J. Math. Soc. Japan
Vol. 65, No. 4 (2013) pp. 1117–1134
doi: 10.2969/jmsj/06541117

Two-point homogeneous quandles with prime cardinality

By Hiroshi Tamaru

(Received Jan. 30, 2012)

Abstract. Quandles can be regarded as generalizations of symmetric spaces. Among symmetric spaces, two-point homogeneous Riemannian manifolds would be the most fundamental ones. In this paper, we define two-point homogeneous quandles analogously, and classify those with prime cardinality.

1. Introduction.

A *quandle* is a set X endowed with a binary operator $* : X \times X \to X$ satisfying three axioms, derived from the Reidemeister moves of a classical knot. Quandles were introduced by Joyce ([**3**]), and have played very important roles, in particular, in knot theory. For quandles and their applications, we refer to a survey [**1**] and the references therein.

Quandles are also related to symmetric spaces. Recall that a *Riemannian symmetric space* is a connected Riemannian manifold M equipped with a symmetry $s_x : M \to M$ for each $x \in M$. For symmetric spaces, we refer to famous textbooks [**4**], [**5**]. It was mentioned in [**3**] that every symmetric space is a quandle, by defining the binary operator $y*x := s_x(y)$. From this correspondence, quandles can be regarded as "discrete symmetric spaces". Our theme is to study quandles from this point of view. The purpose of this paper is to give the first step toward the theory of discrete symmetric spaces.

In this paper, we define the notion of two-point homogeneous quandles, and study them. This notion is a natural analogue of the notion of two-point homogeneous Riemannian manifolds, which form a very fundamental subclass of symmetric spaces. In fact, a Riemannian manifold is two-point homogeneous if and only if it is isometric to the Euclidean space or a Riemannian symmetric space of rank one (see Subsection 2.1). Hence, in the theory of quandles and discrete symmetric spaces, two-point homogeneous quandles would play fundamental roles, similar to rank one symmetric spaces in the theory of symmetric spaces.

The main result of this paper is an explicit classification of two-point homo-

2010 *Mathematics Subject Classification.* Primary 57M25; Secondary 53C30.
Key Words and Phrases. quandles, symmetric spaces, two-point homogeneous Riemannian manifolds.
A part of this research was supported by KAKENHI (20740040, 24654012).

geneous quandles with prime cardinality. We prove that, for each prime number $p \geq 3$, there exists a one-to-one correspondence between isomorphism classes of two-point homogeneous quandles with cardinality p and primitive roots modulo p. As a consequence, although the condition of two-point homogeneity seems to be very strong, two-point homogeneous quandles with cardinality p do exist for every prime number $p \geq 3$.

This paper is organized as follows. In Section 2, we briefly recall some necessary background on two-point homogeneous Riemannian manifolds and quandles. In Section 3, we define two-point homogeneous quandles and study their properties. We also define the notion of quandles of cyclic type, which gives a sufficient condition for quandles to be two-point homogeneous. A classification of two-point homogeneous quandles with prime cardinality, mentioned above, is given in Section 4. On the way to our classification, we recall linear Alexander quandles $\Lambda_p/(t-a)$ with prime cardinality p, and determine their inner automorphism groups. As an appendix, in Section 5, we study whether or not the notion of quandles of cyclic type is a necessary condition for the two-point homogeneity.

The author is deeply grateful to Seiichi Kamada for valuable comments and suggestions, and to the members of Hiroshima University Topology-Geometry Seminar, where he learned many things about knots and quandles. The author is also grateful to Nobuyoshi Takahashi for kind advice, and indebted to the referee for improvements in the exposition.

2. Preliminaries.

In this section we briefly recall some necessary background on two-point homogeneous Riemannian manifolds and quandles.

2.1. Riemannian homogeneous geometry.

In this subsection we briefly recall some fundamental facts on Riemannian symmetric spaces and two-point homogeneous Riemannian manifolds. We refer to [**4**] for the facts mentioned in this subsection.

DEFINITION 2.1. A connected Riemannian manifold (M, g) is called a *Riemannian symmetric space* if, for every $x \in M$, there exists an isometry $s_x : M \to M$, called the *symmetry* at x, such that

(i) x is an isolated fixed point of s_x,
(ii) $s_x^2 = \mathrm{id}_M$ (the identity map).

We here recall one basic property, which will give a connection from symmetric spaces to quandles. Note that the following property is sometimes employed as one of axioms to define symmetric spaces. See [**5**], [**6**], [**7**].

PROPOSITION 2.2. *Let (M, g) be a Riemannian symmetric space. Then, for every $x, y \in M$, we have $s_x \circ s_y = s_{s_x(y)} \circ s_x$.*

Next we recall the definition of two-point homogeneous Riemannian manifolds. For a Riemannian manifold (M, g), we denote by $\mathrm{Isom}(M, g)$ the isometry group, and by d the distance function defined by g.

DEFINITION 2.3. A connected Riemannian manifold (M, g) is said to be *two-point homogeneous* if, for every $(x_1, x_2), (y_1, y_2) \in M \times M$ satisfying $d(x_1, x_2) = d(y_1, y_2)$, there exists $f \in \mathrm{Isom}(M, g)$ such that $f(x_1, x_2) = (y_1, y_2)$.

Note that $f(x_1, x_2) = (y_1, y_2)$ means that $f(x_1) = y_1$ and $f(x_2) = y_2$. We use this notation for simplicity.

