Journal of Knot Theory and Its Ramifications
Vol. 20, No. 3 (2011) 463–468

DOI: 10.1142/S0218216511008863

ON THE STRUCTURE AND AUTOMORPHISM GROUP OF FINITE ALEXANDER QUANDLES

AMIEL FERMAN*,†, TAHL NOWIK and MINA TEICHER
Department of Mathematics, Bar-Ilan University,
Ramat-Gan 52900, Israel
**amielferman3@gmail.com*

Accepted 20 October 2009

ABSTRACT

We prove that an Alexander quandle of prime order is generated by any pair of distinct elements. Furthermore, we prove for such a quandle that any ordered pair of distinct elements can be sent to any other such pair by an automorphism of the quandle.

Keywords: Alexander quandles; finite quandles.

Mathematics Subject Classification 2010: 57M27

1. Introduction

Quandles were first introduced by Joyce [5, 6] and independently by Matveev (under the name *distributive groupoids* [8]) as algebraic invariants of classical knots and links. For an introduction to the use of quandles as computable invariants of framed links in 3-manifolds see [3]. Another important application of quandles was given by Yetter in [11] as a means to study braid monodromies of algebraic surfaces. The quandle binary operation (see Definition 2.1) may be thought of as an abstraction of the conjugation operation in a group.

In this article we study a particular kind of quandle, called an Alexander quandle (see Definition 3.1). It is known that any finite connected quandle with a prime number of elements or a square of a prime number of elements is isomorphic to an Alexander quandle (see [2] and [4] respectively and see Definition 2.4 for the notion of a connected quandle). Furthermore, many quandles with a small number of elements are known to be isomorphic to Alexander quandles (see, for example [10]). These facts and the fact that Alexander quandles are relatively easy to study, due to the arithmetic flavor of their definition, serve as a motivation for their study.

†This article was submitted as part of the first author's PhD Thesis at Bar-Ilan University, Ramat-Gan Israel, written under the supervision of Mina Teicher and Tahl Nowik.

Finite Alexander quandles were studied in [9] where an arithmetic condition was given as a means to determine whether two such quandles are isomorphic.

In this article, we prove that an Alexander quandle of prime order is generated by any pair of distinct elements. Furthermore, we prove for such a quandle that any ordered pair of distinct elements can be sent to any other such pair by an automorphism of the quandle.

Our paper is organized as follows:

In Sec. 2, we give a short introduction to quandles which is necessary for the statements of our results. In Sec. 3, we prove our main results as follows: In Sec. 3.1, we prove a few general formulae regarding finite Alexander quandles (not necessarily of prime order). In Sec. 3.2, we focus on finite Alexander quandles of prime order, and prove our two main results stated above.

2. Basic Definitions and Examples of Quandles

We start with the definition of a quandle.

Definition 2.1 (Quandle). A *quandle* is a set X together with a binary operation $(a, b) \mapsto a^b$ which satisfies the following three properties.

(1) For any $a, b \in X$ there exists a unique $c \in X$ such that $a = c^b$.
(2) For any $a, b, c \in X$, $(a^b)^c = (a^c)^{b^c}$.
(3) For any $a \in X$, $a^a = a$.

Quandle homomorphisms and automorphisms are defined in the natural way. Two important examples of quandles are the following.

Example 2.2. The *trivial quandle* consists of a set X with quandle operation $x^y = x$ for any $x, y \in X$.

Example 2.3. Any group G can be considered as a quandle by letting $a^b \stackrel{\text{def}}{=} b^{-1}ab$. More generally, a union G' of a family of conjugacy classes in G is a quandle with this operation. Such a quandle is called a *Conjugation quandle* and is denoted by G'_{conj}. Note that if G is abelian then G_{conj} is a trivial quandle.

