On The Structure and Automorphism Group of Finite Alexander Quandles

Amiel Ferman*, Tahl Nowik, Mina Teicher

Department of Mathematics, Bar-Ilan University
Ramat-Gan, Israel

September 27, 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.

1 Introduction

Quandles were first introduced by D.E. Joyce ([Joy79, Joy82]) and independently by S.V. Matveev (under the name *distributive groupoids* [Mat82]) 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 [FR92]. Another important application of quandles was given by Yetter in [Ye06] as a means to study braid monodromies of algebraic surfaces.

Quandles (see Definition 2.1) can be considered as an abstraction of groups in the sense that the only binary operation is the analog of the conjugation operation in the group.

In this article we study a particular kind of quandle, called an Alexander quandle (see Definition 3.1). It is known that all finite connected quandles with a prime number of elements or with a square of a prime number of elements are isomorphic to an Alexander quandle (see [EGS01] and [Gr02] respectively and see Definition 2.6 for the notion of a connected quandle). Furthermore, studies have shown that a large number of quandles with a small number of elements are isomorphic to Alexander quandles (see for example [NeHo05]). These facts and the fact that

*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

Alexander quandles are relatively easy to study, due to the arithmetic flavor of their definition, serve as a motivation for their study. Finite Alexander quandles were studied in [Ne03] where an arithmetical 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 **section 2** we give a short introduction to quandles which is necessary for the statements of our results and prove a few important lemmas. In **section 3** we prove our main results as follows : In **subsection 3.1** we prove a few general formulae regarding finite Alexander quandles (not necessarily of prime order). In **subsection 3.2** we focus on finite Alexander quandles of prime order. We prove that every 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.

2 Basic Definitions and Examples of Quandles

In this section we introduce the necessary definitions and properties of quandles needed for our results on Alexander quandles.

We start with the definition of a quandle.

Definition 2.1 (Quandle). *A **quandle** is a set X with a binary operation written as $(a, b) \mapsto a^b$ and satisfies*

- (1) *For every $a, b \in X$ there exists a unique $c \in X$ such that $a = c^b$,*
- (2) *For every $a, b, c \in X$ we have $(a^b)^c = (a^c)^{b^c}$, and*
- (3) *For every $a \in X$ we have $a^a = a$.*

□

Definition 2.2. (Quandle Homomorphisms) *Let Q and R be quandles. A **quandle homomorphism** from Q to R is a map $f: Q \rightarrow R$ that satisfies $f(x^y) = f(x)^{f(y)}$ for all $x, y \in Q$. A bijective quandle homomorphism from Q to itself is called a quandle **automorphism**.* □

Two important examples of quandles are the following

Example 2.3. *The **trivial quandle** consists of a set X with quandle operation $x^y = x$ for any $x, y \in X$.*

Example 2.4. Let G be a group. G can be considered as a quandle by letting $a^b \stackrel{\text{def}}{=} b^{-1}ab$. More generally, a union of conjugacy classes G' in G can be considered as 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. $\square$

Definition 2.5 (Operator Group). 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 . As a consequence, the mapping $b \mapsto \rho_b$ determines a homomorphism $\varphi : F(X) \rightarrow \text{Aut}(X)$ (where $F(X)$ is the free group on X). Thus, each $w \in F(X)$ acts on any $x \in X$ as an automorphism, and this action is denoted x^w . The group $F(X)/\text{Ker}(\varphi)$ is called the **operator group** of the quandle X and it is denoted $\text{Op}(X)$. $\square$

Definition 2.6. A quandle X is **connected** if the operator group of X , $\text{Op}(X)$, acts transitively on X . $\square$

Lemma 2.7. Let X be a quandle. Then

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

Furthermore,

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

Proof. (2.1) is simply a statement of the fact already mentioned in Definition 2.5, that each $w \in F(X)$ acts as an automorphism on X .

Furthermore, (2.1) is equivalent to (2.2) as we now show : Let $a, b \in X$ and $w \in F(X)$. Assume (2.1) holds, then $a^{w^{-1}bw} = ((a^{w^{-1}})^b)^w = ((a^{w^{-1}})^w)^{b^w} = a^{b^w}$. On the other hand, if (2.2) holds then $(a^w)^{b^w} = a^{w^{w^{-1}bw}} = a^{bw} = (a^b)^w$. Hence (2.1) and (2.2) are indeed equivalent. $\square$

3 Alexander Quandles

Let us first give the definition of an Alexander quandle :

Definition 3.1. Given a $\mathbb{Z}[t^{\pm 1}]$ -module M , where t acts as an automorphism $\varphi \in \text{Aut}_{\mathbb{Z}}(M)$, 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**. $\square$

Remark 3.2. Note that if $t = 1$ then M is a trivial quandle and if, on the other hand, $(1-t) \in \text{Aut}_{\mathbb{Z}}(M)$, then the quandle map $a \mapsto \rho_a$ (see Definition 2.5) is injective and M is connected. $\square$

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 $a, b \in Q$ we have*

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

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

$$a^{b^k} = a^{b^{k+m}} \quad (3.2)$$

Lemma 3.4. *Let M be an Alexander quandle, then for any $a, b \in M$ and $k_i \in \mathbb{Z}$ we have that :*

For n odd :

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

For n even :

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

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.

