East Asian Math. J.
Vol. 30 (2014), No. 3, pp. 293–302
http://dx.doi.org/10.7858/eamj.2014.019

REVISIT TO CONNECTED ALEXANDER QUANDLES OF SMALL ORDERS VIA FIXED POINT FREE AUTOMORPHISMS OF FINITE ABELIAN GROUPS

Hyo-Seob Sim* and Hyun-Jong Song

Abstract. In this paper we provide a rigorous proof for the fact that there are exactly 8 connected Alexander quandles of order 2^5 by combining properties of fixed point free automorphisms of finite abelian 2-groups and the classification of conjugacy classes of $\mathrm{GL}(5,2)$. Furthermore we verify that six of the eight associated Alexander modules are simple, whereas the other two are semisimple.

1. Introduction

In knot theory, quandles were considered by G. Wraith and J. Conway in 1959 as a generalization of a group with the binary operation given by conjugation, and further developed by D. Joice [4] in 1980 for invariants of knots. In particular, connected finite quandles receive attentions for generalization of the classical Fox's n-colorings of knots [14].

A family of connected finite quandles were already investigated in the other area of mathematics with terms such as distributive (both left and right) or left-distributive quasigroups which include all connected finite Alexander quandles, a major class of finite quandles in knot theory. For instance, Kepka and Nemec [5] classified distributive quasigroups of order ≤ 15. In particular, they explicitly described 44 nontrivial ones which agree with all connected finite Alexander quandles on the Ohtsuki's list [10]. Indeed, it is not difficult to see that a connected finite Alexander quandle bears another name, i.e., a medial idempotent quasigroup by using the Toyoda representation theorem [15] (the fundamental theorem in quasigroup theory).

Received December 27, 2013; Accepted February 25, 2014.
2010 *Mathematics Subject Classification.* 57M27, 20G40, 20N05.
Key words and phrases. finite connected quandles, fixed point free automorphisms, conjugacy classes, the general linear groups.
* This work was supported by a Research Grant of Pukyong National University (2013 year).

Beginning with Nelson [9], the classification of connected finite Alexander quandles has been further carried out by Murrillo and Nelson [7] for order 2^4, by Grãna [1] and Hou [3] for prime power orders p^2 and p^3, p^4, respectively.

As of 2013 the classification of connected finite Alexander quadles is extended up to order 2^5 by using a computer in [11]. In this paper we provide a rigorous proof for the fact that there are exactly 8 connected Alexander quandles of order 2^5 by combining properties of fixed point free automorphisms of finite abelian 2-groups and the classification of conjugacy classes of $\mathrm{GL}(5, 2)$. Furthermore, we verify that six among the eight associated Alexander modules are simple, whereas the other two are semisimple.

2. Preliminaries

In this section we begin with definition of the Alexander module. Let A be a finite abelian group and let $\mathrm{Aut}(A)$ be the automorphism group of A. Then ϕ in $\mathrm{Aut}(A)$ induces an action of $\Lambda = \mathbb{Z}[t, t^{-1}]$, the ring of Laurent polynomials with integer coefficients on A by extending the action

$$t^{\pm 1}\, a = \phi^{\pm 1}(a) \quad \text{for every} \quad a \in A$$

to that of $f(t)$ in Λ. In this way we have a Λ-module A_ϕ, being referred to as an *Alexander module*.

We here have a well known result.

Lemma 2.1. *Let ϕ, ψ be automorphisms of a finite abelian group A. Then*

(1) *A_ϕ is isomorphic to A_ψ if and only if ϕ is conjugate to ψ in $\mathrm{Aut}(A)$, equivalently, there exists π in $\mathrm{Aut}(A)$ such that $\pi\, \phi\, \pi^{-1} = \psi$;*

(2) *If A is of odd order abelian group, then A is fixed point free.*

Our interests in Alexander modules come from knot theory. Indeed there we have a quandle defined on a set Q with a binary operation $\cdot$ such that for all x, y, z in Q,

1) $x \cdot x = x$,

2) a left multiplication $L_x : Q \to Q$ defined by $L_x(y) = x \cdot y$ is a permutation on Q for each x in Q,

3) $(x \cdot y) \cdot z = (x \cdot z) \cdot (y \cdot z)$.

