}$ with basepoints identified. Then the map $\delta : N \vee N \to N$ is given by $\delta(z,n) = z$. Let $f = a(1 \vee d)\delta$. Then $f : N \to N$ is formulated as

$$f(z) = \begin{cases} z & \text{if } |z| \leq 1, \\ 2(z-1)+1 & \text{if } 1 \leq z \leq 3, \\ 5-8(z-3) & \text{if } 3 \leq z \leq 3.5 \\ \exp(2i(z-3.5)\pi) & \text{if } 3.5 \leq z \leq 4.5 \\ 8(z-4.5)+1 & \text{if } 4.5 \leq z \leq 5. \end{cases}$$

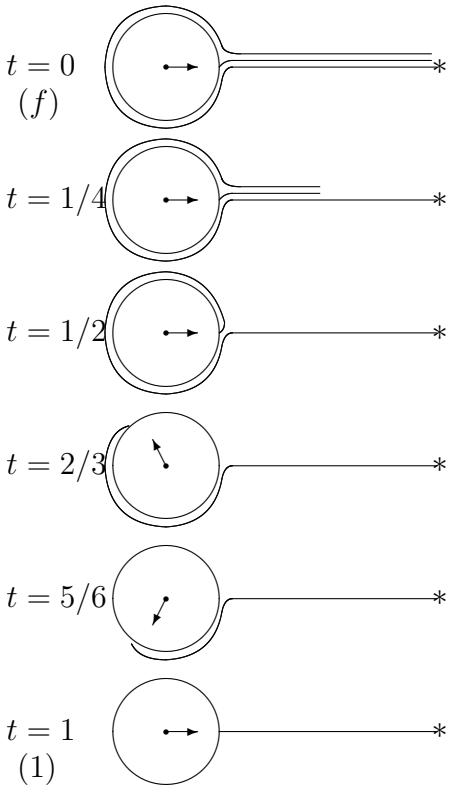
Verbally described, f places the disk of N onto itself, then stretches the rope along and back itself, around the disk, and back to the basepoint. In the category $\mathcal{P}$ a homotopy is not allowed to pass any point of $X - A$ through A; in particular, the rope of N may not pass through the origin. The required homotopy, $f \sim 1$, may be made by rotating the disk counterclockwise one revolution while contracting the string to its initial position. Figure 4.2 illustrates such a homotopy.

In order to show the axiom **AQ2** holds, we must verify that the diagram

$$\begin{array}{ccccc} S & \xrightarrow{\mu} & S \vee S & \xrightarrow{\mu \vee 1} & S \vee S \vee S \\ {\scriptstyle d}\downarrow & & & & \downarrow {\scriptstyle \begin{pmatrix} \sigma & 0 \\ 0 & d \\ 1 & 0 \end{pmatrix}} \\ N & & \xrightarrow{\qquad a \qquad} & & N \vee S \end{array}$$

commutes up to homotopy. Both of the compositions describe a loop in $N \vee S$ starting at the basepoint, clockwise around the circle of $N \vee S$, around the boundary of N in $N \vee S$, and counterclockwise around the circle of $N \vee S$ back to the basepoint. The two loops only differ by their rate, and hence are homotopic.

Figure 4.2: $f = a(1 \vee d)\delta : N \to N$ is homotopic to 1

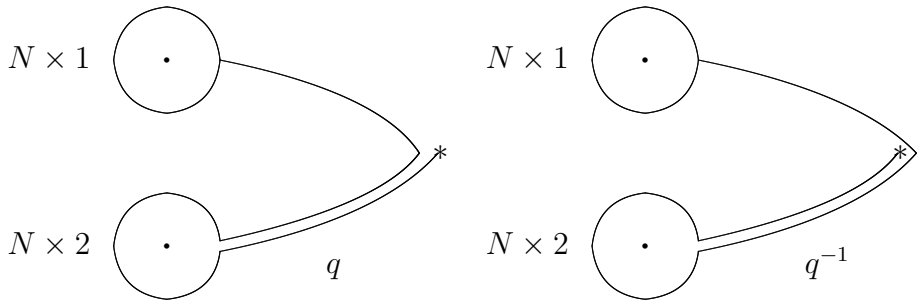


Thus, S and N together represent a contravariant function AQ from $[\mathcal{P}]$ to the category of augmented quandles. Let (X, K) be an object of $\mathcal{P}$. A *noose* about K is a map $\nu : N \to (X, K)$ in in $\mathcal{P}$. If α is a loop in $X - K$ and ν is a noose about K, let $\nu\alpha = a(\nu \vee \alpha)$ and $\epsilon(\nu) = d\nu$. We call $\epsilon(\nu)$ the *boundary loop* of ν. If β is another loop in $X - K$, we have

$$(\nu\alpha)\beta \sim \nu(\alpha\beta), \text{ and}$$
$$\epsilon(\nu\alpha) \sim \alpha^{-1}\epsilon(\nu)\alpha.$$

If μ and ν are nooses about K, let $\mu \triangleright \nu = \mu\epsilon(\nu)$. Then the homotopy classes of nooses in X about K form a quandle, $Q(X, K)$. We name $Q(X, K)$ the *fundamental quandle* of (X, K), and we name $AQ(X, K)$ the *fundamental augmented quandle* of (X, K). $AQ(X, K)$ is the fundamental quandle augmented by the fundamental group of $X - K$.

Figure 4.3: q and q^{-1}



As N is a coquandle, a presentation of its structure is in order. The structure is given by two maps, $q, q' : N \to N \vee N$, q used to represent $\triangleright$ and q' to represent $\triangleright^{-1}$. The map q is to be homotopic to $a(1 \vee d)$. Let $N \vee N$ be $N \times \{1, 2\}$ with basepoints identified. Then such a map is

$$q(z) = \begin{cases} (z, 1) & \text{if } |z| \leq 1, \\ (4(z-1)+1, 1) & \text{if } 1 \leq z \leq 2, \\ (5-4(z-2), 2) & \text{if } 2 \leq z \leq 3, \\ (\exp(2\pi i(z-3)), 2) & \text{if } 3 \leq z \leq 4, \\ (4(z-4)+1, 2) & \text{if } 4 \leq z \leq 5. \end{cases}$$

The map q places the disk of N onto the first disk of $N \vee N$ and stretches the rope of N along the first rope of $N \vee N$ and around the boundary of the second N. See figure 4.3. The map q' is defined similarly except that $(\exp(-2\pi i(z-e)), 2)$ is used in the case $3 \leq z \leq 4$.

In forthcoming proofs we will have occasion to compose nooses with paths as well as loops. If ν is a noose in X about K with basepoint $*$, and α is a path in $X - K$ from $*$ to $*'$, then let $\nu\alpha$ denote the composition. $\nu\alpha$ is a noose in X about K with basepoint

$*'$. Let $\operatorname{Disk}\nu$ denote the noose with basepoint $\nu(1)$, ($\operatorname{Disk}\nu : N \to (X, K)$ is constantly $\nu(1)$ on the rope of N). Let $\operatorname{Rope}\nu$ denote the path from $\nu(1)$ to $*$ along the image of ν. Then $\nu \sim (\operatorname{Disk}\nu)(\operatorname{Rope}\nu)$.

4.2 The fundamental quandle of a disk

Let $(D, 0)$ be the object in $\mathcal{P}$ where D is the closed unit disk in the complex plane and 0 is the center of the disk.

Proposition. Any element of $Q(D, 0)$ is uniquely representable as a noose $f : N \to (D, 0)$

$$f(z) = \begin{cases} re^{in\theta} & \text{if } |z| \leq 1, z = re^{i\theta}, \\ 1 & \text{if } 1 \leq z \leq 5, \end{cases}$$

for a unique integer n. n is the winding number of the boundary of f around 0.

Proof. In order to simplify computations, we may take N to be $(D, 0)$ as they are homotopically equivalent in the category $\mathcal{P}$. To further simplify the description of the homotopies, we will take D to be $S^1 \times [0, \infty)$ union a point at infinity (to correspond to the center of D).

Let $f : D \to D$ be continuous such that $f^{-1}(\infty) = \infty$. First we construct a homotopy so that we may assume $f(S^1 \times 0) \subseteq S^1 \times 0$. Since $f(S^1 \times 0)$ is compact and misses ∞, there is an x_0 such that $f(S^1 \times 0) \subseteq S^1 \times [0, x_o]$. We use a homotopy to squeeze $S^1 \times [0, x_0]$ to $S^1 \times 0$. Using the notation $f(\theta, x) = (f^1(\theta, x), f^2(\theta, x))$, define $h : D \times I \to D$ by

$$h(\theta, x, t) = \begin{cases} (f^1(\theta, x), f^2(\theta, x) - tx_0) & \text{if } x \geq tx_0 \\ (f^1(\theta, x), 0) & \text{if } x \leq tx_0. \end{cases}$$

Then $h(\theta, x, 0) = f(\theta, x)$ while $h(\theta, 0, 1) \subseteq S^1 \times 0$. We may therefore assume that $f(S^1 \times 0) \subseteq S^1 \times 0$.

