Global Scientific JOURNALS

GSJ: Volume 8, Issue 10, October 2020, Online: ISSN 2320-9186
www.globalscientificjournal.com

# ON THE CLASSIFICATION OF ORDER p LATIN QUANDLES

Ezurike Julia Ugochi [1], Ononogbo Benjamin Chibuike [2]

[1,2](Department of Mathematics, Ambrose Alli University Ekpoma, Nigeria.)

**ABSTRACT:**

Latin quandles are special subclass of finite quandles. In this paper, we study Latin quandles of order p (prime) and of cyclic type. The set of isomorphism classes of Latin quandles are described in the result of this paper through which we gave a classification of Latin quandles of cyclic type of order p; $p \leq 13$.



## I. INTRODUCTION

The work of Joyce and Matveev put the foundation for the modern theory of quandles, which covers, to some extent, many traditional aspects of self-distributive as a special case ( self-distributive quasigroups, or Latin quandles, in particular)[16].

Quandles are strictly non-associative binary algebras that are idempotent and distributive. However, the notion of self-distributive binary algebra is not new in literature. It appears with many different names [3], and [4]. One of the earliest examples is the work of [2].

Since then, different authors at different times have helped to develop this notion either in part or whole. For example [5], called this notion Kei. Today, Kei has been understood as Involutory quandle. [6] Acknowledge that several authors have worked on self distributive systems and distributive quasigroups respectively. The later has become known as Latin quandle in present terminology. In this paper, we will be focusing more on Latin quandles especially of cyclic type. This brief review shows that there are many examples of quandles. What makes quandles

popular in literature is that they provide several invariants of knots, especially the class of connected quandles [6]. It is less surprising, therefore that researchers pay more attention to connected quandles. However, all Latin quandles are connected quandles but not all connected quandles are Latin quandles. [7], describes the set of isomorphism classes of quandles of cyclic type with cardinality up to 12 in terms of cyclic permutation. A quandle with cardinality n is said to be a cyclic type if all right multiplication are cyclic permutations of order n-1. Since this quandle structure is very tractable. Latin quandles of cyclic type are potentially useful for applications in knot theory and cryptography. Many researchers have done a great deal of work on Latin quandles, worthy of note are, [8], studied quandle of cyclic type, which they called quandles of constant profile ({1, n-1}, …, {1,n-1}). They studied such quandles in terms of cyclic permutation, and classify those with cardinality up to 8. In addition, [15] studied structures of quandles of cyclic type and gave a table of those with cardinality up to 35. Note that his table is obtained by using the list of connected quandle with cardinality up to 35 ( Vendramin's list of indecomposable quandles). From this point of view we study Latin quandles of order P (where P is a prime number). The classes of quandles are not only connected quandles but are also having symmetric and less complicated structures which made it a special subclass of finite quandles that is very fruitful in many areas of applications such as cryptography. All quandles of cyclic type with one *fixed point* are Latin quandles but all Latin quandles are not quandles of cyclic type.[12]. Therefore, Latin quandles are a generalization of quandles of cyclic type. In particular, for every prime number $p \geq 3$, there exists a quandle of cyclic type with cardinality P. This suggests that the classes of quandles of cyclic type is fruitful. In this paper, we study and describe Latin quandles with cardinality P and of cyclic type. However, our main theorem gives a bijection from $X_n$ onto $\mathrm{Q}_n$ when $\mathrm{Q}_n$ denotes the set of cyclic permutations of order n-1 satisfying two conditions. This bijection is useful for studying Latin quandles of cyclic type since the Latin quandles can be characterized by certain cyclic permutations. Therefore, we apply our

main theorem to the classification of quandles of cyclic type and provide a list of those with cardinality up to 13. Our study extend some results by [11], [12] and [1]. Our new contribution sequel to Kamada's, is Latin quandles application to cryptography. The paper is organized as follows; in Section 2 we recall some fundamental notions on quandles. In Section 3, the definition and some properties of quandles of cyclic type are summarized. In section 4 we stated the main theorem and give table of quandles of cyclic type of order p≤ 13. Section 5 contains the proof of the main theorem. For the purpose of clarity we define the following.