A quandle is said to be *connected* if and only if for any pair y, z in Q there exists x in Q such that $L_x(y) = z$. Let ϕ be an automorphism of finite abelian group A with the operation written additively. Then defining

$$a \cdot_\phi b = \phi(a) + (1 - \phi)(b)$$

for all a, b in A, we have so called a finite *Alexader quandle* denoted by $(A, \cdot_\phi)$.

An automorphism ϕ of a group G is said to be *fixed point free* if ϕ fixes only the identity element of G. A finite group G is said to be *fixed point free* if G has a fixed point free automorphism.

The following basic facts are well known.

Theorem 2.2. ([9]) *Let ϕ and ψ be automorphisms of a finite abelian group A. Then $(A, \cdot_\phi)$ is isomorphic to $(A, \cdot_\psi)$ if and only if $(1-t)A_\phi$ is isomorphic to $(1-t)A_\psi$ as Λ-module.*

Lemma 2.3. *Let ϕ be an automorphism of a finite abelian group A. The following satements are equivalent:*
(1) *ϕ is fixed point free;*
(2) *$I - \phi \in \mathrm{Aut}(A)$;*
(3) *$(1-t)A_\phi = A_\phi$;*
(4) *$(A, \cdot_\phi)$ is connected.*

Corollary 2.4. *Let ϕ and ψ be fixed point free automorphisms of a finite abelian group A. Then the followings are equivalent:*
(1) *$(A, \cdot_\phi)$ is isomorphic to $(A, \cdot_\psi)$ (as quandles);*
(2) *A_ϕ is isomorphic to A_ψ (as Λ-modules);*
(3) *ϕ is conjugate to ψ in $\mathrm{Aut}(A)$.*

Thus the problem of classifying connected Alexander quandles up to isomorphism is equivalent to that of classifying fixed point free automorphisms of a finite abelian group up to conjugacy.

Here we have well known properties of fixed point free finite abelian groups.

Lemma 2.5. *If A is an abelian group of odd order, then A is fixed point free.*

Lemma 2.6. *If A is an elementary abelian group of order 2^r, then A is fixed point free if and only if $r \geq 2$.*

Lemma 2.7. *If both A and B are fixed point free, so is $A \times B$. The converse is also true if both A and B are characteristic subgroups of $A \times B$.*

Corollary 2.8. *If A is an abelian group of order $4k+2$, then A is not fixed point free.*

Proof. By the classification of finite abelian groups, A is a direct product of a group of order 2 and a group of order $2k+1$. Since both are characteristic subgroups of A, the assertion follows from Lemma 2.6 and Lemma 2.7. □

Corollary 2.9. *There are no connected Alexander quandles of order $4k+2$.*

For a finite abelian p-group A, the omega subgroups are defined to be the series of subgroups of A, indexed by the natural numbers as follows:

$$\Omega_i(A) = \{a \in A \mid a^{p^i} = 1\}$$

Since the Frattini subgroup $\Phi(A)$ of A is a characteristic subgroup of A, we may associate with each automorphism of A its induced action on the factor group $A/\Phi(A)$, and we have the natural homomorphism $\lambda : \mathrm{Aut}(A) \to \mathrm{Aut}(A/\Phi(A))$.

Let $A(p^m, n)$ be the direct product of n-copies of the cyclic group of order p^m; equivalently,

$$A(p^m, n) \cong \mathbb{Z}_{p^m} \times \cdots \times \mathbb{Z}_{p^m} \text{ (with } n \text{ factors)}$$

In particular, $A(p,n)$ denotes the elementary abelian p-group of order p^n.