Now f restricted to $S^1 \times 0$ gives a loop in $S^1 \times 0$, so is homotopic to the map $(\theta, 0) \to (n\theta, 0)$, where n is the winding number. Then there is a map $h : S^1 \times 0 \times I \to S^1 \times 0$ such that $h(\theta, 0, 0) = f(\theta, 0)$ and $h(\theta, 0, 1) = (n\theta, 0)$. We construct a homotopy $H : D \times I \to D$ extending h. Let

$$H(\theta, x, t) = \begin{cases} f(\theta, x - t) & \text{if } x \geq t, \\ h(\theta, 0, t - x) & \text{if } x \leq t. \end{cases}$$

Then $H(\theta, x, 0) = f(\theta, x)$ while $H(\theta, 0, 1) = (n\theta, 0)$. Thus, we may assume $f(\theta, 0) = (n\theta, 0)$.

Finally, we show f is homotopic to the map $(\theta, x) \mapsto (n\theta, x)$. We will define a homotopy $H : D \times I \to D$ which spreads the influence of the restriction of f to $S^1 \times 0$ down the entire cylinder $S^1 \times [0, \infty)$. Let

$$H(\theta, x, t) = (f^1(\theta, (1 - t)x), f^2(1 - t)x + tx).$$

Then $H(\theta, x, 0) = (f^1(\theta, x), f^2(\theta, x)) = f(\theta, x)$, and $H(\theta, x, 1) = (f^1(\theta, 0), f^2(\theta, 0) + x) = (n\theta, x)$. We should check that setting $H(\infty, t)$ to ∞ leaves H continuous. Given $N > 0$, we must show there exists an $M > 0$ such that for all $x > M$, $H^2(\theta, x, t) > N$. Let M_1 be such that if $x > M_1$, then $f^2(\theta, x) > N$. Let $M = \max\{2M_1, 2N\}$. Suppose $x > M$. Then $x/2 > M_1$ and $x/2 > N$.

Case 1. $t \geq \frac{1}{2}$. $H^2(\theta, x, t) = f^2(\theta, (1-t)x) + tx \geq tx \geq x/2 > N$.

Case 2. $t \leq \frac{1}{2}$. $H^2(\theta, x, t) = f^2(\theta, (1-t)x) + tx \geq f^2(\theta, (1-t)x)$ which is greater than N since $(1-t)x \geq x/2 > M_1$.

Thus, H gives a homotopy of f to the map $(\theta, x) \mapsto (n\theta, x)$. □

The quandle operation on $Q(D, 0)$ is first projection, that is $x \triangleright y = x$.

4.3 The Seifert-Van Kampen theorem

Recall the Seifert-Van Kampen theorem for the fundamental group. Let X be an arcwise connected topological space with a basepoint, and let $\{U_i\}$ be a covering of X by arcwise connected open sets closed under pairwise intersections such that each open set U_i contains the basepoint. Then

$$\pi_1(X) = \varinjlim \pi_1(U_i).$$

We will prove an analogous theorem for the fundamental quandle of a pair of spaces.

Theorem. Let (X, K) be an object in $\mathcal{P}$. Let $\{U_i\}$ be a covering of X closed under pairwise intersection. Assume for each index i that U_i is a neighborhood of $U_i \cap K$ and that $U_i - k$ is arcwise connected and contains the basepoint of X. Then

$$AQ(X, K) = \varinjlim AQ(U_i, U_i \cap K).$$

Proof. Let $AQ(X, K) = (Q, G)$. Then by the Seifert-Van Kampen theorem, $G = \pi_1(X - K) = \varinjlim \pi_1(U_i - K)$. By the theorem of section 2.10, the $\varinjlim AQ(U_i, U_i \cap K)$ is then of the form (L, G). By the universal property of (L, G), there is a unique $\psi : L \to Q$ determined by the maps $AQ(U_i, U_i \cap K) \to AQ(X, K) = (Q, G)$. We will show ψ is an isomorphism.

Surjectivity of ψ. By the theorem of section 2.10, it suffices to show that every noose γ about K is homotopic to some $\alpha\beta$ where α is a noose in some $(U_i, U_i \cap K)$, and β is a loop in $X - K$. Let γ be an arbitrary noose about K. $\gamma(0)$ lies in some U_i. Since $\gamma^{-1}(U_i)$ is a neighborhood of 0 in N, there is some $r > 0$ such that $|z| \leq r$ implies $\gamma(z) \in U_i$. Using the homotopy

$$H(z) = \begin{cases} \gamma(zr) & \text{if } |z| \leq 1 \\ \gamma((z-1)(5-4)/r + r) & \text{if } 1 \leq z \leq 5, \end{cases}$$

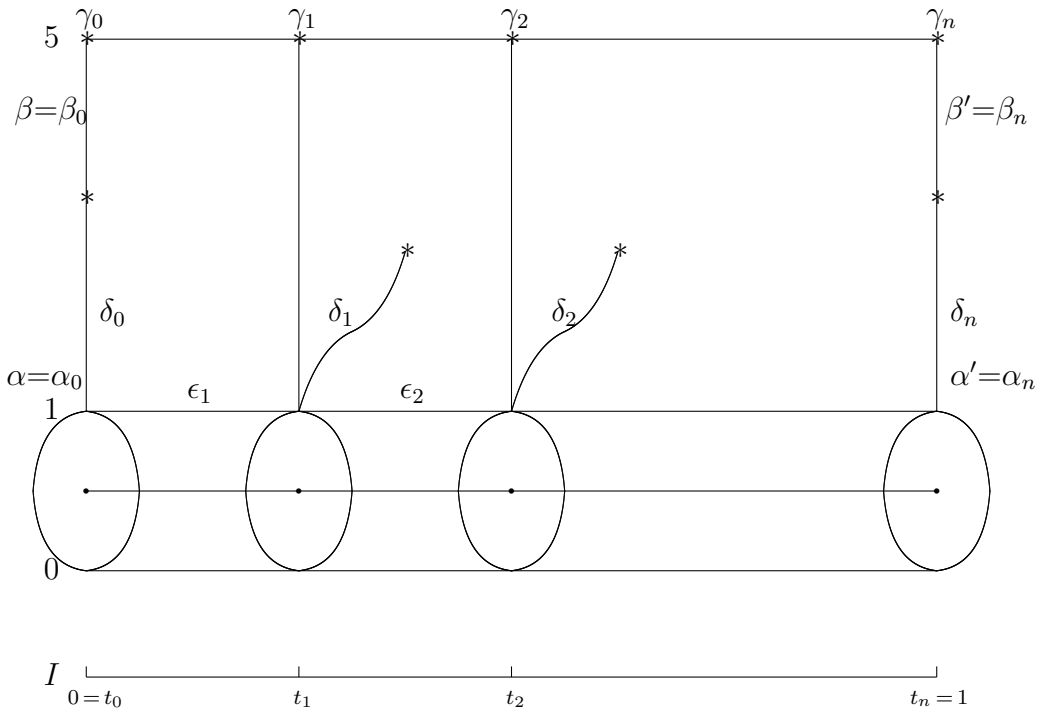
we may adjust γ so that we may assume $\gamma(z) \in U_i$ for $|z| \leq 1$. Choose a path δ in $U_i - K$ from $\gamma(1)$ to $*$. Let α be the noose $(\mathrm{Disk}\,\gamma)\delta$ in $(U_i, U_i \cap K)$ and β be the loop

$\delta^{-1}(\text{Rope}\,\gamma)$ in $X - K$. Then $\alpha\beta = (\text{Disk}\,\gamma)\delta\delta^{-1}(\text{Rope}\,\gamma) \sim (\text{Disk}\,\gamma)(\text{Rope}\,\gamma) \sim \gamma$ as required.