## II. PRELIMINARIES

We briefly review some definitions and examples of quandles.

**Definition 2.1:** [13], [1]; A quandle $(X,*)$ is a set with a binary operation $(a,b)\to a*b$ satisfying the following conditions

(1). For any $a\in X$ , a ∗ a = a

(2). for any $b,c\in X$ ,there is a unique $a\in X$ such that a ∗ $b$ = c

(3). for any $a,b,c\in X$, we have $(a*b)*c=(a*c)*(b*c)$

If $(X,*)$ is a quandle then $*$ is called quandle structure on X. we restate the definition of quandle of quandle as follows

**Proposition 2.1 :** [11], let X be a set , and assume that there exist a map $s_x : X\to X$ for every x ∈ $X$. then, the binary operation $*$ defined by $y*x:=s_x(y)$ is a quandle structure on X if and only if

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

Instead of definition 2.1, throughout this paper, we denote the quandle by $X=(Q,s)$ with the quandle structure

$s: Q\to Map(Q,Q): x\mapsto s_x$ Here Map (Q,Q) denotes the set of all maps from Q to Q

**Example 2.3:** [11] and [1], the following (Q, s) are quandles:

Let Q be any set and $s_x := id_q$ for every q ∈ Q. then the pair (Q,s) is called the trival quandle.

(1) Let $Q := \{1,...n\}$ and $s_i(j) := 2i - j \pmod n$ for any i,j ∈ Q. then the pair (Q,s) is called the dihedral quandle with cardinality n

(2) Let $Q := \{1,2,3,4,5\}$ and $s_1 := (2354), s_2 := (1534), s_3 := (1452), s_4 := (1325), s_5 := (1243)$. then the pair (Q,s) is called pentahedron quandle ( Latin quandle of order 5). Note that (2354), (1534), and this symbol regularly in the later sections.

(3) All quandle of prime order are connected and are cyclic type must be connected.

**Remark 2.1:** property (1) implies that every element in a quandle has self identity, and inverse elements are general not unique in quandles.

**Definition 2.2:** [12], An involutory quandle is a quandle which satisfies $(a * b) * b = a$

**Remark 2.2:** Any involutory quandles X is also called kei, particularly if the right translations are involutions: $R_a^2 = id$ for all $a \in X$ .

Joyce reported a class of quandles in which the symmetries S(y) are all involutions. For this class of quandle the two operations in a quandle coincide.

**Definition 2.3: J.** [14], let $(Q, s^X), (X, s^Y)$ be quandles and $f : Q \to X$ be a map.

(1) f is called a homomorphism if for every $x \in Q$, $f \circ s_x^X = s_{f(x)}^X \circ f$ holds.

(2) f is called an isomorphism if is a bijective homomorphism.

An isomorphism from a quandle (Q, s) onto itself is called an automorphism. The set of automorphisms of (Q, s) forms a group, which is called the automorphism group and denoted by Aut (Q,s). Note that $s_x (x \in Q)$ is an automorphism of (Q,s). the subgroup of Aut (Q,s) generated by $\{s_x \mid x \in Q\}$ is called the inner automorphism group of (Q,s) and denoted by Inn(Q,s).

**Definition 2.4.** A quandle (Q,s) is said to be connected if Inn(Q,s) acts transitively on X.

On the connectedness of the quandles in Example 2.3.the following is well-known. We denoted by #Q the cardinality of Q

**Example 2.6.** One has the following:

(1) The trivial quandle (Q,s) is connected if and only if #Q=1.
(2) The dihedral quandle (Q,s) is connected if and only if #Q is odd.
(3) The pentahedron quandle is connected
(4) The Latin quandle of prime order is cyclic type.