Lemma 2.10. *For* $A = A(p^m, n)$,

(1) *the homomorphism* $\lambda : \mathrm{Aut}(A) \to \mathrm{Aut}(A/\Phi(A)) \cong \mathrm{GL}(n,p)$ *is surjective;*

(2) ϕ *in* $\mathrm{Aut}(A)$ *is fixed point free if and only if* $\lambda(\phi)$ *in* $\mathrm{Aut}(A/\Phi(A))$ *is fixed point free.*

Theorem 2.11. (Gross [2]) *Let* A *be an ableian* 2*-group isomorphic with* $A(2^{m_1}, n_1) \times A(2^{m_2}, n_2) \times \cdots \times A(2^{m_r}, n_r)$ *where* $0 < m_1 < m_2 < \cdots < m_r$. *Then* A *is fixed point free if and only if* $n_i \geq 2$ *for all* $i = 1, 2, ..., r$.

Proof. The *'if'* part follows from Lemma 2.6, Lemma 2.7 and Lemma 2.10.

For *'only if'* part, we simply denote $A_i = A(2^{m_i}, n_i)$, $H_i = \Omega_{m_i}(A)\Phi(A)$ for $i = 1, 2, ..., r$ and $H_0 = \Phi(A)$. We recall $A_i \cong \mathbb{Z}_{p^{m_i}} \times \cdots \times \mathbb{Z}_{p^{m_i}}$ (with n_i factors) for each $i = 1, 2, ..., r$, and $m_1 < m_2 < \cdots < m_r$. Then

1) $\Omega_{m_i}(A) \cong \Omega_{m_i}(A_1) \times \cdots \times \Omega_{m_i}(A_r)$, $\Phi(A) \cong \Phi(A_1) \times \cdots \times \Phi(A_r)$;

2) $\Omega_{m_i}(A_j) = P_j \supseteq \Phi(A_j)$ for $j \leq i$, $\Omega_{m_i}(A_j) \subseteq \Phi(A_j)$ for $j \geq i+1$.

Thus for each $i = 1, 2, ..., r$,

3) $H_i \cong A_1 \times \cdots \times A_{i-1} \times A_i \times \Phi(A_{i+1}) \times \cdots \times \Phi(A_r)$;

4) $H_{i-1} \cong A_1 \times \cdots \times A_{i-1} \times \Phi(A_i) \times \Phi(A_{i+1}) \times \cdots \times \Phi(A_r)$.

Consequently,

$$H_i/H_{i-1} \cong A_i/\Phi(A_i) \cong \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p \text{ (with } n_i \text{ summands)}$$

for all $i = 1, 2, ..., r$. Thus we have a proof of *'only if'* part from Lemma 2.6. □

Corollary 2.12. *For an abelian group* A *of order* 2^2, 2^3 *or* 2^5, A *is fixed point free if and only if* A *is elementary abelian.*

Proof. By the classification of finite abelian 2-groups, there are exactly following types of 2-groups with given orders:

$\mathbb{Z}_{2^2}$, $\mathbb{Z}_2^2$ of order 2^2,

$\mathbb{Z}_{2^3}$, $\mathbb{Z}_{2^2} \times \mathbb{Z}_2$, $\mathbb{Z}_2^3$ of order 2^3,

$\mathbb{Z}_{2^4} \times \mathbb{Z}_2$, $\mathbb{Z}_{2^3} \times \mathbb{Z}_{2^2}$, $\mathbb{Z}_{2^3} \times \mathbb{Z}_2^2$, $\mathbb{Z}_{2^2}^2 \times \mathbb{Z}_2$, $\mathbb{Z}_{2^2} \times \mathbb{Z}_2^3$, $\mathbb{Z}_2^5$ of order 2^5.

Thus if A are not elementary abelian, then A are not fixed point free by Theorem 2.11. □

3. Main results

The problem of classifying connected Alexander quandles of order 2^5 is boiled down to that of classfying conjugacy classes of fixed point free automorphisms of the elementary abelian group $A(2,5)$ of order 2^5.