Injectivity of ψ. It suffices to show that if $\alpha\beta \sim \alpha'\beta'$ where α is a noose in $(U_i, U_i \cap K)$, β and β' are loops in $X - K$, and α' is a noose in $(U_{i'}, U_{i'} \cap K)$, then as elements of L, $\alpha\beta = \alpha'\beta'$. Let H effect the homotopy $\alpha\beta \sim \alpha'\beta'$; $H : N \times I \to X$, $H(z, 0) = (\alpha\beta)(z)$, $H(z, 1) = (\alpha'\beta')(z)$. The inverse images of the open sets U_i under $H(0, t)$ cover the unit interval I. Hence, we may divide I into subintervals $0 = t_0 < t_1 < \cdots < t_n = 1$ so that for each $j = 1, \ldots, n$ there is an index $i(j)$ for which $H(0, t) \in U_{i(j)}$ when $t_{i-1} \le t \le t_i$. We may take $i(1) = i$ and $i(n) = i'$. There is an $r > 0$ so that for $|z| \le r$ and $t_{j-1} \le t \le t_j$ we have $H(z, t) \in U_{i(j)}$. One r suffices for all j. By appropriate adjustments of α, α', and H we may assume $r = 1$.

Figure 4.4 illustrates the remainder of the proof. For $j = 0, 1, \ldots, n$ define the nooses $\gamma_j = H(z, t_j)$ in (X, K). Also choose paths δ_j from $\gamma_j(1)$ to $*$ in $U_{i(j-1)} \cap U_{i(j)} - K$ for $j = 1, 2, \ldots, n-1$, and set $\delta_0 = \text{Rope}\,\alpha$ and $\delta_n = \text{Rope}\,\alpha'$.

Figure 4.4: Seifert-Van Kampen noose homotopy



For $j = 0, \ldots, n$ define α_j to be the noose $(\text{Disk}\,\gamma_j)\delta_j$ in $(U_{i(j-1)} \cap U_{i(j)} - K, U_{i(j-1)} \cap U_{i(j)})$ and β_j to be the loop $\delta_j^{-1}(\text{Rope}\,\gamma_j)$ in $X - K$. Then $\alpha = \alpha_0$, $\alpha' = \alpha_n$. As nooses

in $(U_i, U_i \cap K)$ and $(U_{i'}, U_{i'} \cap K)$, $\alpha\beta \sim \alpha_0\beta_0$ and $\alpha'\beta' \sim \alpha_n\beta_n$, respectively. In order to show $\alpha\beta$ equals $\alpha'\beta'$ in L, we will show for $j = 1, \ldots, n$ that $\alpha_{j-1}\beta_{j-1}$ equals $\alpha_j\beta_j$.

Fix j between 1 and n. We must show $\alpha_{j-1} = \alpha_j\beta_j\beta_{j-1}^{-1}$. Let ϵ_j be the path from $\gamma_{j-1}(1)$ to $\gamma_j(1)$ in $U_{i(j-1)} - K$ given by $\epsilon_j(t) = H(1, t_{j-1} + t(t_j - t_{j-1}))$. The portion of the homotopy H on $[1, 5] \times [t_{j-1}, t_j]$ yields a homotopy in $X - K$ of ϵ_j to $(\mathrm{Rope}\,\gamma_{j-1})(\mathrm{Rope}\,\gamma_j)^{-1}$. Thus

$$\begin{aligned} \beta_{j-1}\beta_j^{-1} &= \delta_{j-1}^{-1}(\mathrm{Rope}\,\gamma_{j-1})(\mathrm{Rope}\,\gamma_j)^{-1}\delta_j \\ &= \delta_{j-1}^{-1}\epsilon_j\delta_j \end{aligned}$$

as elements of $\pi_1(X - K)$. The noose $\alpha_j\delta_{j-1}^{-1}\epsilon_j\delta_j$ lies entirely in $U_{i(j-1)}$ as does α_{j-1}. Moreover, the restriction of H to $\{|z| \leq 1\} \times [t_{j-1}, t_j]$ has an image in $U_{i(j-1)}$ and yields a homotopy of α_{j-1} to $\alpha_j\delta_{j-1}^{-1}\epsilon_j\delta_j$ in $(U_{i(j-1)} \cap K, U_{i(j-1)})$. Thus, $\alpha_{j-1} = \alpha_j\delta_{j-1}^{-1}\epsilon_j\delta_j = \alpha_j\beta_{j-1}\beta_j^{-1}$ as elements of L. □

Corollary. Let (X, K) be an object in $\mathcal{P}$. Let U and V be an open covering of X such that $U - K$, $V - K$, and $U \cap V - K$ are arcwise connected and contain the basepoint of X. Then $AQ(X, K)$ is the pushout

$$\begin{array}{ccc} AQ(U \cap V, U \cap V \cap K) & \longrightarrow & AQ(V, V \cap K) \\ \downarrow & & \downarrow \\ AQ(U, U \cap K) & \longrightarrow & AQ(X, K) \end{array}$$

□

4.4 Applications of the Seifert-Van Kampen theorem

The proposition in section 4.2 implies that if K is a point in the plane X, then $AQ(X, K) = (\mathrm{Conj}\,F, F)$ where F is the free group on one element. Consider a generalization where X is a 2-manifold.

Proposition 1. Let K be a point in a 2-manifold X, and let $G = \pi_1(X - K)$. Let U be the union of a small disk around K and a path to the basepoint, and let α be a loop in U winding once around K. Let F be the free group generated by one element and $f : F \to G$ send the generator of F to the homotopy class of α. Then

$$AQ(K, X) = (\mathrm{Conj}\,F \otimes_F G, G).$$

Proof. Let $V = X - K$. Then by the Seifert-Van Kampen theorem,

$$\begin{array}{ccc} AQ(U \cap V, \emptyset) = (\emptyset, F) & \longrightarrow & AQ(V, \emptyset) = (\emptyset, G) \\ \downarrow & & \downarrow \\ AQ(U, K) = (\mathrm{Conj}\,F, F) & \longrightarrow & AQ(X, K) \end{array}$$

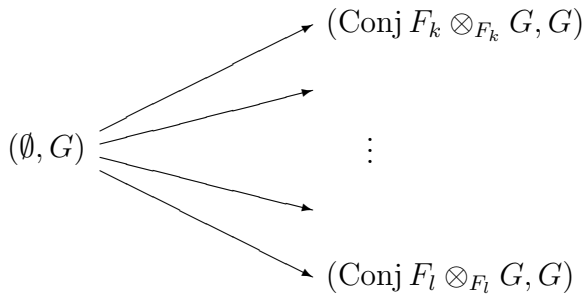
is a pushout square. Hence, by the theorem of section 2.10, we have $AQ(K, X) = (\mathrm{Conj}\, F \otimes_F G, G)$. □

Another generalization of the same proposition is where X remains the plane and K is a discrete subset of X. For each point k in K let $\alpha(k)$ be a small loop winding once around k. Then $G = \pi_1(X - K)$ is free on $\{\alpha(k) \,|\, k \in K\}$. For k in K let F_k be the free group on $\alpha(k)$ and $F_k \to G$ the inclusion homomorphism.

Proposition 2. X, K, G, F_k as above. Then

$$AQ(X, K) = (\bigcup_{k \in K} \mathrm{Conj}\, F_k \otimes_{F_k} G, G).$$

Proof. For k in K let $U_k = (X - K) \cup \{k\}$. Then $AQ(U_k, \{k\}) = (\mathrm{Conj}\, F_a \otimes_{F_a} G, G)$ by proposition 1. If $k, l \in K, k \neq l$, then $AQ(U_k \cap U_l, \emptyset) = (\emptyset, G)$. Thus, $AQ(X, K)$ is the limit of the diagram



which is $(\bigcup_{k \in K} \mathrm{Conj}\, F_k \otimes_{F_k} G, G)$. □

In most of the applications that follow K will be a submanifold of X of codimension two. When this is the case we will try to restrict our attention to those nooses in X "winding once" about K. For instance if X is an oriented 2-manifold and K is a discrete subset of X, "winding once" is well-defined.

Let X be the plane and K a discrete subset of X. Orient X and let $\overline{Q}$ consist of the nooses which wind exactly once (in the positive sense) around a point of K, and let $\overline{AQ}(X, K)$ be $\overline{Q}$ augmented by $G = \pi_1(X - K)$. Then by proposition 2, $\overline{AQ}(X, K) = (\bigcup_{k \in K} \{\alpha(k)\} \otimes_{F_k} G, G)$. Then $\overline{Q}$ is just the free quandle on $|K|$ elements, and is isomorphic to the quandle consisting of the conjugates of the generators of G.