Now we recall a nice characterization and a classification of two-point homogeneous Riemannian manifolds. We refer to [**4**, Chapter IX, Section 5] and the references therein. Let $\mathrm{Isom}(M, g)_x$ be the isotropy subgroup of $\mathrm{Isom}(M, g)$ at x, which naturally acts on the tangent space T_xM.

THEOREM 2.4. *For a connected Riemannian manifold (M, g), the following conditions are mutually equivalent*:

(1) *(M, g) is two-point homogeneous,*
(2) *(M, g) is isotropic, that is, for every $x \in M$, the action of $\mathrm{Isom}(M, g)_x$ on the unit sphere in T_xM is transitive,*
(3) *(M, g) is isometric to the Euclidean space $\mathbb{R}^n$ or a Riemannian symmetric space of rank one.*

The action of $\mathrm{Isom}(M, g)_x$ on T_xM is called the *isotropy representation* at x. It is important that the two-point homogeneity can be characterised in terms of the isotropy representations. We will have an analogous characterization for two-point homogeneous quandles.

Recall that a Riemannian symmetric space of rank one is either the sphere S^n, the projective spaces $\mathbb{R}\mathrm{P}^n$, $\mathbb{C}\mathrm{P}^n$, $\mathbb{H}\mathrm{P}^n$, $\mathbb{O}\mathrm{P}^2$, or the hyperbolic spaces $\mathbb{R}\mathrm{H}^n$, $\mathbb{C}\mathrm{H}^n$, $\mathbb{H}\mathrm{H}^n$, $\mathbb{O}\mathrm{H}^2$. Therefore, two-point homogeneous Riemannian manifolds form a very fundamental subclass of the class of Riemannian symmetric spaces.

2.2. Quandles.

In this subsection, we recall some fundamental notions and examples of quandles. We employ a formulation similar to symmetric spaces, but start from the usual definition.

DEFINITION 2.5. Let X be a set and $* : X \times X \to X$ be a binary operator. The pair $(X, *)$ is called a *quandle* if

(Q1) $\forall x \in X$, $x * x = x$,
(Q2) $\forall x, y \in X$, $\exists! z \in X : z * y = x$, and
(Q3) $\forall x, y, z \in X$, $(x * y) * z = (x * z) * (y * z)$.

If $(X, *)$ is a quandle, then $*$ is called a *quandle structure* on X. We restate this definition in a similar way to symmetric spaces.

PROPOSITION 2.6. *Let X be a set, and assume that there exists a map $s_x : X \to X$ for every $x \in X$. Then, the binary operator $*$ defined by $y * x := s_x(y)$ is a quandle structure on X if and only if*

(S1) $\forall x \in X$, $s_x(x) = x$,
(S2) $\forall x \in X$, s_x *is bijective, and*
(S3) $\forall x, y \in X$, $s_x \circ s_y = s_{s_x(y)} \circ s_x$.

The proof is easy from Definition 2.5. Note that, for quandles, $s_x^2 = \mathrm{id}_X$ is not required. Throughout this paper, we denote quandles by $X = (X, s)$ with the quandle structures

$$s : X \to \mathrm{Map}(X, X) : x \mapsto s_x. \tag{2.1}$$

Here, $\mathrm{Map}(X, X)$ denotes the set of all maps from X to X. From our formulation, one easily has the following (see Proposition 2.2).

PROPOSITION 2.7 ([**3**]). *Every Riemannian symmetric space is a quandle.*

We here describe some other easy examples of quandles.

EXAMPLE 2.8. The following (X, s) are quandles:

(1) The *trivial quandle*: X is any set and $s_x := \mathrm{id}_X$ for every $x \in X$.
(2) The *dihedral quandle of order n*: $X = \{0, 1, 2, \ldots, n-1\}$ and

$$s_i(j) := 2i - j \pmod{n}.$$

(3) The *regular tetrahedron quandle*: $X = \{1, 2, 3, 4\}$ and

$$s_1 := (234), \quad s_2 := (143), \quad s_3 := (124), \quad s_4 := (132).$$

Note that (234), (143), and so on, denote the cyclic permutations. The dihedral quandle of order n can be realized geometrically as the set of n-equal dividing points on the unit circle S^1. The quandle structure is nothing but the restriction of the canonical symmetry of S^1, that is, s_x is the reflection with respect to the line

through x and the center of S^1. The regular tetrahedron quandle can be realized geometrically as the set of vertices of the regular tetrahedron.

Next, we recall some fundamental notions for quandles, such as homomorphisms, (inner) automorphisms, and connectedness.

DEFINITION 2.9. Let (X, s^X), (Y, s^Y) be quandles. A map $f : X \to Y$ is called a *homomorphism* if, for every $x \in X$, $f \circ s_x^X = s_{f(x)}^Y \circ f$ holds.

As usual, a bijective homomorphism is called an *isomorphism*, and an isomorphism from X onto X itself is called an *automorphism* of X. By definition, one can see that the automorphism group, denoted by

$$\mathrm{Aut}(X, s) := \{f : X \to X : \text{automorphism}\}, \tag{2.2}$$

is a group. It follows from (S2) and (S3) that $s_x \in \mathrm{Aut}(X, s)$ for every $x \in X$.

DEFINITION 2.10. The subgroup of $\mathrm{Aut}(X, s)$ generated by $\{s_x \mid x \in X\}$ is called the *inner automorphism group* of a quandle (X, s), and denoted by $\mathrm{Inn}(X, s)$.