Note that the automorphism group of the elementary abelian group of order p^n is isomorphic to $\mathrm{GL}(n,p)$, the general linear group of dimension n over the field $\mathbb{Z}_p$. Each element g of $\mathrm{GL}(n,p)$ affords a $\mathbb{Z}_p[t]$-module via the action on the vector space $V = \mathbb{Z}_p^n$ defined by $t\,v = g(v)$ for every v in V. The module is denoted by V_g, or V in short. We say that a $\mathbb{Z}_p[t]$-module is *singular* if $t\,v = 0$ for some non-zero vector v in V; otherwise, *nonsingular*.

It is well known that the conjugacy classes in $\mathrm{GL}(n,p)$ are therefore in one to one correspondence with the isomorphism classes of nonsingular $\mathbb{Z}_p[t]$-modules of dimension n.

We now enumerate the conjugacy classes in $\mathrm{GL}(n,p)$ in terms of the nonsingular $\mathbb{Z}_p[t]$-modules of dimension n up to isomorphism; the presentation is largely based on the treatment of [6].

A finite sequence $\lambda = (\lambda_1, \lambda_2, ..., \lambda_k)$ of positive integers such that $\lambda_1 \le \lambda_2 \le \cdots \le \lambda_k$ is said to be a *partition* of the integer $\sum_{i=1}^{k} \lambda_i$, which is denoted by $[\lambda]$. It is also convenient to consider the partition of zero as the sequence (0). We denote the set of partitions of nonnegative integers by P.

From the structure theorem for finitely generated modules over a principal ideal domain, we see that every nonsingular $\mathbb{Z}_p[t]$-modules V of dimension n is a direct sum of cyclic modules of the form $\mathbb{Z}_p[t]\,/(f^m)$ where m is a positive integer and f is an irreducible monic polynomial in $\mathbb{Z}_p[t]$.

Let Γ be the set of all irreducible monic polynomials in $\mathbb{Z}_p[t]$ with t being excluded. It follows that each f in Γ maps to a partition $\lambda(f)$ such that $\sum_{f\in\Gamma} [\lambda(f)] \deg(f) = n$, which yields a function from Γ into P.

On the other hand, for each f in Γ and a partition $\lambda = (\lambda_1, \lambda_2, ..., \lambda_k)$ in P, we can associate the $\mathbb{Z}_p[t]$-modules

$$W_{f,\lambda} = \bigoplus_{i=1}^{k} \mathbb{Z}_p[t]\,/\big(f^{\lambda_i}\big)$$

Note that $\dim_{\mathbb{Z}_p} W_{f,\lambda} = \sum_{i=1}^{k} \lambda_i \deg(f) = [\lambda] \deg(f)$.

Now taking mutually distinct irreducible polynomials f in Γ and a partition $\lambda(f)$ so that

$$\dim_{\mathbb{Z}_p} \left(\bigoplus_{f\in\Gamma} W_{f,\lambda(f)} \right) = \sum_{f\in\Gamma} [\lambda(f)] \deg(f) = n,$$

we have a nonsingular $\mathbb{Z}_p[t]$-module $V = \bigoplus_{f\in\Gamma} W_{f,\lambda(f)}$ of dimension n. It is also well known that the function from Γ into P which maps f to $\lambda(f)$ is an invariant of the isomorphism class of V.