Let X be a quandle and let $b \in X$. As a consequence of the first and second quandle axioms (see Definition 2.1), the function $\rho_b : x \mapsto x^b$ is an automorphism of X. Let $\text{Aut}(X)$ denote the group of quandle automorphisms of X (acting on the right), and let $F(X)$ denote the free group on X. Then the mapping $X \to \text{Aut}(X)$ given by $b \to \rho_b$ determines a homomorphism $F(X) \to \text{Aut}(X)$, that is, a right action of $F(X)$ on X as automorphisms of X. The action of $w \in F(X)$ on $x \in X$ is denoted x^w.

Definition 2.4. A quandle X is called *connected* if $F(X)$ acts transitively on X.

Lemma 2.5. *Let X be a quandle. Then*

$$(a^b)^w = (a^w)^{b^w} \quad a, b \in X, \quad w \in F(X) \tag{2.1}$$

and

$$a^{b^w} = a^{w^{-1}bw} \quad a, b \in X, \quad w \in F(X). \tag{2.2}$$

Proof. (2.1) is simply a statement of the fact mentioned before Definition 2.4, that each $w \in F(X)$ acts as an automorphism on X. We show (2.1) and (2.2) are equivalent: Let $a, b \in X$ and $w \in F(X)$. If (2.1) holds, then $a^{w^{-1}bw} = ((a^{w^{-1}})^b)^w = ((a^{w^{-1}})^w)^{b^w} = a^{b^w}$. If (2.2) holds then $(a^w)^{b^w} = a^{ww^{-1}bw} = a^{bw} = (a^b)^w$. □

3. Alexander Quandles

Let us first give the definition of an Alexander quandle:

Definition 3.1. Given an abelian group M, and $t \in \mathrm{Aut}_{\mathbb{Z}}(M)$ (where $\mathrm{Aut}_{\mathbb{Z}}$ is used to denote the automorphisms of M as an abelian group), we define a quandle structure on M by the quandle operation $a^b \stackrel{\text{def}}{=} ta + (1-t)b$. This is called an Alexander quandle.

Remark 3.2. Note that if $t = \mathrm{Id}$ then M is a trivial quandle. On the other hand, if $(\mathrm{Id} - t) \in \mathrm{Aut}_{\mathbb{Z}}(M)$, then the quandle homomorphism $b \mapsto \rho_b$ (see paragraph preceding Definition 2.4) is injective, and M is connected. (By (2.2) in Lemma 2.5, this is indeed a quandle homomorphism $X \to \mathrm{Aut}(X)_{\mathrm{conj}}$.)

3.1. *Finite Alexander quandles*

The following is clear by induction on k.

Lemma 3.3. *Let Q be a finite Alexander quandle. For any $k \in \mathbb{Z}$ and any $a, b \in Q$:*

$$a^{b^k} = t^k a + (1 - t^k)b. \tag{3.1}$$

Furthermore, if m is the order of $t \in \mathrm{Aut}(Q)$ then for any $k \in \mathbb{Z}$:

$$a^{b^k} = a^{b^{k+m}}. \tag{3.2}$$

Lemma 3.4. *Let M be an Alexander quandle. Then for any $a, b \in M$, $k_i \in \mathbb{Z}$ and natural n the following holds.*

For n odd:

$$a^{b^{k_1}a^{k_2}\ldots b^{k_{n-2}}a^{k_{n-1}}b^{k_n}} = \left(\sum_{i=1}^{n}(-1)^{i+1}t^{k_i+\cdots+k_n}\right)(a-b) + b. \tag{3.3}$$

For n even:

$$a^{b^{k_1}a^{k_2}\cdots b^{k_{n-1}}a^{k_n}} = \left(\sum_{i=1}^{n}(-1)^{i+1}t^{k_i+\cdots+k_n}\right)(a-b)+a. \tag{3.4}$$

Proof. The case $n = 1$ follows from (3.1) in Lemma 3.3. The rest of the proof follows by combined induction for (3.3) and (3.4). □

3.2. *Alexander quandles of prime order*

In this section, we prove our two main results regarding Alexander quandles of prime order. We determine that each such quandle is generated by any two elements and we also describe its set of quandle automorphisms.