Note that $\mathrm{Inn}(X, s)$ and $\mathrm{Aut}(X, s)$ are different in general. For example, if X is a trivial quandle, then $\mathrm{Inn}(X, s)$ consists of only the identity, but $\mathrm{Aut}(X, s)$ coincides with the group of all bijections.

DEFINITION 2.11. A quandle (X, s) is said to be *connected* if $\mathrm{Inn}(X, s)$ acts transitively on X.

The following gives some easy examples of connected quandles. The results are well-known, and the proofs are not difficult. Note that $\#X$ denotes the cardinality of X.

EXAMPLE 2.12. We have the following properties:

(1) the trivial quandle (X, s) is not connected if $\#X > 1$,
(2) the dihedral quandle (X, s) is connected if and only if $\#X$ is odd,
(3) the regular tetrahedron quandle is connected.

Finally in this subsection, we recall the notion of dual quandles.

DEFINITION 2.13. Let (X, s) be a quandle. Then, (X, s^{-1}) defined by the following is called the *dual quandle*:

$$s^{-1} : X \to \mathrm{Map}(X, X) : x \mapsto s_x^{-1}. \tag{2.3}$$

It is easy to see that the dual quandle (X, s^{-1}) is also a quandle. A quandle

and its dual quandle share many properties, as we will see in the latter sections. The reason is the following, which can be proved directly from the definition.

PROPOSITION 2.14. $\mathrm{Inn}(X, s) = \mathrm{Inn}(X, s^{-1})$.

DEFINITION 2.15. A quandle (X, s) is said to be *self-dual* if it is isomorphic to the dual quandle (X, s^{-1}).

EXAMPLE 2.16. The trivial quandles, the dihedral quandles, and the regular tetrahedron quandle are self-dual.

3. Two-point homogeneous quandles.

In this section, we define two-point homogeneous quandles, and give a characterization and a sufficient condition for quandles to be two-point homogeneous. We denote by $G := \mathrm{Inn}(X, s)$ the inner automorphism group of a quandle $X = (X, s)$.

3.1. Definition.

In this subsection, we define two-point homogeneous quandles, analogously to two-point homogeneous Riemannian manifolds.

DEFINITION 3.1. A quandle X is said to be *two-point homogeneous* if for all $(x_1, x_2), (y_1, y_2) \in X \times X$ satisfying $x_1 \neq x_2$ and $y_1 \neq y_2$, there exists $f \in G$ such that $f(x_1, x_2) = (y_1, y_2)$.

It would be more exact to call it *two-point homogeneous with respect to the inner automorphism group* G. One can naturally think of a two-point homogeneous quandle with respect to the automorphism group $\mathrm{Aut}(X)$. These two notions are different. For example, a trivial quandle X with $\#X > 1$ is always two-point homogeneous with respect to $\mathrm{Aut}(X)$, but not two-point homogeneous with respect to G.

Since the two-point homogeneity is defined in terms of the action of G, one can immediately see the following.

PROPOSITION 3.2. *If a quandle (X, s) is two-point homogeneous, then so is the dual quandle (X, s^{-1}).*

PROOF. This follows easily from Proposition 2.14. □

3.2. A characterization.

Recall that two-point homogeneous Riemannian manifolds can be characterized in terms of the isotropy representations (see Theorem 2.4). In this subsection, we give a similar characterization for two-point homogeneous quandles. Let G_x be the isotropy subgroup of G at $x \in X$, that is,

$$G_x := \{f \in G \mid f(x) = x\}. \tag{3.1}$$

PROPOSITION 3.3. *Let X be a quandle and assume that $\#X \geq 3$. Then the following conditions are mutually equivalent*:

(1) *X is two-point homogeneous,*
(2) *for every $x \in X$, the action of G_x on $X \setminus \{x\}$ is transitive,*
(3) *X is connected, and there exists $x \in X$ such that the action of G_x on $X \setminus \{x\}$ is transitive.*

PROOF. We show (1) $\Rightarrow$ (2). Take any $x \in X$. To show the transitivity, take any $y_1, y_2 \in X \setminus \{x\}$. Since $x \neq y_1$ and $x \neq y_2$, there exists $f \in G$ such that $f(x, y_1) = (x, y_2)$ by (1). This means $f \in G_x$ and $f(y_1) = y_2$.

We show (2) $\Rightarrow$ (3). We have only to show that X is connected. Take any $x, y \in X$. Since $\#X \geq 3$, there exists $z \in X \setminus \{x, y\}$. By (2), the action of G_z on $X \setminus \{z\}$ is transitive. Since $x, y \in X \setminus \{z\}$, there exists $f \in G_z$ such that $f(x) = y$.

We show (3) $\Rightarrow$ (1). Take any $(x_1, x_2), (y_1, y_2) \in X \times X$ satisfying $x_1 \neq x_2$ and $y_1 \neq y_2$. By (3), there exists $x \in X$ such that the action of G_x on $X \setminus \{x\}$ is transitive. Also by (3), X is connected, and hence there exist $f_1, f_2 \in G$ such that $f_1(x_1) = x$ and $f_2(y_1) = x$. One now has

$$f_1(x_1, x_2) = (x, f_1(x_2)), \quad f_2(y_1, y_2) = (x, f_2(y_2)). \tag{3.2}$$

Note that $f_1(x_2), f_2(y_2) \in X \setminus \{x\}$. Thus, there exists $f_3 \in G_x$ such that

$$f_3(f_1(x_2)) = f_2(y_2). \tag{3.3}$$

One can see that $f_2^{-1} \circ f_3 \circ f_1 \in G$ maps (x_1, x_2) onto (y_1, y_2). □

Examples of two-point homogeneous quandles will be given later. Here we see examples of quandles which are not two-point homogeneous. This shows that the condition of the two-point homogeneity is very strong.