4.5 Knot quandles

Recall that a *knot* is a subspace K of the 3-sphere $X = S^3$ which is homeomorphic to a circle. A *link* is a subspace K of X homeomorphic to a disjoint union of circles. Two knots or links K and K' are *equivalent* if there is a homeomorphism h of X such that $h(K) = K'$, that is, in the category $\mathcal{P}$, (X, K) is homeomorphic to (X, K'). We will

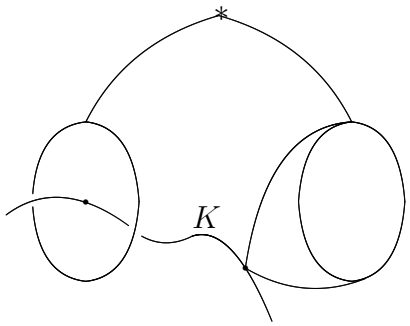
deal with oriented spaces; we assume X and K are endowed with orientations. (If K is a link, then we assume each component circle is oriented.) An *oriented equivalence* of K and K' is an orientation-preserving homeomorphism h of X such that $h(K) = K'$ and h preserves the orientation of each component of K. An equivalence class of oriented knots or links (under oriented equivalence) is called an *oriented knot type* or *oriented link type*, respectively. We assume all knots, links, and equivalences are oriented and henceforth omit the adjective "oriented".

The fundamental group of $X - K$, $\pi_1(X - K)$, is called the *knot group* (or *link group*). This definition assumes either that $X - K$ has a designated basepoint or else that the knot group is only defined up to noncanonical isomorphism; we assume a basepoint.

Recall that a *tame knot* is a knot equivalent to a closed polygonal curve in X. Some of the results below are restricted to tame knots and tame links.

Associated to a knot (X, K) we have the fundamental quandle $Q(X, K)$. An element of $Q(X, K)$ is represented by a noose ν about K. The boundary loop $\epsilon(\nu)$ may or may not link with K as shown in figure 4.5.

Figure 4.5: Noose boundary loops



In order to decide when a loop in $X - K$ links once with K, it suffices to choose a generator of $H_1(X - K) \cong \mathbf{Z}$. Then loops homologous to that generator have linking number 1 with K. Since we assume K and X have orientations, such a generator may be naturally chosen (say, by the right-hand rule).

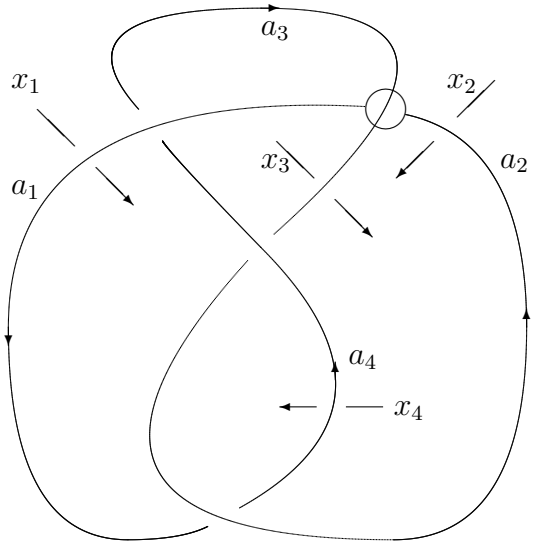
Let f be the compostion

$$Q(X, K) \xrightarrow{\epsilon} \pi_1(X - K) \to H_1(X - K),$$

and let $\overline{Q} = \overline{Q}(X, K) = f^{-1}(\text{generator})$. Then $\overline{Q}$ consists of the nooses linking once with K. $\overline{Q}$ is an invariant of the knot type of K; if $(X, K) \cong (X, K')$, then $\overline{Q}(X, K) \cong \overline{Q}(X, K')$. The boundaries of the nooses in $\overline{Q}$ are called *meridians* of K. $\pi_1(X - k)$ acts on $\overline{Q}(X, K)$ as well as $Q(X, K)$. Call $\overline{Q}$ the *knot quandle* of the knot (X, K).

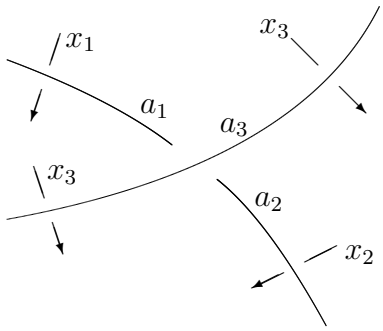
4.6 A presentation of the knot quandle

Figure 4.6: The figure-8 knot



Let (X, K) be a tame knot, such as the figure-8 knot shown in figure 4.6. Recall Wirtinger's presentation for the knot group.

Figure 4.7: A knot crossing



Project the knot onto a suitably chosen plane so that the image contains no triple points and only finitely many, n, double points. Such a projection is called a *regular projection.* . The n "underpoints" (one for each double point) divide the knot into n arcs, an arc going from one underpass, over whatever overpasses there may be, to another underpass. Label the arcs $a_1, a_2, \ldots, a_n$, placing the labels each to the right of the knot (using the orientation of (X, K)). For each arc a_i pass a loop x_i in $X - K$ under the arc

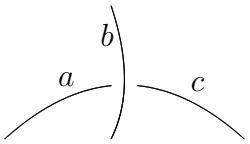
a_i from right to left. These loops generate the knot group. Each underpass yields one relation among the loops. For instance, the circled intersection of the knot in figure 4.6, blown up in figure 4.7, yields the relation $x_3^{-1}x_1x_3 = x_2$. Together these n generators and n relations give a presentation of the knot. For the figure-8 knot we have the presentation

$$G = (x_1, x_2, x_3, x_4 : x_3^{-1}x_1x_3 = x_2, x_4x_2x_4^{-1} = x_3, x_1^{-1}x_3x_1 = x_4, x_2x_4x_2^{-1} = x_1).$$

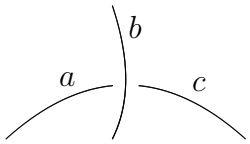
Since each relation states that one generator is a conjugate of another, we may give a presentation of a quandle just by using quandle notation. For the figure-8 knot we then have

$$Q = (x_1, x_2, x_3, x_4 : x_1 \triangleright x_3 = x_2, x_2 \triangleright^{-1} x_4 = x_3, x_3 \triangleright x_1 = x_4, x_4 \triangleright^{-1} x_2 = x_1).$$

By construction, $\operatorname{Adconj} Q = G$. We may arrive at the same presentation more simply. Take a regular projection of the knot. Label the arcs putting the labels always on the one side of the knot. For each intersection derive a relation on the arcs, as



gives $a \triangleright b = c$, while



gives $a \triangleright^{-1} b = c$.

The n relations on the n generators give a presentation of the quandle.

In section 4.7 we will give a direct combinatorial demonstration that this quandle is an invariant of the knot (that is, it does not depend on the choice of regular projection). In 4.8 we show that this quandle is isomorphic to the knot quandle defined in 4.5. In 4.9 we represent the knot quandle in terms of the knot group and show that it is a complete knot invariant. That is, if $Q(K) \cong Q(K')$, then K is equivalent to K'.

4.7 The invariance of the knot quandle

In this section we directly demonstrate the invariance of the quandle of a tame knot given by generators and relations as described in the previous section. There are three basic deformations of regular projections of knots which do not change the knot type. The deformation Ω_1 removes or adds a kink, Ω_2 slides one arc under another, and Ω_3 slides an arc under an intersection.

These three deformations account for the equivalences among tame knots in the following sense. If two tame knots are equivalent, then for any regular projections of the two knots, there is a sequence of basic deformations transforming one projection into the other. A detailed proof of this fact is proved by Alexander and Briggs [1]. See also Reidemeister [11]. In order to show the invariance of the knot quandle it suffices to show its invariance under these basic deformations.

For the deformation Ω_1, we have two cases depending on which side of the arc is labelled. Figure 4.9 indicates that the knot quandle is invariant under Ω_1 since in a quandle, the identities $x \triangleright x = x$ and $x \triangleright^{-1} x = x$ are satisfied.