Summing up the above discussion, we have:

Lemma 3.1. *Let P be the set of partitions of nonnegative integers. There exists a one-to-one correspondence between the conjugacy classes of* $\mathrm{GL}(n,p)$ *and the functions from Γ into P which map each $f \in \Gamma$ to a partition $\lambda(f) \in P$ such that $\sum_{f\in\Gamma} [\lambda(f)] \deg(f) = n$.*

Based upon Lemma 3.1, we can enumerate a rational canonical form corresponding to the decomposition: $V = \bigoplus_{f\in\Gamma} W_{f,\lambda(f)}$ with

$$W_{f,\lambda(f)} = \bigoplus_{i=1}^{k} \mathbb{Z}_p[t]\,/\big(f^{\lambda_i}\big)$$

where $\lambda(f) = (\lambda_1, \lambda_2, ..., \lambda_k)$ is a partition for each f in Γ such that

$$\sum_{f \in \Gamma} [\lambda(f)] \deg(f) = n.$$

Example 1. The rational canonical form

$$\begin{pmatrix} b & 1 & & & \\ & b & 1 & & \\ & & b & 1 & \\ & & & b & \\ & & & & c \end{pmatrix}$$

with b, c in $\mathbb{Z}_p^\times$ has the minimal polynomial $(t-b)^4(t-c)$ corresponding to the module $\mathbb{Z}_p[t] \big/ (t-b)^4 \oplus \mathbb{Z}_p[t]/(t-c)$.

Example 2. The rational canonical form

$$\begin{pmatrix} 0 & 1 & 0 & 1 & & \\ -b_0 & -b_1 & 0 & 0 & & \\ & & 0 & 1 & 0 & 1 \\ & & -b_0 & -b_1 & 0 & 0 \\ & & & & 0 & 1 \\ & & & & -b_0 & -b_1 \end{pmatrix}$$

has the minimal polynomial $(t^2 + b_1 t + b_0)^3$ corresponding to the module $\mathbb{Z}_p[t]/(t^2 + b_1 t + b_0)^3$ for an irreducible polynomial $t^2 + b_1 t + b_0$ in $\mathbb{Z}_p[t]$.

To count the number of irreducible polynomials of degree d in $\mathbb{Z}_p[t]$, we need the following well known result.

Lemma 3.2. *Let $I_p(d)$ is the number of irreducible polynomials of degree d in $\mathbb{Z}_p[t]$. Then*

$$p^n = \sum_{d|n} d\, I_p(d).$$

Example 3. If n is a prime then $I_p(n) = \frac{p^n - p}{n}$, since $p^n = I_p(1) + nI_p(n)$. The followings are a list of irreducible polynomials over Z_2 with degree 2, 3 and 5.

$$\begin{aligned} &t^2 + t + 1, t^3 + t^2 + 1,\ t^3 + t + 1, \\ &t^5 + t^4 + t^3 + t^2 + 1,\ t^5 + t^3 + t^2 + t + 1,\ t^5 + t^3 + 1, \\ &t^5 + t^4 + t^3 + t + 1,\ t^5 + t^2 + 1,\ t^5 + t^4 + t^2 + t + 1. \end{aligned}$$

Example 4. (1) $I_p(4) = \frac{p^4 - p^2}{4}$, since

$$p^4 = I_p(1) + 2I_p(2) + 4I_p(4) = p + (p^2 - p) + 4I_p(4).$$

(2) $I_p(6) = \frac{p^6-p^3-p^2+p}{6}$, since

$p^6 = I_p(1) + 2I_p(2) + 3I_p(3) + 6I_p(6) = p + (p^2 - p) + (p^3 - p) + 6I_p(6)$.

Lemma 3.3. *Among irreducible polynomial in $\mathbb{Z}_p[t]$ with degree n, the number of ways of choosing r polynomials allowing duplicate choices is* $\begin{pmatrix} I_p(n) + r - 1 \\ r \end{pmatrix}$.