EXAMPLE 3.4. The dihedral quandle of order $n \geq 4$ is not two-point homogeneous.

PROOF. Let X be the dihedral quandle of order n, which we identify with the set of n-equal dividing points on the unit circle S^1 centered at $(0, 0) \in \mathbb{R}^2$. Let $\mathrm{O}(2)$ be the orthogonal group, which is naturally acting on S^1. Since $s_x \in \mathrm{O}(2)$ for every x, we have $G \subset \mathrm{O}(2)$.

Take $x \in X$. The isotropy subgroup at x satisfies

$$G_x \subset \mathrm{O}(2)_x = \{\mathrm{id}, s_x\} \cong \mathbb{Z}_2. \tag{3.4}$$

By assumption, one has $\#(X \setminus \{x\}) \geq 3$. Therefore, G_x cannot act transitively on $X \setminus \{x\}$. From the characterization given in Proposition 3.3, X is not two-point homogeneous. □

3.3. A sufficient condition.

From now on we assume that a quandle $X = (X, s)$ is finite and satisfies $\#X \geq 3$. In this subsection, we give a sufficient condition, called the cyclic type property, for quandles to be two-point homogeneous. We also see some basic properties of them.

DEFINITION 3.5. A quandle (X, s) with $\#X = n \geq 3$ is said to be of *cyclic type* if, for every $x \in X$, s_x acts on $X \setminus \{x\}$ as a cyclic permutation of order $(n-1)$,

Let us denote by $\langle s_x \rangle$ the cyclic group generated by s_x. The cyclic type property is a sufficient condition for quandles to be two-point homogeneous.

PROPOSITION 3.6. *Every quandle of cyclic type is two-point homogeneous.*

PROOF. Let X be a quandle of cyclic type. Take any $x \in X$. From Proposition 3.3, we have only to show that the action of G_x on $X \setminus \{x\}$ is transitive. By assumption, $\langle s_x \rangle$ acts transitively on $X \setminus \{x\}$. Thus, so does G_x, since $\langle s_x \rangle \subset G_x$. □

In the remaining of this subsection, we study some properties of quandles of cyclic type. The first one is the invariance under duality.

PROPOSITION 3.7. *If (X, s) is of cyclic type, then so is the dual quandle (X, s^{-1}).*

PROOF. Take any $x \in X$. By assumption, s_x acts on $X \setminus \{x\}$ as a cyclic permutation of order $(n-1)$. Then, so does s_x^{-1}. □

The second property of quandles of cyclic type is a characterization, similar to Proposition 3.3 for two-point homogeneous ones. It will be stated after a small lemma.

LEMMA 3.8. *Let $X = (X, s)$ be a connected quandle. Then, for every $x, y \in X$, there exists $f \in G$ such that $s_y = f \circ s_x \circ f^{-1}$.*

PROOF. Take any $x, y \in X$. Since X is connected, there exists $f \in G$ such that $y = f(x)$. Since f is an automorphism, we have

$$f \circ s_x = s_{f(x)} \circ f = s_y \circ f. \tag{3.5}$$

This completes the proof. □

PROPOSITION 3.9. *Let $X = (X, s)$ be a quandle with $\#X = n \geq 3$. Then the following conditions are mutually equivalent*:

(1) *X is of cyclic type,*
(2) *X is connected, and there exists $x \in X$ such that s_x acts on $X \setminus \{x\}$ as a cyclic permutation of order $(n-1)$,*
(3) *X is connected, and there exists $x \in X$ such that $\langle s_x \rangle$ acts transitively on $X \setminus \{x\}$.*

PROOF. We prove (1) ⇒ (2). Assume that X is of cyclic type. We have only to show that X is connected. One knows X is two-point homogeneous from Proposition 3.6, and hence connected from Proposition 3.3.

We prove (2) ⇒ (1). Assume that X is connected, and there exists $x \in X$ such that s_x acts on $X \setminus \{x\}$ as a cyclic permutation of order $(n-1)$. Take any $y \in X$. Since X is connected, Lemma 3.8 yields that s_y is conjugate to s_x. Thus, s_y acts as a cyclic permutation of order $(n-1)$, since so does s_x. Hence X is of cyclic type.

The equivalence (2) ⇔ (3) is obvious. □

We here see some easy examples of quandles of cyclic type. They thus give examples of two-point homogeneous quandles. Further examples will be given in the next section.

EXAMPLE 3.10. The following quandles are of cyclic type, and hence two-point homogeneous:

(1) the dihedral quandle of order 3, and
(2) the regular tetrahedron quandle.

PROOF. Recall that both quandles are connected (see Example 2.12). Thus, we have only to study the action of s_x on $X \setminus \{x\}$ for some x.

Let $X^3 = \{0, 1, 2\}$ be the dihedral quandle of order 3. For $x = 0$, one has $s_0 = (12)$, which acts on $X^3 \setminus \{0\} = \{1, 2\}$ as a cyclic permutation of order 2.