Figure 4.8: Basic knot deformations

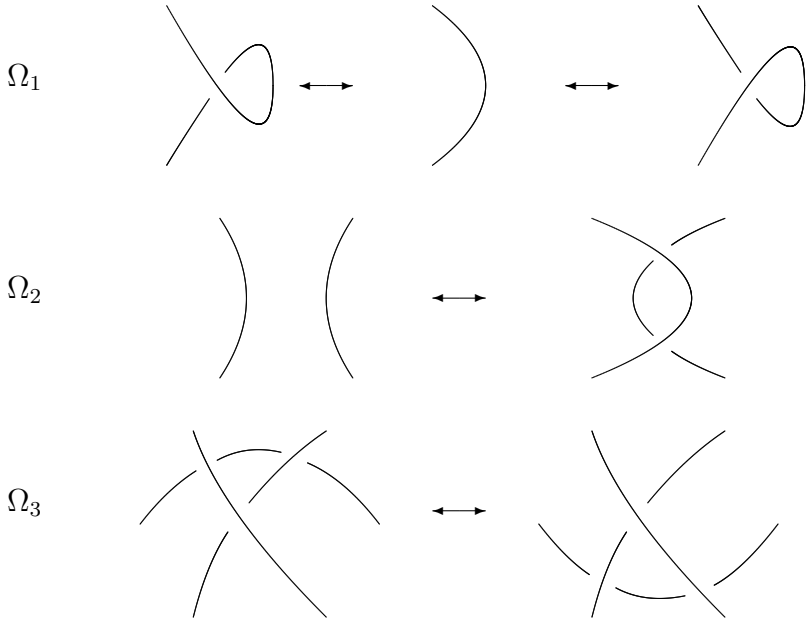


Figure 4.9: Invariance under Ω_1

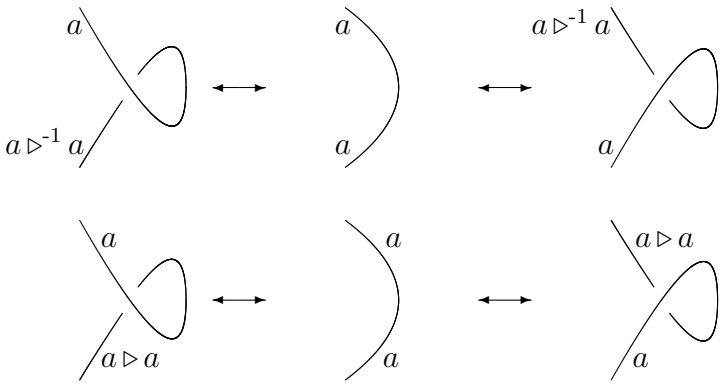
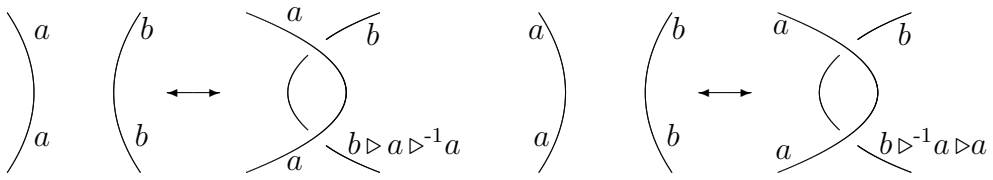
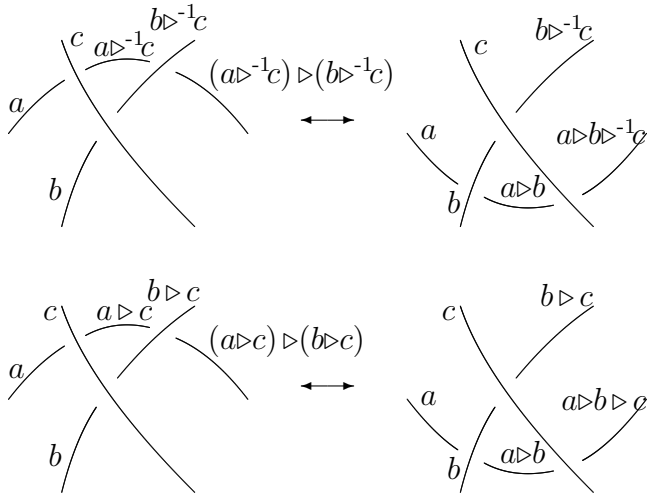


Figure 4.10: Invariance under Ω_2



Deformation Ω_2 requires that $x \triangleright y \triangleright^{-1} y = x$ and $x \triangleright^{-1} y \triangleright y = x$ as shown in figure 4.10.

Figure 4.11: Invariance under Ω_3



The deformation Ω_3 gives four requirements depending again on the labeling. Figure 4.11 illustrates two of these requirements.

The requirements for the invariance of the knot quandle under the basic deformations are all satisfied. Thus, the quandle is an invariant of the knot type.

4.8 A presentation of the knot quandle (continued)

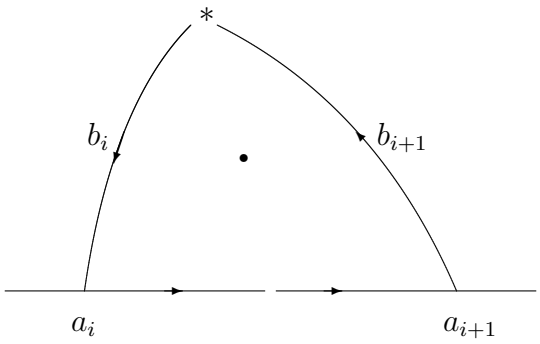
Proposition. Let K be a tame knot and Q be the quandle presented in terms of a regular projection as described in section 4.6. Then Q is isomorphic to the knot quandle $\overline{Q}$ defined in section 4.5.

Proof. Assume that the projection p of the knot to the plane is projection from the basepoint $*$. Label the arcs in order $a_1, a_2, \ldots, a_n$. For $i = 1, \ldots, n$, let b_i be a path down from $*$ to the center of the arc a_i. Let γ_i be the loop which travels from $*$ down b_i, along a_i and a_{i+1}, then up b_{i+1} to $*$ as illustrated in figure 4.12.
Let U_i be a small toroidal neighborhood of γ_i. Then $U_{i-1} \cap U_i$ is a neighborhood of b_i. Let V be $X - K$. Then $X = V \cup U_1 \cup \cdots \cup U_n$. In order to construct $\overline{Q}$, we need to know only the quandles of $(U_i, U_i \cap K)$, $(U_i \cap U_{i+1}, U_i \cap U_{i+1} \cap K)$, $(V, \emptyset)$, $(U_i \cap V, \emptyset)$, and $(U_i \cap U_{i+1} \cap V, \emptyset)$.

Let ν_i be a noose in $U_{i-1} \cap U_i$ linking once about a_i. Then $\pi_1(U_{i-1} \cap U_i - K) = (x_i)$ is the free group on one element $x_i = \epsilon(\nu_i)$. Thus

$$AQ(U_{i-1} \cap U_i, U_{i-1} \cap U_i \cap K) = (\mathrm{Conj}(x_i), (x_i)).$$

Figure 4.12: The loop γ_i



Restricting to the nooses linking once with K, we have

$$\overline{AQ}(U_{i-1} \cap U_i, U_{i-1} \cap U_i \cap K) = (\{x_i\}, (x_i)).$$

Let $G = \pi_1(X - K)$ and $G_i = \pi_1(U_i - K)$. Then

$$\begin{aligned} AQ(U_i, U_i \cap K) &= (\mathrm{Conj}(x_i) \otimes_{(x_i)} G_i, G_i), \text{ and} \\ \overline{AQ}(U_i, U_i \cap K) &= (\{x_i\} \otimes_{(x_i)} G_i, G_i). \end{aligned}$$

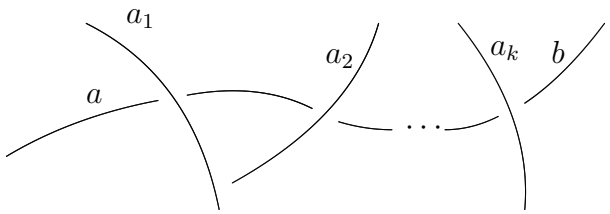
In order to find $\overline{AQ}(X, K)$, we may first tensor the various $\overline{AQ}$ with $G = \pi_1(X - K)$. According to the theorem of section 2.10 and the Seifert-Van Kampen theorem, upon taking the colimit of the various $\overline{AQ} \otimes G$, we will have $\overline{AQ}(X, K)$.

Both $\overline{AQ}(U_{i-1} \cap U_i, U_{i-1} \cap U_i \cap K)$ and $\overline{AQ}(U_i, U_i \cap K)$ become $(\{x_i\} \otimes_{(x_i)} G, G)$ when tensored with G. Thus, $\overline{Q}$ is generated by the $x_1, \ldots, x_n$ modulo the relations induced by tensoring with G. These relations are determined by the action of the generators of G on $\overline{Q}$ and the relations among the generators of G. It is exactly these relations which were used in the definition of Q in section 4.6. Thus, $\overline{Q} \cong Q$. □

We have already noted and used the fact that $\mathrm{Adconj}\, Q$ is the knot group G. As Q is isomorphic to the knot quandle $\overline{Q}$, we have $\mathrm{Adconj}\, \overline{Q} \cong G$. In particular, $\epsilon(\overline{Q})$ generates G.

Corollary. Let K be a tame knot, G its knot group, and Q its knot quandle. Then $Q \times G \to Q$ is a transitive group action.