Let p be a fixed prime number. In what follows we consider $\mathbb{Z}_p$ as an Alexander quandle with $t \in \mathrm{Aut}_{\mathbb{Z}}(\mathbb{Z}_p)$ as defined in Definition 3.1. Note that any group automorphism of $\mathbb{Z}_p$ is a multiplication by an element in $\mathbb{Z}_p^*$ and so we will also consider t as an element in $\mathbb{Z}_p^*$.

The following theorems apply to any connected finite quandle of prime order since it was proved in [2] that any connected finite quandle of prime order is isomorphic to an Alexander quandle with $t \neq 1$.

Theorem 3.5. *Let $p > 2$ be some prime number and consider $\mathbb{Z}_p$ as an Alexander quandle Q with $t \in \mathbb{Z}_p^*$, $t \neq 1$. Then any two elements $a, b \in Q$, $a \neq b$, generate Q. More precisely we have that for any $c \in Q$ there exists an even $n \in \mathbb{N}$ and $k_1, \ldots, k_n \in \mathbb{Z}$ such that*

$$a^{b^{k_1}a^{k_2}\cdots b^{k_{n-1}}a^{k_n}} = c. \tag{3.5}$$

Proof. Let $a, b \in Q$, $a \neq b$. We will prove that for any $c \in Q$ there exists an even $n \in \mathbb{N}$ and $k_1, \ldots, k_n \in \mathbb{Z}$, such that (3.5) holds. According to Lemma 3.4, (3.5) is equivalent to

$$\left(\sum_{i=1}^{n}(-1)^{i+1}t^{k_i+\cdots+k_n}\right)(a-b)+a = c. \tag{3.6}$$

Denote $d = (c-a)(a-b)^{-1}$, then we need $k_1, \ldots, k_n$, for some even n, such that

$$\sum_{i=1}^{n}(-1)^{i+1}t^{k_i+\cdots+k_n} = d. \tag{3.7}$$

Take $m \in \mathbb{N}$ satisfying $m = (1-t)^{-1}d \mod p$, and let $k_i = (-1)^i$ for $i = 1, \ldots, 2m$, then

$$\sum_{i=1}^{2m}(-1)^{i+1}t^{k_i+\cdots+k_{2m}} = \sum_{i=1}^{2m}(-1)^{i+1}t^{(-1)^i+\cdots+(-1)^{2m}} = m - mt = m(1-t) = d. \qquad \square$$

Theorem 3.6. *Let $p > 2$ be some prime number and consider $\mathbb{Z}_p$ as an Alexander quandle Q with $t \in \mathbb{Z}_p^*$, $t \neq 1$. For any $a, b, c, d \in Q$ such that $a \neq b$ and $c \neq d$ there exists a unique quandle automorphism $\alpha \in \mathrm{Aut}(Q)$ such that $\alpha(a) = c$ and $\alpha(b) = d$.*

Proof. Let $r \in Q$, then by (3.5) in Theorem 3.5 there is an $x \in F(\{a, b\})$ such that $r = a^x$. Define $\alpha(r)$ as follows:

$$\alpha(r) = \alpha(a^x) = c^{\beta(x)} \tag{3.8}$$

where $\beta : F(\{a, b\}) \to F(\{c, d\})$ is the group homomorphism defined by $\beta(a) = c$ and $\beta(b) = d$.

To show that α is well defined we need to check that for any $x, y \in F(\{a, b\})$, if $a^x = a^y$ then $c^{\beta(x)} = c^{\beta(y)}$. There are two possible forms for such an element:

$$a^{b^{k_1} a^{k_2} \cdots b^{k_{n-2}} a^{k_{n-1}} b^{k_n}}, \tag{3.9}$$

$$a^{b^{k_1} a^{k_2} \cdots b^{k_{n-1}} a^{k_n}}. \tag{3.10}$$

According to Lemma 3.4, the words in (3.9) and (3.10) are equal, respectively, to

$$\left(\sum_{i=1}^{n} (-1)^{i+1} t^{k_i + \cdots + k_n} \right) (a - b) + b, \tag{3.11}$$

$$\left(\sum_{i=1}^{n} (-1)^{i+1} t^{k_i + \cdots + k_n} \right) (a - b) + a. \tag{3.12}$$