Let $X^4 = \{1, 2, 3, 4\}$ be the regular tetrahedron quandle. For $x = 1$, one has $s_1 = (234)$, which acts on $X^4 \setminus \{1\} = \{2, 3, 4\}$ as a cyclic permutation of order 3. □

4. Classification for prime cardinality case.

In this section we classify two-point homogeneous quandles with prime cardinality $p \geq 3$. The proof is based on the classification of connected quandles with prime cardinality, namely, they must be linear Alexander quandles $\Lambda_p/(t-a)$. We determine the inner automorphism groups of $\Lambda_p/(t-a)$, and apply it to our classification.

4.1. Review on linear Alexander quandles.

In this subsection, we review some known results on linear Alexander quandles. In fact, every connected quandle with prime cardinality is isomorphic to some linear Alexander quandle.

DEFINITION 4.1. Let $\Lambda_n := \mathbb{Z}_n[t^{\pm 1}]$ be the Laurant polynomial ring over $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. The quotient Λ_n/J by an ideal J equipped with the following operator is called the *Alexander quandle*:

$$s_{[x]}([y]) := [ty + (1-t)x]. \tag{4.1}$$

It is easy to check that Λ_n/J is a quandle, that is, the above operator satisfies the conditions (S1), (S2) and (S3).

DEFINITION 4.2. Let $a \in \mathbb{Z}$ and $J := (t-a)$, the ideal generated by $t-a$ in Λ_n. Then, the Alexander quandle of the form $\Lambda_n/(t-a)$ is said to be *linear*.

For a linear Alexander quandle, there is a natural identification $\Lambda_n/(t-a) = \mathbb{Z}_n$. The quandle operation can be written, in terms of the addition and the multiplication on $\mathbb{Z}_n$, as follows:

$$s_{[x]}([y]) := [ty + (1-t)x] = [a][y] + [1-a][x]. \tag{4.2}$$

EXAMPLE 4.3. The linear Alexander quandle $\Lambda_n/(t-1)$ is trivial, and $\Lambda_n/(t+1)$ is isomorphic to the dihedral quandle of order n.

PROOF. We only prove the second assertion. Consider $\Lambda_n/(t+1)$, that is, $a = n-1$. Then, (4.2) yields that

$$s_{[x]}([y]) = [n-1][y] + [1-(n-1)][x] = [2x-y]. \tag{4.3}$$

This shows that $\Lambda_n/(t+1)$ is the dihedral quandle (see Example 2.8). □

From now on we concern with the case $n = p$, a prime number. We recall some results obtained by Nelson ([**8**]).

PROPOSITION 4.4 ([**8**]). *Let p be a prime number. Then we have the following*:

(1) *There are exactly $p-1$ distinct linear Alexander quandles with cardinality p up to isomorphism. They are $\Lambda_p/(t-a)$ for $a = 1, 2, \ldots, p-1$.*
(2) *If $a = 2, \ldots, p-1$, then $\Lambda_p/(t-a)$ is connected.*
(3) *$\Lambda_p/(t-a)$ is dual to $\Lambda_p/(t-b)$ if and only if $ab \equiv 1 \pmod{p}$.*

Now we recall the classification of connected quandles with prime cardinality obtained in [**2**]. We also refer to [**9**, Section 5].

THEOREM 4.5 ([**2**]). *Every connected quandle with prime cardinality p is isomorphic to a linear Alexander quandle $\Lambda_p/(t-a)$ for some $a = 2, 3, \ldots, p-1$.*

Recall that two-point homogeneous quandles must be connected (Proposition 3.3). Therefore, for the classification of prime cardinality ones, we have only to determine which linear Alexander quandles are two-point homogeneous or not.

4.2. The inner automorphism groups of linear Alexander quandles. Let $X = \Lambda_p/(t-a)$ be a linear Alexander quandle with prime cardinality p, where $a = 2, 3, \ldots, p-1$. In this subsection, we determine the inner automorphism groups $G = \mathrm{Inn}(X)$ of X. We identify $X = \mathbb{Z}_p$ as in the previous subsection.

Recall that G is the group generated by $\{s_{[x]} \mid [x] \in X\}$. First of all, we see formulas for the compositions of generators.

LEMMA 4.6. *For $[x], [x_1], [x_2] \in X$ and $k, k_1, k_2 \in \mathbb{Z}$, we have*

$$(s_{[x]})^k([y]) = [a^k][y] + [1-a^k][x], \tag{4.4}$$

$$(s_{[x_1]})^{k_1}(s_{[x_2]})^{k_2}([y]) = [a^{k_1+k_2}][y] + [a^{k_1}][1-a^{k_2}][x_2] + [1-a^{k_1}][x_1]. \tag{4.5}$$

PROOF. Recall that $s_{[x]}$ is given by (4.2). Then, one can show (4.4) by induction. The proof of (4.5) easily follows from (4.4). □

Using these formulas, we see that G contains some particular transformations. For $[m] \in X$, let us define

$$\varphi_{[m]} : X \to X : [x] \mapsto [x+m]. \tag{4.6}$$

LEMMA 4.7. *For every $[m] \in X$, we have $\varphi_{[m]} \in G$.*

PROOF. Since $\varphi_{[m]} = (\varphi_{[1]})^m$, we have only to show that $\varphi_{[1]} \in G$. This follows from the following claim:

$$(s_{[1-a]^{-1}})(s_{[0]})^{p-2} = \varphi_{[1]}. \tag{4.7}$$

Note that $[1-a]$ is invertible. We show (4.7). Take any $[y] \in X$. It follows from Lemma 4.6 and $[a^{p-1}] = [1]$ that

$$(s_{[1-a]^{-1}})(s_{[0]})^{p-2}([y]) = [a^{p-1}][y] + [1-a][1-a]^{-1} = [y] + [1] = \varphi_{[1]}([y]). \tag{4.8}$$

This shows (4.7), and hence completes the proof of the lemma. □

Note that $\{\varphi_{[m]} \mid [m] \in X\}$ is a subgroup of G, and obviously acts transitively on X. This immediately yields that X is connected. Hence, Lemma 4.7 gives a simple proof of Proposition 4.4 (2).