Theorem 3.4. *There are exactly eight connected Alexander quandles of order 2^5. The associated Alexander modules are isomorphic to one of the following modules:*

$$\begin{array}{ll} \mathbb{Z}_2[t]\,/(t^3+t+1) \oplus \mathbb{Z}_2[t]\,/(t^2+t+1)\ , & \mathbb{Z}_2[t]\,/(t^5+t^4+t^3+t^2+1)\ , \\ \mathbb{Z}_2[t]\,/(t^3+t^2+1) \oplus \mathbb{Z}_2[t]\,/(t^2+t+1)\ , & \mathbb{Z}_2[t]\,/(t^5+t^3+t^2+t+1), \\ \mathbb{Z}_2[t]\,/(t^5+t^3+1)\ , & \mathbb{Z}_2[t]\,/(t^5+t^4+t^3+t+1)\ , \\ \mathbb{Z}_2[t]\,/(t^5+t^2+1)\ , & \mathbb{Z}_2[t]\,/(t^5+t^4+t^2+t+1). \end{array}$$

Proof. In Table 1, we have a list of rational canonical forms of $\mathrm{GL}(5,p)$. The completeness of enumeration can be checked by comparing the total number of rational canonical forms with $c_5 = p^5 - p^2 - p + 1$, given explicitly in [6]. One immediately realizes that for $p = 2$ rational canonical forms with linear factors in their minimal polynomials must have nontrivial fixed points because those linear factors are $t + 1$. Thus there are only two types of rational canonical forms with no linear factors:

$$A = \begin{pmatrix} 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \\ -b_0 & -b_1 & -b_2 & & \\ & & & 0 & 1 \\ & & & -c_0 & -c_1 \end{pmatrix}$$

where $t^3 + b_2t^2 + b_1t + b_0, t^2 + b_1t + b_0$ is irreducible in $\mathbb{Z}_2[t]$.

$$B = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ -b_0 & -b_1 & -b_2 & -b_3 & -b_4 \end{pmatrix}$$

where $t^5 + b_4t^4 + b_3t^3 + b_2t^2 + b_1t + b_0$ is irreducible in $\mathbb{Z}_2[t]$.

From the two rational canonical forms of type A we have the semisimple modules, and from the six rational canonical forms of type B we have the simple modules. Thus we have the assertion of the theorem from Corollary 2.12. □

Remark. In a website [11] maintained by M. Saito, the above 8 modules are described by polynomials of degree 5. Indeed we have following factorizations over $\mathbb{Z}_2$:

$$t^5 + t^4 + 1 = (t^3 + t + 1)(t^2 + t + 1),$$
$$t^5 + t + 1 = (t^3 + t^2 + 1)(t^2 + t + 1).$$

Thus we see that

$$\begin{aligned} C[32,16] &= \mathbb{Z}_2[t]/(t^5+t^4+1) \cong \mathbb{Z}_2[t]/(t^3+t+1) \oplus \mathbb{Z}_2[t]/(t^2+t+1), \\ C[32,17] &= \mathbb{Z}_2[t]/(t^5+t+1) \cong \mathbb{Z}_2[t]/(t^3+t^2+1) \oplus \mathbb{Z}_2[t]/(t^2+t+1). \end{aligned}$$