Proof. In order to show G acts transitively on Q it suffices to show that for generators a, b of Q there is an x in G such that $ax = b$. But by passing under sufficiently many arcs of the regular projection, a becomes b, as suggested in the drawing



Hence, $b = a\epsilon(a_1)^{\pm 1} \cdots \epsilon(a_k)^{\pm 1}$. □

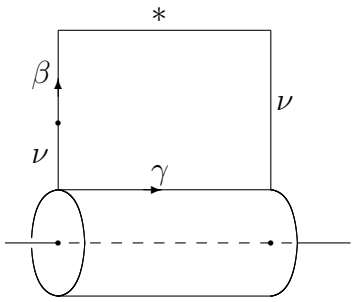
The theorems in sectons 4.5 through 4.8 hold not only for knots, but also for links when careful attention is paid to the orientation of the components of the links. An exception is the preceding corollary which holds only for knots. The quandle of a link is algebraically connected if and only if the link is a knot.

4.9 A representation of the knot quandle

Recall that a *meridian* about a knot K is a loop in the complement of K that links once with K and bounds a disk intersecting K at one point. Equivalently, a meridian is a boundary of a noose in the knot quandle. Let U be a *regular neighborhood* of K in X, that is, U is the image of $S^1 \times$ (disk) embedded in X with $K = \text{image}(S^1 \times \{0\})$. The boundary ∂U of U is a torus. Connect U to the basepoint $*$ by a path γ in $X - U$. Then the inclusion $U \cup \gamma \subseteq X - K$ induces a homomorphism from $\pi_1(U \cup \gamma) \cong \mathbf{Z} \oplus \mathbf{Z}$ to $G = \pi_1(X - K)$. This is a monomorphism unless K is a trivial knot. The image of this map is called a *peripheral subgroup* of the knot group G. Each peripheral subgroup P contains exactly one meridian. Another distinguished element of P is the *longitude* l. l is a generator of the subgroup of P consisting of loops which are not linked with K.

Proposition. Let K be a tame knot with group G and quandle Q. Let $\nu \in Q$ and $G_\nu = \{x \in G \,|\, \nu x = \nu\}$. Then G_ν is a peripheral subgroup of G.

Proof. Let U be a regular neighborhood of K containing the disk of the noose ν. Connect U to $*$ by Rope ν. Then the loops in $U \cup \text{Rope}\,\nu$ form a peripheral subgroup P of G. We show $P = G_\nu$. Without loss of generality we may assume $*$ lies on U and $\text{Rope}\,\nu = \{*\}$. Let $U = f(S^1 \times \text{disk})$, $U = f(S^1 \times S^1)$, $* = f(1,1)$. We may also assume $\epsilon(\nu) = f(S^1 \times 1)$. P is generated by the meridian $\epsilon(\nu)$ and the longitude $\alpha = f(1 \times S^1)$. $\nu\alpha$ is homotopic to ν (slide the disk of $\nu\alpha$ around the solid torus U by one revolution). Hence, $P \subseteq G_\nu$. Let β be a loop in $X - K$ such that $\nu\beta \sim \nu$. The homotopy H of $\nu\beta$ to ν may be chosen so that the disk portion of the homotopy lies inside U.



Let γ be the loop from $\nu(1)$ to $\nu(1)$ given by $\gamma(t) = H(1,t)$. Then $\beta \sim (\text{Rope}\,\nu)\gamma(\text{Rope}\,\nu)^{-1}$ which lies in P. Thus, $G_\nu = P$. □

Corollary 1. Let K be a knot with knot group G and knot quandle Q. Let P be a peripheral subgroup of G containing the meridian m. Then $(P\backslash G; m)$, as described in section 2.4, is isomorphic to the knot quandle.

Proof. Follows from the corollary of secton 4.8. □

Thus, the knot quandle contains the same information as the triple (G, P, m) consisting of the knot group G, a peripheral subgroup P, and a meridian m in P.

Neuwirth [10] remarks that if two tame knot groups are isomorphic by a map which sends a meridian to a meridian and the group system (the conjugate peripheral subgroups) of one onto the group system of the other, then the (unoriented) knots are equivalent. Conway and Gordon [6] use a slightly stronger principle to construct a group that classifies oriented knots. If two tame knot groups are isomorphic by a map which sends a meridian and corresponding longitude of one onto those of the other, then the oriented knots are equivalent. A proof of this principle may be found in Waldhausen [19].

Corollary 2. If the knot quandles of two tame knots are isomorphic, then the (unoriented) knots are equivalent. □

Other algebraic characterizations of knots have been described by Simon [14] and Whitten [20]. The constructions given by Conway and Gordon, Simon, and Whitten are not functorial, unlike the knot quandle.

4.10 The Alexander invariant of a knot

Let K be a knot in $X = S^3$ and $Y = X - K$. Let $\tilde{Y}$ be the infinite cyclic cover of Y. Then $\pi_1(\tilde{Y}) = G' = [G, G]$ where $G = \pi_1(Y)$ is the knot group. Also $G/G' = \mathbf{Z}$ and $H_1(\tilde{Y}) \cong G'/G''$. If x in G is such that the map $G \to G/G' \cong \mathbf{Z}$ sends x to 1, then conjugation by x gives an automorphism t of $H_1(\tilde{Y})$, and t is independent of x. Thus, $H_1(\tilde{Y})$ is not only an Abelian group, but also a module over the ring $\Lambda = \mathbf{Z}[t, t^{-1}]$. This Λ-module is called the *Alexander invariant* A of the knot K. We will show in this section that A carries the same information as the Abelian knot quandle.

The usual presentation of the Alexander invariant is by means of a matrix. Take a Seifert surface for the knot K and let n be the genus of the surface. Let $a_1, \ldots, a_n$ be generating cycles for the homology of the surface. and let v_{ij} be the linking number of a_i with a_j. The matrix (v_{ij}) is called a *Seifert matrix* of the knot. $P = (v_{ij} - tv_{ji})$ is an *Alexander matrix* of the knot. The entries of P lie in Λ. Then the Alexander invariant is the cokernel

$$\Lambda^n \xrightarrow{P} \Lambda^n \to A \to 0.$$

The determinant of P is called the *Alexander polynomial* $\Delta(t)$ of the knot. $\Delta(t)$ is defined only up to a unit of Λ. One important property of $\Delta(t)$ is that $|\Delta(1)| = 1$. A more direct definition of $\Delta(t)$ is that it is a generator of the annihilator ideal of A.

We first show that A may be constructed from the Abelian knot quandle $\operatorname{Ab} Q$. As noted in section 4.8, $\operatorname{Adconj} Q = G$. Hence $\operatorname{Adconj} \operatorname{Ab} Q = G/N$ where N is the normal subgroup of G generated by elements of the form

$$ab^{-1}ca^{-1}bc^{-1}, \text{ with } a, b, c \in \epsilon(Q).$$

Lemma 1. $N = G''$.

Proof. Part 1. $N \subseteq G''$. Let $a, b, c \in \epsilon(Q)$. Since Q is algebraically connected, there exist x, y in G such that $b = x^{-1}ax$ and $c = y^{-1}ay$. Then

$$ab^{-1}ca^{-1}bc^{-1} = (ax^{-1}a^{-1}x)(y^{-1}aya^{-1})(x^{-1}axy^{-1}a^{-1}y).$$

Both $ax^{-1}a^{-1}x$ and $y^{-1}aya^{-1}$ lie in G', so, modulo G'',

$$ab^{-1}ca^{-1}bc^{-1} \equiv (y^{-1}aya^{-1})(ax^{-1}a^{-1}x)(x^{-1}axy^{-1}a^{-1}y) = 1.$$

Hence, $ab^{-1}ca^{-1}bc^{-1} \in G''$. Thus, $N \subseteq G''$.

Part 2. $G'' \subseteq N$. Let $a, b \in G'$. a is of the form $a_1^{e_1} \cdots a_n^{e_n}$ with $a_i \in \epsilon(Q)$ and $\sum e_i = 0$. Note that if $x, y \in \epsilon(Q)$, then $xy^{-1} = yz^{-1}$ where $z = x \triangleright^{-1} y \in \epsilon(Q)$. Hence, a may be written as

$$a = a_1 a_2^{-1} a_3 a_4^{-1} \cdots a_{n-1} a_n^{-1}$$

with each a_i in $\epsilon(Q)$. Similarly,

$$b = b_1 b_2^{-1} b_3 b_4^{-1} \cdots b_{m-1} b_m^{-1}$$

with each b_i in $\epsilon(Q)$. Therefore, modulo N,

$$\begin{aligned} ab &= a_1 a_2^{-1} a_3 a_4^{-1} \cdots a_{n-1} a_n^{-1} b_1 b_2^{-1} b_3 b_4^{-1} \cdots b_{m-1} b_m^{-1} \\ &\equiv b_1 b_2^{-1} b_3 b_4^{-1} \cdots b_{m-1} b_m^{-1} a_1 a_2^{-1} a_3 a_4^{-1} \cdots a_{n-1} a_n^{-1} = ba. \end{aligned}$$

Hence, $[a, b] \in N$. Thus, $G'' = N$. □

Therefore, $\operatorname{Adconj} \operatorname{Ab} Q = G/G''$ is constructable from AQ, and, whence, its commutator G'/G'' is also. The symmetry at a point a_0 in $\operatorname{Ab} Q$ is an automorphism of $\operatorname{Ab} Q$ which induces conjugation by $\epsilon(a_0)$ on G'/G'', the required Λ-structure on $H_1(\tilde{Y}) \cong G'/G''$.