We now determine the inner automorphism groups G, by giving explicit expressions in terms of $s_{[x]}$ and $\varphi_{[m]}$

THEOREM 4.8. *The inner automorphism group of $X = \Lambda_p/(t-a)$ satisfies*

$$G = \{(s_{[x]})^k \mid [x] \in X,\, k \in \mathbb{Z}\} \cup \{\varphi_{[m]} \mid [m] \in X\}. \tag{4.9}$$

PROOF. We denote by (R) the right-hand side of (4.9) for simplicity. One knows $G \supset$ (R) from Lemma 4.7. We prove $G \subset$ (R). Note that (R) contains generators of G, that is,

$$\{s_{[x]} \mid [x] \in X\} \subset \text{(R)}. \tag{4.10}$$

Therefore, it is enough to show that (R) is a group. To show this, one has only to check

$$(s_{[x_1]})^{k_1}(s_{[x_2]})^{k_2}, \quad (s_{[x]})^k(\varphi_{[m]}), \quad (\varphi_{[m]})(s_{[x]})^k \in \text{(R)}. \tag{4.11}$$

Claim 1: $(s_{[x_1]})^{k_1}(s_{[x_2]})^{k_2} \in$ (R). For simplicity, let

$$[z] := [a^{k_1}][1-a^{k_2}][x_2] + [1-a^{k_1}][x_1]. \tag{4.12}$$

Then, Lemma 4.6 yields that

$$(s_{[x_1]})^{k_1}(s_{[x_2]})^{k_2}([y]) = [a^{k_1+k_2}][y] + [z]. \tag{4.13}$$

Case 1: Assume that $[a^{k_1+k_2}] = [1]$. In this case, we have

$$(s_{[x_1]})^{k_1}(s_{[x_2]})^{k_2}([y]) = [y] + [z] = \varphi_{[z]}([y]). \tag{4.14}$$

This yields that

$$(s_{[x_1]})^{k_1}(s_{[x_2]})^{k_2} = \varphi_{[z]} \in (\mathrm{R}). \tag{4.15}$$

Case 2: Assume that $[a^{k_1+k_2}] \neq [1]$. In this case, one has

$$\begin{aligned}(s_{[x_1]})^{k_1}(s_{[x_2]})^{k_2}([y]) &= [a^{k_1+k_2}][y] + [1-a^{k_1+k_2}][1-a^{k_1+k_2}]^{-1}[z] \\ &= (s_{[1-a^{k_1+k_2}]^{-1}[z]})^{k_1+k_2}([y]).\end{aligned} \tag{4.16}$$

This yields that

$$(s_{[x_1]})^{k_1}(s_{[x_2]})^{k_2} = (s_{[1-a^{k_1+k_2}]^{-1}[z]})^{k_1+k_2} \in (\mathrm{R}). \tag{4.17}$$

From the arguments in Case 1 and Case 2, we conclude Claim 1.

Claim 2: $(s_{[x]})^k(\varphi_{[m]}) \in (\mathrm{R})$. First of all, one has

$$\begin{aligned}(s_{[x]})(\varphi_{[m]})([y]) &= s_{[x]}([y+m]) \\ &= [a][y+m] + [1-a][x] \\ &= [a][y] + [1-a]([1-a]^{-1}[am] + [x]) \\ &= s_{[1-a]^{-1}[am]+[x]}([y]).\end{aligned} \tag{4.18}$$

Hence, Claim 1 yields that

$$(s_{[x]})^k(\varphi_{[m]}) = (s_{[x]})^{k-1}(s_{[1-a]^{-1}[am]+[x]}) \in (\mathrm{R}). \tag{4.19}$$

This concludes the proof of Claim 2.

Claim 3: $(\varphi_{[m]})(s_{[x]})^k \in (\mathrm{R})$. This can be proved similarly to Claim 2. □

As a corollary, we have an explicit expression of the isotropy subgroup $G_{[0]}$ of G at $[0] \in X$. This expression is crucial for the classification of two-point homogeneous quandles. Recall that $\langle s_{[0]} \rangle$ denotes the cyclic group generated by $s_{[0]}$.

COROLLARY 4.9. *The inner automorphism group of $X = \Lambda_p/(t-a)$ satisfies*

$$G_{[0]} = \langle s_{[0]} \rangle. \tag{4.20}$$

PROOF. One knows ($\supset$). To prove ($\subset$), it is enough to show that

$$\#G_{[0]} \leq \#\langle s_{[0]} \rangle. \tag{4.21}$$

We show this inequality. From Theorem 4.8, one has

$$G = \{\mathrm{id}\} \cup \bigcup_{[x] \in X} (\langle s_{[x]} \rangle \setminus \{\mathrm{id}\}) \cup \{\varphi_{[m]} \mid [0] \neq [m] \in X\}. \tag{4.22}$$

Since X is connected, Lemma 3.8 yields that $s_{[x]}$ and $s_{[0]}$ are conjugate for every $[x] \in X$. One thus has

$$\#\langle s_{[x]} \rangle = \#\langle s_{[0]} \rangle. \tag{4.23}$$

This yields that

$$\#G \leq 1 + \sum_{[x] \in X} (\#\langle s_{[x]} \rangle - 1) + (p-1) = \#\langle s_{[0]} \rangle \cdot p. \tag{4.24}$$

Recall that G acts transitively on X, and hence $X = G/G_{[0]}$. We thus have

$$p = \#X = \#G/\#G_{[0]} \leq (\#\langle s_{[0]} \rangle \cdot p)/\#G_{[0]}. \tag{4.25}$$

This proves (4.21), and hence completes the proof of the corollary. □

4.3. A classification.

In this subsection, we classify two-point homogeneous quandles and quandles of cyclic type, with prime cardinality $p \geq 3$.