Table 1. Rational Canonical Forms of the conjugacy classes in $\mathrm{GL}(5,p)$

Canonical forms	Conditions	Number of classes
$\begin{pmatrix} b &&&& \\ & c &&& \\ && d && \\ &&& e & \\ &&&& f \end{pmatrix}$	$0 < b \le c \le d \le e \le f < p$	$\binom{(p-1)+5-1}{5}$
$\begin{pmatrix} b & 1 &&& \\ & b &&& \\ && c && \\ &&& d & \\ &&&& e \end{pmatrix}$	$b \in \mathbb{Z}_p^\times,\ 0 < c \le d \le e < p$	$(p-1)\binom{(p-1)+3-1}{3}$
$\begin{pmatrix} b & 1 &&& \\ & b &&& \\ && c & 1 & \\ &&& c & \\ &&&& d \end{pmatrix}$	$d \in \mathbb{Z}_p^\times,\ 0 < b \le c < p$	$\binom{(p-1)+2-1}{2}(p-1)$
$\begin{pmatrix} b & 1 &&& \\ & b & 1 && \\ && b && \\ &&& c & \\ &&&& d \end{pmatrix}$	$b \in \mathbb{Z}_p^\times,\ 0 < c \le d < p$	$(p-1)\binom{(p-1)+2-1}{2}$
$\begin{pmatrix} b & 1 &&& \\ & b & 1 && \\ && b && \\ &&& c & 1 \\ &&&& c \end{pmatrix}$	$b, c \in \mathbb{Z}_p^\times$	$(p-1)^2$
$\begin{pmatrix} b & 1 &&& \\ & b & 1 && \\ && b & 1 & \\ &&& b & \\ &&&& c \end{pmatrix}$	$b, c \in \mathbb{Z}_p^\times$	$(p-1)^2$
$\begin{pmatrix} b & 1 &&& \\ & b & 1 && \\ && b & 1 & \\ &&& b & 1 \\ &&&& b \end{pmatrix}$	$b \in \mathbb{Z}_p^\times$	$(p-1)$
$\begin{pmatrix} 0 & 1 &&& \\ -b_0 & -b_1 &&& \\ && c && \\ &&& d & \\ &&&& e \end{pmatrix}$	$t^2+b_1t+b_0$ irreducible in $\mathbb{Z}_p[t]$ $0 < c \le d \le e < p$	$\frac{p^2-p}{2}\binom{(p-1)+3-1}{3}$
$\begin{pmatrix} 0 & 1 &&& \\ -b_0 & -b_1 &&& \\ && c & 1 & \\ &&& c & \\ &&&& d \end{pmatrix}$	$t^2+b_1t+b_0$ irreducible in $\mathbb{Z}_p[t]$ $c, d \in \mathbb{Z}_p^\times$	$\frac{p^2-p}{2}(p-1)^2$
$\begin{pmatrix} 0 & 1 &&& \\ -b_0 & -b_1 &&& \\ && c & 1 & \\ &&& c & 1 \\ &&&& c \end{pmatrix}$	$t^2+b_1t+b_0$ irreducible in $\mathbb{Z}_p[t]$ $c \in \mathbb{Z}_p^\times$	$\frac{p^2-p}{2}(p-1)$

Canonical forms	Conditions	Number of classes
$\begin{pmatrix} 0 & 1 & & & \\ -b_0 & -b_1 & & & \\ & & 0 & 1 & \\ & & -c_0 & -c_1 & \\ & & & & d \end{pmatrix}$	$t^2+b_1t+b_0$ irreducible in $\mathbb{Z}_p[t]$ $t^2+c_1t+c_0$ irreducible in $\mathbb{Z}_p[t]$ $(b_1, b_0) \leq (c_1, c_0)$ in lexicographic order $d \in \mathbb{Z}_p^\times$	$\binom{\frac{1}{2}(p^2-p)+1}{2}(p-1)$
$\begin{pmatrix} 0 & 1 & 0 & 1 & \\ -b_0 & -b_1 & 0 & 0 & \\ & & 0 & 1 & \\ & & -b_0 & -b_1 & \\ & & & & c \end{pmatrix}$	$t^2+b_1t+b_0$ irreducible in $\mathbb{Z}_p[t]$ $c \in \mathbb{Z}_p^\times$	$\frac{p^2-p}{2}(p-1)$
$\begin{pmatrix} 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \\ -b_0 & -b_1 & -b_2 & & \\ & & & c & \\ & & & & d \end{pmatrix}$	$t^3+b_2t^2+b_1t+b_0$ irreducible in $\mathbb{Z}_p[t]$ $0 < c \leq d < p$	$\frac{p^3-p}{3}\binom{(p-1)+2-1}{2}$
$\begin{pmatrix} 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \\ -b_0 & -b_1 & -b_2 & & \\ & & & c & 1 \\ & & & & c \end{pmatrix}$	$t^3+b_2t^2+b_1t+b_0$ irreducible in $\mathbb{Z}_p[t]$ $c \in \mathbb{Z}_p^\times$	$\frac{p^3-p}{3}(p-1)$
$\begin{pmatrix} 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \\ -b_0 & -b_1 & -b_2 & & \\ & & & 0 & 1 \\ & & & -c_0 & -c_1 \end{pmatrix}$	$t^3+b_2t^2+b_1t+b_0$ irreducible in $\mathbb{Z}_p[t]$ $t^2+c_1t+c_0$ irreducible in $\mathbb{Z}_p[t]$	$\frac{p^3-p}{3}\frac{p^2-p}{2}$
$\begin{pmatrix} 0 & 1 & 0 & 0 & \\ 0 & 0 & 1 & 0 & \\ 0 & 0 & 0 & 1 & \\ -b_0 & -b_1 & -b_2 & -b_3 & \\ & & & & c \end{pmatrix}$	$t^4+b_3t^3+b_2t^2+b_1t+b_0$ irreducible in $\mathbb{Z}_p[t]$ $c \in \mathbb{Z}_p^\times$	$\frac{p^4-p^2}{4}(p-1)$
$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ -b_0 & -b_1 & -b_2 & -b_3 & -b_4 \end{pmatrix}$	$t^5+b_4t^4+b_3t^3+b_2t^2+b_1t+b_0$ irreducible in $\mathbb{Z}_p[t]$	$\frac{p^5-p}{5}$