Next, we show that the Alexander invariant A of a knot determines $\operatorname{Ab} Q$.

Theorem. Let A be given the quandle structure $x \triangleright y = t(x-y)+y$, $x \triangleright^{-1} y = t^{-1}(x-y)+y$. Then with this structure A is isomorphic to $\operatorname{Ab} Q$.

Proof. Choose $a_0 \in \operatorname{Ab} Q$. Let P be the peripheral subgroup for a_0. By corollary 1 in section 4.9, $\varphi : P\backslash G \cong Q$, $\varphi(Px) = a_0 x$, φ is a quandle isomorphism where $\triangleright$ on $P\backslash G$ is given by $Px \triangleright Py = Pxy^{-1}\epsilon(a_0)y$. Now $\operatorname{Ab} Q$ is Q/N where N is defined above and shown in the lemma to be G''. Hence

$$(P/P \cap G'')\backslash(G/G'') = (P/P \cap N)\backslash(G/N) \cong \operatorname{Ab} Q.$$

Now, the map $G \to Q$ sending x to $a_0 x$ is still surjective when restricted to G', so

$$(P \cap G'/P \cap G'')\backslash(G'/G'') \cong \operatorname{Ab} Q.$$

Let l be a longitude in P. Then $P \cap G' = (l)$.

Lemma 2. $l \in G''$.

Proof of lemma 2. Let $m = \epsilon(a_o)$. As $l \in P$, $m^{-1}lm = l$. In the notation of A, $l \in A$ and $tl = l$. Hence, $(t-1)l = 0$. A is presented as

$$\Lambda^n \xrightarrow{p} \Lambda^n \to A \to 0.$$

As an element of Λ^n, $(t-1)l = Pa$, some $a \in \lambda^n$. Evaluate at $t = 1$ to get $0 = P(1) \cdot a(1)$. Now $P(1)$ is invertible as a matrix in $M_n(\mathbf{Z})$ since $\det P(1) = \Delta(1) = \pm 1$. Hence, $0 = a(1)$, that is, $(t-1)$ divides a, and $a = (t-1)b$. So $(t-1) = P \cdot (t-1)b$. Therefore, $l = Pb \in$ image P. So $l = 0$ in A, $l \in G''$. □

Proof of theorem continued. So $P \cap G'' = (l) = P \cap G'$. Therefore, $G'/G'' = \operatorname{Ab} Q$. Examine the quandle structure on G'/G''. In $P\backslash G$, $\triangleright$ is

$$Px \triangleright Py = Pxy^{-1}my = Pmxy^{-1}my = P(x \triangleright m)(y \triangleright m)^{-1}y.$$

So in G'/G'', $\triangleright$ is

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

which in the notation of A becomes

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

□

The Alexander invariant is not enough to distinguish all knots from the trivial knot. For instance, the Alexander invariant of any doubled knot is trivial.

4.11 The cyclic invariants of a knot

In this section let K be a knot in $X = S^3$ and Y the complement of the knot. Let n be a positive integer. Let $\tilde{Y}_n$ be the n-fold cyclic cover of Y and Σ_n be the n-fold branched cyclic cover. Then $H_1(\tilde{Y}_n) \cong H_1(\Sigma_n) \oplus \mathbf{Z}$. $H_1(\Sigma_n)$ is a finite Abelian group. The *n-th torsion numbers* of K are the subscripts in the canonical decomposition

$$H_1(\Sigma_n) \cong \mathbf{Z}_{k_1} \oplus \cdots \oplus \mathbf{Z}_{k_r}, \quad k_i \,|\, k_{i+1},\ i = 1, \ldots, r-1.$$

The order of $H_1(\Sigma_2)$ is called the *determinant* of K, $\det K$. Let $P(t) = (v_{ij} - tv_{ji})$ be an Alexander matrix for K. Then $P(-1) = (v_{ij} + v_{ji})$ presents $H_1(\Sigma_2)$ as a module over $\mathbf{Z}$. The determinant of $P(-1)$ gives $\det K$; $\det K = |\det P(-1)|$. Hence, the Alexander polynomial $\Delta(t)$ evaluated at -1 gives $\det K$; $\det K = |\Delta(-1)|$.

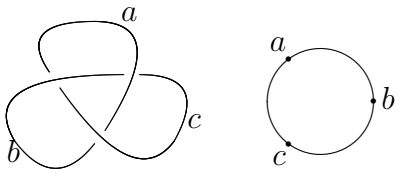
$H_1(\Sigma_n)$ has an automorphism induced from conjugation by an x in $G = \pi_1(Y)$ for which $G \to \mathbf{Z}$ sends x to 1. That is, $H_1(\Sigma_n)$ is a module over $\Lambda_n = \mathbf{Z}[t]/(t^n - 1)$. Then $H_1(\Sigma_n)$ has a quandle structure given by the formula $x \triangleright y = tx + (1-t)y$. With this structure $H_1(\Sigma_n)$ is an n-quandle, in fact, it is the largest quotient of the Alexander invariant which is an n quandle. For $n = 2$, $H_1(\Sigma_n)$ is the involutory Abelian knot quandle.

4.12 The involutory knot quandle

Let K be a knot with quandle Q. The involutory knot quandle Q_2 results from imposing the identity $(x \triangleright y) \triangleright y = x$ on Q.

Example 1. The trefoil knot 3_1.

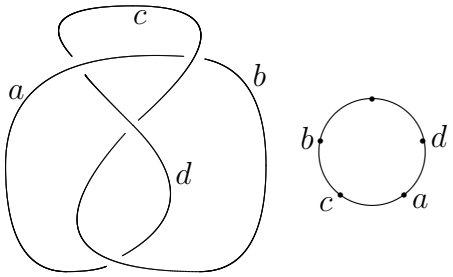
Figure 4.13: The trefoil knot 3_1



$Q = (a, b, c : a \triangleright b = c, b \triangleright c = a, c \triangleright a = b)$. Q_2 has the same presentation as Q as long as the relations $(x \triangleright y) \triangleright y = x$ are understood. Viewed with geodesics (see section 3.1), Q_2 has three points shown to the right.

Example 2. The figure-8 knot 4_1.
$Q = (a, b, c, d : a \triangleright c = b, b \triangleright^{-1} d = c, c \triangleright a = d, d \triangleright^{-1} b = a)$.
$Q_2 = (a, b, c, d : a \triangleright c = b, b \triangleright d = c, c \triangleright a = d, d \triangleright b = a)$.
Very little work shows $|Q_2| = 5$.

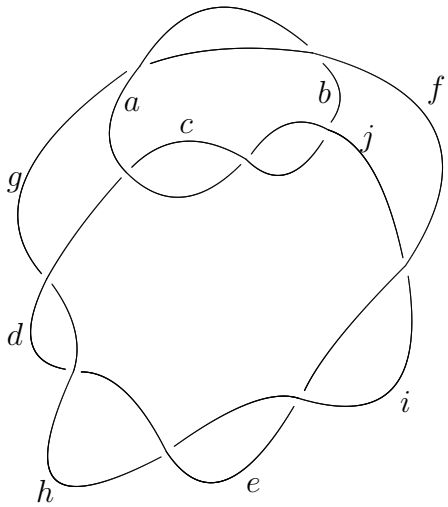
Figure 4.14: The figure-8 knot 4_1



For these two examples Q_2 is Abelian as well as involutory. The next example has a nonAbelian Q_2.

Example 3. The knot 10_{124}.

Figure 4.15: The knot 10_{124}



The Alexander polynomial of 10_{124} is $\Delta(t) = t^{-4} - t^{-3} + t^{-1} - 1 + t - t^3 + t^4$, so the determinant of 10_{124} is 1. Thus, $\mathrm{Ab}\, Q_2$ is trivial. A few computations will show that Q_2 may be faithfully represented as the 30 edges of a dodecahedron projected onto a sphere. Figure 4.16 displays these points in stereographic projection in the plane.