For the classification, we have only to study linear Alexander quandles. We begin with an elementary observation.

LEMMA 4.10. *Let $X = \Lambda_p/(t-a) = \mathbb{Z}_p$ be a linear Alexander quandle. Then we have*

$$\langle s_{[0]} \rangle.[1] = \{[1], [a], [a^2], [a^3], \ldots\}. \tag{4.26}$$

PROOF. By definition, one has

$$s_{[0]}([y]) = [a][y] + [1-a][0] = [ay]. \tag{4.27}$$

Then the proof easily follows. □

We denote the multiplicative group of $\mathbb{Z}_p$ by

$$(\mathbb{Z}_p)^\times := \mathbb{Z}_p \setminus \{[0]\}. \tag{4.28}$$

One knows that $(\mathbb{Z}_p)^\times$ is a cyclic group of order $p-1$. An integer a $(2 \leq a \leq p-1)$ is called a *primitive root modulo* p if $[a]$ generates $(\mathbb{Z}_p)^\times$.

THEOREM 4.11. *Let X be a quandle with prime cardinality $p \geq 3$. Then, the following conditions are mutually equivalent*:

(1) *X is two-point homogeneous,*
(2) *X is isomorphic to the linear Alexander quandle $\Lambda_p/(t-a)$, where a is a primitive root modulo p,*
(3) *X is of cyclic type.*

PROOF. We prove (1) $\Rightarrow$ (2). Assume that X is two-point homogeneous. Proposition 3.3 yields that X is connected and $G_{[0]}$ acts transitively on $X \setminus \{[0]\}$. Since X is connected, it is isomorphic to $\Lambda_p/(t-a)$ for some $a = 2, 3, \ldots, p-1$ (see Theorem 4.5). Since $G_{[0]}$ acts transitively on $X \setminus \{[0]\}$, one has

$$G_{[0]}.[1] = X \setminus \{[0]\} = (\mathbb{Z}_p)^\times. \tag{4.29}$$

Furthermore, from Corollary 4.9 and Lemma 4.10, we have

$$G_{[0]}.[1] = \langle s_{[0]} \rangle.[1] = \{[1], [a], [a^2], [a^3], \ldots\}. \tag{4.30}$$

Therefore, $[a]$ generates $(\mathbb{Z}_p)^\times$, and hence a is a primitive root modulo p.

We prove (2) $\Rightarrow$ (3). Let $X := \Lambda_p/(t-a)$ and assume that a is a primitive root modulo p. Since $a \neq 1$, one knows that X is connected (see Proposition 4.4). Thus, from Proposition 3.9, we have only to show that $\langle s_{[0]} \rangle$ acts transitively on $X \setminus \{[0]\}$. This follows from Lemma 4.10 and the assumption on a,

$$\langle s_{[0]} \rangle.[1] = \{[1], [a], [a^2], [a^3], \ldots\} = (\mathbb{Z}_p)^\times = X \setminus \{[0]\}. \tag{4.31}$$

Hence X is of cyclic type.

One knows (3) $\Rightarrow$ (1) from Proposition 3.6. □

Recall that, for every prime number $p \geq 3$, there always exists a primitive root a modulo p. This implies the following.

COROLLARY 4.12. *For each prime number $p \geq 3$, there exists a two-point homogeneous quandle with cardinality p.*

Furthermore, in general, there are several non-isomorphic two-point homogeneous quandles with the same cardinality p. We list the number of two-point homogeneous quandles with prime cardinality $p \leq 37$ in Table 1. The first column denote the prime number p. The second column # represents the number of the isomorphism classes of two-point homogeneous quandles with cardinality p. The third column lists a so that $\Lambda_p/(t-a)$ is two-point homogeneous, that is, a is a primitive root modulo p (we refer to [**10**]). Here, $a \leftrightarrow b$ means that $\Lambda_p/(t-a)$ and $\Lambda_p/(t-b)$ are dual to each other, that is, $ab \equiv 1 \pmod{p}$ (see Proposition 4.4).