Let us rewrite these expressions as follows:

$$\left(\sum_{i=1}^{n} (-1)^{i+1} t^{k_i + \cdots + k_n} - 1 \right) (a - b) + a, \tag{3.13}$$

$$\left(\sum_{i=1}^{n} (-1)^{i+1} t^{k_i + \cdots + k_n} \right) (a - b) + a. \tag{3.14}$$

Hence the equation $a^x = a^y$ is equivalent to an equation of the form $K(a-b)+a = K'(a-b)+a$, or

$$(K - K')(a - b) = 0, \tag{3.15}$$

where $K, K' \in \mathbb{Z}_p$ are independent of a and b and only depend on the integers $k_1, \ldots, k_n$ appearing in the powers of the expressions in (3.9) and (3.10). But since $a \neq b$ we have that (3.15) is equivalent to $K - K' \equiv 0 (\mathrm{mod}\ p)$ which in turn is equivalent to (recall that $c \neq d$ by assumption) $(K-K')(c-d) = 0$ or $K(c-d)+c = K'(c-d)+c$ which is precisely the equation $c^{\beta(x)} = c^{\beta(y)}$. This concludes the proof that α is well defined.

In the same way we verify that $\alpha(b) = d$ as needed. Namely, note that $b = -1(a-b)+a$, so if $b = a^x$ for $x \in F(\{a, b\})$, then the K' attached to this

presentation must satisfy $K' \equiv -1 \mod p$ so the same holds for the corresponding expression with c, d. But also $d = -1(c-d)+c$, so $\alpha(b) = d$.

By Theorem 3.5 any element of Q can also be written as c^x where $x \in F(\{c,d\})$ and so α is onto. Since Q is finite, α is also one-to-one.

Let us now show that α is a quandle homomorphism. Let $x, y \in F(\{a,b\})$. Then using (3.8) and (2.2) in Lemma 2.5 we have

$$\alpha((a^x)^{a^y}) = \alpha(a^{xy^{-1}ay}) = c^{\beta(x)\beta(y)^{-1}c\beta(y)} = (c^{\beta(x)})^{c^{\beta(y)}} = \alpha(a^x)^{\alpha(a^y)}.$$

We remark that in this expression the length of the exponent may be odd. This is why we considered exponents of both even and odd lengths when showing that α is well defined.

Finally note that α is unique since a, b generate Q (in the sense of (3.5)). □

References

[1] M. Eisermann, Quandle coverings and their Galois correspondence, preprint, arXiv:math.GT/0612459.

[2] P. Etingof, R. Guralnik and A. Soloviev, Indecomposable set-theoretical solutions to the quantum Yang-Baxter equation on a set with prime number of elements, *J. Algebra* **242** (2001) 709–719.

[3] R. Fenn and C. Rourke, Racks and links in codimension two, *J. Knot Theory Ramifications* **1** (1992) 343–406.

[4] M. Grana, Indecomposable racks of order p^2, preprint, arXiv:math.QA/0203157.

[5] D. E. Joyce, An algebraic approach to symmetry with applications to knot theory, PhD thesis, University of Pennsylvania (1979).

[6] D. E. Joyce, A classifying invariant of knots, the knot quandle, *J. Pure Appl. Algebra* **23** (1982) 37–65.

[7] P. Lopes and D. Roseman, On finite racks and quandles, may be found on http://arXiv.org: math.GT/0412487.

[8] S. V. Matveev, Distributive groupoids in knot theory, *Matematicheskii Sbornik* **119**(1) (1982) 78–88 (in Russian; English translation in: *Mathematics of the USSR-Sbornik* **47**(1) (1984) 73–83).

[9] S. Nelson, Classification of finite Alexander quandles, preprint, arXiv.org:math.GT/0202281.

[10] S. Nelson and B. Ho, Matrices and finite quandles, *Homology Homotopy Appl.* **7**(1) (2005) 197–208.

[11] D. Yetter, Quandles and monodromy, *J. Knot Theory Ramifications* **12**(4) (2003) 523–541.