Proposition. The link quandle is not an invariant of the complement of the link.

Proof. We examine the involutory link quandles of the links K_1 and K_2 displayed in figure 4.17. As described on page 49 in [13], the complements of K_1 and K_2 are

Figure 4.16: $Q_2(10_{124})$

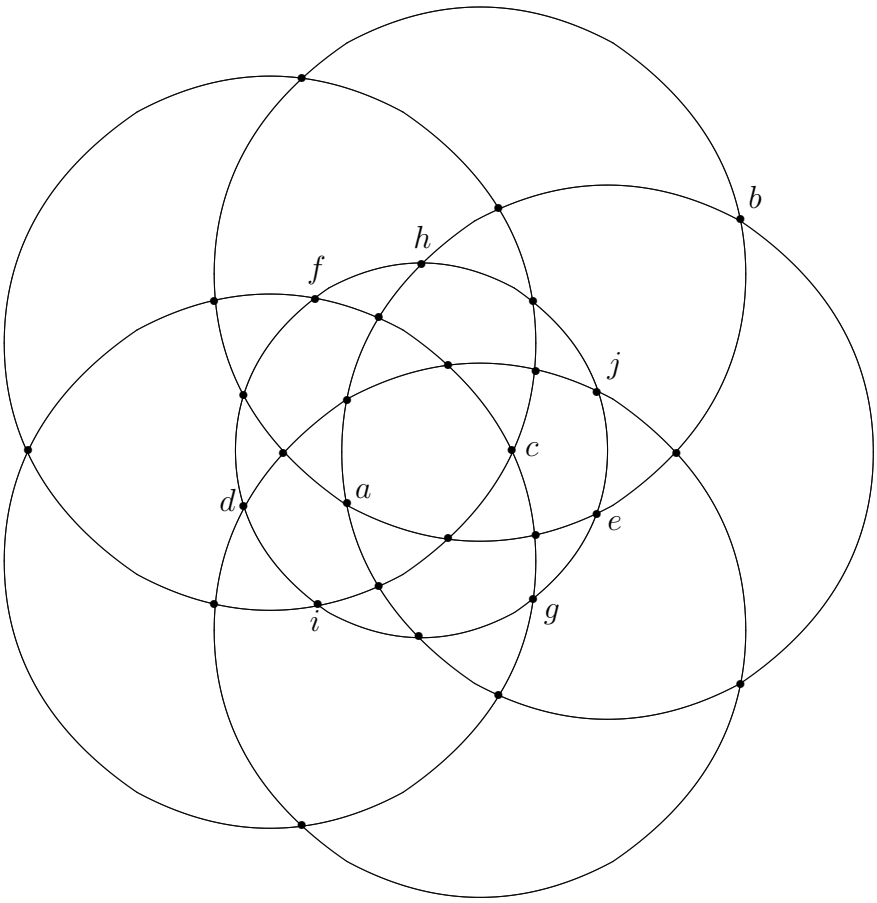
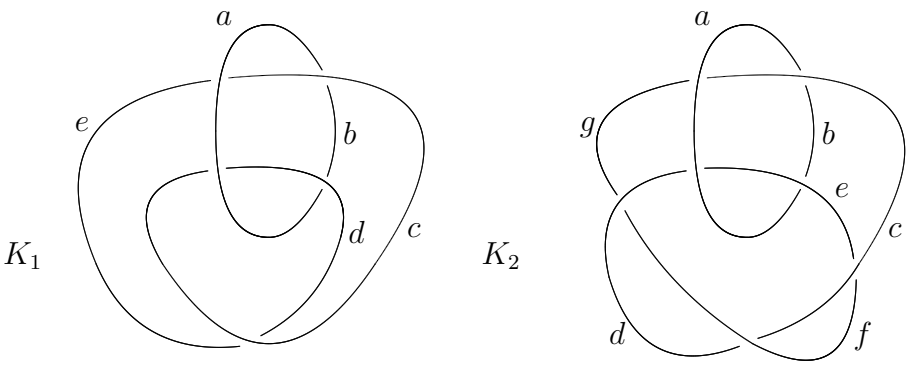


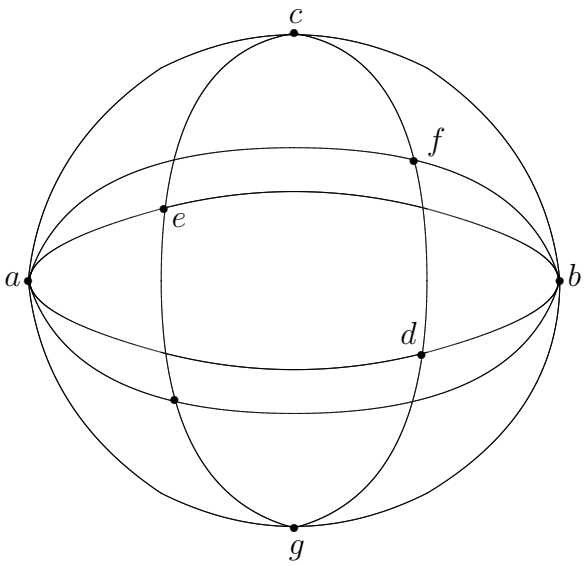
Figure 4.17: Two links with homeomorphic complements but different quandles



homeomorphic.

$$\begin{aligned} Q_2(K_1) &= (a,b,c,d,e : a \triangleright c = b, b \triangleright d = a, c \triangleright a = d, d \triangleright c = e, e \triangleright a = c) \\ &= \text{Core}\, \mathbf{Z}_4. \\ Q_2(K_2) &= (a,\ldots,g : a \triangleright c = b, b \triangleright e = a, c \triangleright f = d, d \triangleright a = e, e \triangleright c = f, f \triangleright d = g, g \triangleright a = c). \end{aligned}$$

$Q_2(K_2)$ has order 8. It may be represented with geodesics as



Since the involutory quandles of K_1 and K_2 are distinct, so are their quandles. □

Bibliography

[1] Alexander, J. W., and G. B. Briggs, On types of knotted curves. *Ann. of Math.* 28 (1926), 562–566.

[2] Blaschke, W., and G. Bol, *Geometrie der Gewebe*. Springer, Berlin, 1938.

[3] Bruck, R., H., *A Survey of Binary Systems*. Springer, Berlin, 1958.

[4] Burn, R. P., Finite Bol loops. *Math. Proc. Cambridge Phil. Soc.* 84 (1978), 377–385.

[5] Burstin, C., and W. Mayer, Distributive Gruppen, *J. Reine Angew. Math.* 160 (1929), 111–130.

[6] Conway, J. H., and C. McA. Gordon, A group to classify knots, *Bull. London Math. Soc.* 7 (1975), 84–88.

[7] Loos, O., Spiegelungsraüme und homogene symmetrische Raume, *Math. Z.* 99 (1967), 141–170.

[8] Loos, O., *Symmetric Spaces*. Benjamin, New York, 1969.

[9] Moufang, R., Zur Struktur von Alternativekörpern, *Math. Ann.* 110 (1935), 416–430.

[10] Neuworth, L. P., *Knot Groups*. Princeton Univ. Press, 1965.

[11] Reidemeister, K., *Knotentheorie*. Chelsea, New York, 1949 (reprint).

[12] Robinson, D. A., Bol loops, *Trans. Amer. Math. Soc.* 123 (1966), 341–354.

[13] Rolfsen, D., *Knots and Links*. Publish or Perish, Berkeley, 1976.

[14] Simon, J., An algebraic classification of knots in S^3, *Ann. of Math.* 93 (1973), 1–13.

[15] Soublin, J.-P., Étude algebrique de la notion de moyenne, *J. Math. Pures Appl.* (9) 50 (1971), 53–264.

[16] Takasaki, M, Abstractions of symmetric functions, *Tôhoku Math. J.* 49 (1943), 143–207, [Japanese]. *Math. Reviews* 9, p. 8.

[17] Thomsen, G., Un teorema topologico sulle schiere de curve e una caratterizzazione geometrica delle superficie isotermo-asintotiche, *Boll. Union Mat. Ital. Bologna* 6 (1927), 80–85.

[18] Thomsen, G., *Grundlagen der Elentargeometrie in gruppen algebraischer Behandlung*, Hamburger Math. Einzelschr., no. 15, Teubner, Leipzig, 1933.

[19] Waldhausen, F., On irreducible 3-manifolds which are sufficiently large, *Ann. of Math.* 87 (1968), 56–88.

[20] Whitten, W., Characterization of knots and links, *Bull. Amer. Math. Soc.* 80 (1974), 1265–1270.

Index