Table 1. The number of two-point homogeneous quandles.

p	#	a (so that $\Lambda_p/(t-a)$ is two-point homogeneous)
3	1	2
5	2	$2 \leftrightarrow 3$
7	2	$3 \leftrightarrow 5$
11	4	$2 \leftrightarrow 6, \quad 7 \leftrightarrow 8$
13	4	$2 \leftrightarrow 7, \quad 6 \leftrightarrow 11$
17	8	$3 \leftrightarrow 6, \quad 5 \leftrightarrow 7, \quad 10 \leftrightarrow 12, \quad 11 \leftrightarrow 14$
19	6	$2 \leftrightarrow 10, \quad 3 \leftrightarrow 13, \quad 14 \leftrightarrow 15$
23	10	$5 \leftrightarrow 14, \quad 7 \leftrightarrow 10, \quad 11 \leftrightarrow 21, \quad 15 \leftrightarrow 20, \quad 17 \leftrightarrow 19$
29	12	$2 \leftrightarrow 15, \quad 3 \leftrightarrow 10, \quad 8 \leftrightarrow 11, \quad 14 \leftrightarrow 27, \quad 18 \leftrightarrow 21, \quad 19 \leftrightarrow 26$
31	8	$3 \leftrightarrow 21, \quad 11 \leftrightarrow 17, \quad 12 \leftrightarrow 13, \quad 22 \leftrightarrow 24$
37	12	$2 \leftrightarrow 19, \quad 5 \leftrightarrow 15, \quad 13 \leftrightarrow 20, \quad 17 \leftrightarrow 24, \quad 18 \leftrightarrow 35, \quad 22 \leftrightarrow 32.$

5. Appendix.

We saw in Proposition 3.6 that, if X is of cyclic type, then it is two-point homogeneous. We are interested in whether the converse of this statement holds or not. Our naive conjecture is the following.

CONJECTURE 5.1. *Let X be a two-point homogeneous quandle with finite cardinality. Then X is of cyclic type.*

Theorem 4.11 yields that, our conjecture is true if $\#X$ is prime. We show in this Appendix that, our conjecture is also true if $\#X - 1$ is prime.

LEMMA 5.2. *Let (X, s) be a quandle and $x \in X$. Then, s_x is contained in the center of G_x.*

PROOF. Take any $f \in G_x$. Then we have

$$f \circ s_x = s_{f(x)} \circ f = s_x \circ f,$$

since f is an automorphism and $f(x) = x$. □

PROPOSITION 5.3. *Let X be a two-point homogeneous quandle, and assume that $\#X = p + 1$, where p is a prime number. Then X is of cyclic type.*

PROOF. Let X be a two-point homogeneous quandle with $\#X = p+1$. Note that X is connected from Proposition 3.3. Take any $x \in X$. From Proposition 3.9, we have only to show that $\langle s_x \rangle$ acts transitively on $X \setminus \{x\}$.

Let us consider the orbit decomposition

$$X \setminus \{x\} = \coprod_{i=1}^{m} \langle s_x \rangle . y_i,$$

where $\langle s_x \rangle . y_i$ denotes the $\langle s_x \rangle$-orbit through y_i, and m is the number of orbits. We are going to show that $m = 1$.

Claim 1: All $\langle s_x \rangle$-orbits have the same cardinality. To show this, take any $y, z \in X \setminus \{x\}$. Since X is two-point homogeneous, Proposition 3.3 yields that there exists $f \in G_x$ such that $f(y) = z$. From Lemma 5.2, we have

$$f(\langle s_x \rangle . y) = \langle s_x \rangle . f(y) = \langle s_x \rangle . z.$$

This implies that $\langle s_x \rangle . y$ and $\langle s_x \rangle . z$ have the same cardinality.

Claim 2: $\#(\langle s_x \rangle . y_1) > 1$. Assume that $\#(\langle s_x \rangle . y_1) = 1$. Then, Claim 1 yields that every $\langle s_x \rangle$-orbit has the cardinality 1. This means $s_x = \mathrm{id}_X$. Since X is connected, Lemma 3.8 yields that $s_z = \mathrm{id}_X$ for all $z \in X$. This implies that X is a trivial quandle, which contradicts the connectedness of X.

Claim 3: $m = 1$. From Claim 1, we have

$$p = \#(X \setminus \{x\}) = m \cdot \#(\langle s_x \rangle . y_1).$$

Since p is a prime number by assumption, Claim 2 yields that $m = 1$. □

References

[1] J. S. Carter, A survey of quandle ideas, In: Introductory Lectures on Knot Theory, Ser. Knots Everything, **46**, World Sci. Publ., Hackensack, NJ, 2012, pp. 22–53.

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

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

[4] S. Helgason, Differential Geometry and Symmetric Spaces, Pure Appl. Math., **12**, Aca-

demic Press, New York, London, 1962.
[5] O. Loos, Symmetric Spaces. I: General Theory, W. A. Benjamin, Inc., New York, Amsterdam, 1969.
[6] T. Nagano, Geometric theory of symmetric spaces (in Japanese), RIMS Kôkyûroku, **1206** (2001), 55–82.
[7] T. Nagano and M. S. Tanaka, The involutions of compact symmetric spaces. V, Tokyo J. Math., **23** (2000), 403–416.
[8] S. Nelson, Classification of finite Alexander quandles, In: Proceedings of the Spring Topology and Dynamical Systems Conference, University of Texas, Austin, TX, 2002, Topology Proc., **27**, Auburn, AL, 2003, pp. 245–258.
[9] T. Ohtsuki, Problems on invariants of knots and 3-manifolds, In: Invariants of Knots and 3-Manifolds, Kyoto, 2001, Geom. Topol. Monogr., **4**, Geometry & Topology Publications, Coventry, 2002, pp 377–572.
[10] T. Takagi, Lectures on Elementary Number Theory, 2nd ed. (in Japanese), Kyoritsu Shuppan Co., Ltd., Tokyo, 1971.

Hiroshi TAMARU
Department of Mathematics
Hiroshima University
Higashi-Hiroshima
Hiroshima 739-8526, Japan
E-mail: tamaru@math.sci.hiroshima-u.ac.jp