Fix p to be some prime number. In what follows we will consider $\mathbb{Z}_p$ as an Alexander quandle with $t \in \text{Aut}_{\mathbb{Z}}(\mathbb{Z}_p)$ as defined in Definition 3.1. Note that each group automorphism of $\mathbb{Z}_p$ is a multiplication by a number in $\mathbb{Z}_p^*$ and so we will sometimes consider t as a number in $\mathbb{Z}_p^*$.

The following theorems apply to any connected finite quandle of prime order since it was proved in [EGS01] that any connected finite quandle of prime order is isomorphic to an Alexander quandle X with $t \neq 1$.

Theorem 3.5. *Let $p > 2$ be some prime number and consider $\mathbb{Z}_p$ as an Alexander quandle 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 $c \in \mathbb{Z}_p$ there exists an even $n \in \mathbb{N}$ and $k_1, \dots, k_n \in \mathbb{Z}$ such that*

$$a^{b^{k_1} a^{k_2} \dots b^{k_{n-1}} a^{k_n}} = c \quad (3.5)$$

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

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

Denote $d = (c - a)(a - b)^{-1}$, then we need $k_1, \dots, k_n$ such that

$$\sum_{i=1}^n (-1)^{i+1} t^{k_i + \dots + k_n} = d \quad (3.7)$$

For any $m \in \mathbb{N}$ let $k_i = (-1)^i$, for $i = 1, \dots, 2m$ then

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

We take $m \in \mathbb{N}$ satisfying $m = (1 - t)^{-1} d \bmod p$ to get (3.7) with $n = 2m$.

□

Theorem 3.6. *Consider $Q = \mathbb{Z}_p$ as an Alexander quandle for some prime number p 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 $\alpha \in \text{Aut}(Q)$ such that $\alpha(a) = c$ and $\alpha(b) = d$.*

Proof. According to (3.5) in Theorem 3.5, any element of Q is of the form a^x where $x \in F(\{a, b\})$. Hence, it is enough to define α on elements of this form. Let a^x be an element of this form. Define α as follows

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

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

To show that α is well defined we need to check that for any two elements in Q of the above mentioned form, a^x and a^y , the equation $a^x = a^y$ in Q implies that $\alpha(a^x) = \alpha(a^y)$. There are two possible forms for such an element :

$$a^{b^{k_1} a^{k_2} \dots b^{k_{n-2}} a^{k_{n-1}} b^{k_n}} \quad (3.9)$$

$$a^{b^{k_1} a^{k_2} \dots b^{k_{n-1}} a^{k_n}} \quad (3.10)$$

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

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

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

Let us rewrite these expressions as follows :

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

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

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

$$(K - K')(a - b) = 0 \quad (3.15)$$

where $K, K' \in \mathbb{Z}_p$ are independent of a and b and only depend on the indices $k_1, \dots, k_n$ 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 $K - K' \equiv 0 \pmod{p}$ which in turn is equivalent to (recall that $c \neq d$ by assumption) $(K - K')(c - d) = 0$ or $K(c - d) + c = K'(c - d) + c$ and this is exactly the equation $c^{\beta(x)} = c^{\beta(y)}$. This concludes the proof that α is well defined.

In exactly the same way we show that $\alpha(b) = d$. Namely, note that $b = -1(a - b) + a$, so if $b = a^w$ then the K' attached to this presentation must satisfy $K' \equiv -1 \pmod{p}$ 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 then α must also be 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 2.7 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

- [E07] M. Eisermann, *Quandle Coverings and their Galois Correspondence*, Preprint, [arXiv:math.GT/0612459](https://arxiv.org/abs/math.GT/0612459).
- [EGS01] P. Etingof, R. Guralnik, 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.
- [FR92] Fenn R., Rourke C., *Racks and Links in Codimension two*, Journal of Knot Theory and its Ramifications, **Volume 1** (1992), pages 343-406
- [Gr02] M. Grana, *Indecomposable Racks of order p^2* , Preprint, [arXiv:math.QA/0203157](https://arxiv.org/abs/math.QA/0203157)
- [Joy79] D.E. Joyce. *An algebraic approach to symmetry with applications to knot theory*. PhD thesis, University of Pennsylvania, 1979.
- [Joy82] D.E. Joyce. A classifying invariant of knots, the knot quandle. *Journal of Pure and Applied Algebra*, 23:37–65, 1982.
- [LoRo] P. Lopes, D. Roseman, *On finite racks and quandles*, may be found on [http://arXiv.org, math.GT/0412487](http://arxiv.org/math.GT/0412487).
- [Mat82] Matveev, S.V. (1982), *Distributive groupoids in knot theory*, Matematicheskii Sbornik, **119**, No. 1, pp. 78-88 (in Russian; English translation in: Mathematics of the USSR-Sbornik, **47** (1984), No 1, Pages 73-83).
- [Ne03] S. Nelson, *Classification of Finite Alexander Quandles*, [arXiv.org:math.GT/0202281](https://arxiv.org/abs/math.GT/0202281)
- [NeHo05] S. Nelson, B. Ho, *Matrices and Finite Quandles*, Homology Homotopy Appl. Volume 7, Number 1 (2005), 197-208
- [Ye06] Yetter D., *Quandles and Monodromy*, Journal of Knot Theory and Its Ramifications (JKTR) Volume 12, Number 4 (2003), 523-541