References

[1] M. Grãna, *Indecomposable racks of order p^2*, Beiträge Algebra Geom. **45** (2004), 665-676.

[2] F. Gross, *Some remarks on groups admitting a fixed-point-free automorphism*, Canad. J. Math. **20** (1968), 1300-1307.

[3] X.-D. Hou, *Finite modules over* $\mathbb{Z}[t, t^-1]$, J. Knot Theory Ramifications **22** (2013), 37-65.

[4] D. Joice, *A classifying invariants of knots, the knot quandles*, J. Pure Appl. Alg. **23** (1982), 37-65.

[5] T. Kepka and P. Nemec, *Commutative Moufang loops and distributive groupoids of small orders*, Czechoslovak Math. J. **31(106)** (1981), no. 4, 633-669.

[6] I. G. Macdonald, *Numbers of conjugacy classes in some finite classical groups*, Bull. Austral. Math. Soc. **23** (1981), 23-48.

[7] G. Murillo and S. Nelson, *Alexander quandles of order 16*, J. Knot Theory Ramifications **17** (2008), 273-278.

[8] G. Murillo and S. Nelson, *Erratum: Alexander quandles of order 16*, J. Knot Theory Ramifications **18** (2009), 727.

[9] S. Nelson, *Classification of finite Alexander quandles*. Proceedings of the Spring Topology and Dynamic Systems Conference. Topology Proc. **27** (2003), no. 1, 245-258.
[10] T. Ohtsuki, (ed.) *Problems on Invariants in Knots and 3-Manifolds*, Geom. Topol. Monogr. **4** 377-572.
[11] M. Saito, *Characteization of small connected quandles*, Nov. 23, 2013, http://shell.cas.usf.edu/~saito/QuandleColor/characterization.pdf. Maintained by M. Saito
[12] J.-P. Soublin, *Etude algebique de la notion de moyenne(suite et fin)*, J. Math. Pures Appl.(9) **50** (1971), 193-264.
[13] S. Stein, *On the foundations of quasigroups*, Trans. Amer. Math. Soc. **85** (1957) 228-256.
[14] D. S. Siver and S.G. Williams, *Generalized n-colorings of links*, Knot Theory (in Banach Center Publications) **42** (1998), 381-394.
[15] K. Toyoda, *On axioms of linear functions*, Proc. Imp. Acad. Tokyo **17** (1941), 221-227.

Hyo-Seob Sim
Department of Applied Mathematics, Pukyong National University, Pusan 608-737, Korea
E-mail address: hsim@pknu.ac.kr

Hyun-Jong Song
Department of Applied Mathematics, Pukyong National University, Pusan 608-737, Korea
E-mail address: hjsong@pknu.ac.kr