## III. QUANDLES OF CYCLIC TYPE

**Definition 3.1** [15], A quandle (Q, s) with $\#Q = n \geq 3$ is said to be cyclic type if for every $Q, s_x$ acts on $Q \setminus \{x\}$ as a cyclic permutation of order n-1. This notion is closely related to the notion of

two-point homogeneous quandle. A quandle (Q,s) is said to be two-point homogeneous if for any $(x_1, x_2), (y_1, y_2) \in Q \times Q$ satisfying $x_1 \neq x_2$ *and* $y_1 \neq y_2$, there exist $f \in Inn(Q,s)$ such that $(f(x_1), f(x_2)) = (y_1, y_2)$

The second author studied quandles of cyclic type in [15] because of the following proposition.

**Proposition 3.1** [15], every quandle of cyclic type is two-point homogeneous. The following is a characterization of quandles of cyclic type, which we use in the latter arguments. In particular, quandles of cyclic type must be connected.

**Proposition 3.2** [15], let $Q = (Q, s)$ be a quandle with $\#Q = n \geq 3$. then, X is of cyclic type if and only if

(i) Q is connected, and
(ii) There exist $q \in Q$ such $s_x$ acts on $Q \setminus \{x\}$ as a cyclic permutation of order n-1.

## IV. MAIN THEOREM

If the structure of a quandle is given, then one can easily check whether it is of cyclic type or not. We here give some easy examples.

**Example 3.3** we have the following;

(1) The trivial quandles are not of cyclic type
(2) The dihedral quandle (Q,s) is of cyclic type if and only if #X= 3.
(3) The pentahedron quandle is of cyclic type
(4) The Latin quandle of prime order 13 is cyclic type.



In this section, we state our main theorem, and give a table of quandles of cyclic type with cardinality 13. The following notations will be used throughout the remaining of this paper;

- ✓ $Q := \{1, 2, ..., n\}$ with $n \geq 3$
- ✓ $S_n$ denoted the symmetry group of order n.
- ✓ $(S_n)_{n-1} := \{\sigma \in S_n | \sigma$ is a cyclic permutation of order n-1$\}$.

**Definition 4.1** [11], we denote by $C_n^{\#}$ the set of all quandles structures of cyclic type on Q that is

$C_n^{\#} := \{s : Q \to (S_n)_{n-1} | s$ satistfies (S1),(S3)$\}$ (Note that every $s \in C_n^{\#}$ automatically satisfies (S2). We denoted by $C_n$ to the set of isomorphism classes of quandles of cyclic type with cardinality n.

**Definition 4.2**[11], let $S_1 := (23...n)$ we denote by $Q_n$ *the* set of $S_2 \in (S_n)_{n-1}$ satisfying the following two conditions:
$(Q1)$ $S_2(2) = 2$ and
$(Q2)$ $\{S_m S_m S_r^{-1} S_m | m = 2, 3...n, r = 1, 2...n-1\} = \{S_m S_m S_r^{-1} S_m | m = 2, 3...n, r = 1, 2...n-1\}$

Recall that (23...n) denotes the cyclic permutation. The following is the main theorem of this paper which gives a one-to-one correspondence between $C_n$ *and* $Q_n$

**Theorem 4.1**

Let $S_1 := (2\,3\,...n)$, $S_2 \in Q_n$ *and define* $\varphi(S_2) : Q \to Map(Q, Q)$ *by*

$$\left(\varphi\left(S_2\right)\right)_i := \begin{cases} S_1 & i = 1 \\ S_2 & i = 2 \\ S_2 S_1^{-1} S_2 = S_3 & \end{cases}$$ Then we have $\varphi\left(S_2\right) \in C_n^{\#}$, *and* hence give a Map $\varphi : Q_n \to C_n^{\#}$.

This induces from $Q_n$ *onto* $C_n$

**Proposition 4.2** recall that $Q_n = \{(13)\}$ *and* $Q_5 = \{(15\,3\,4)\}$

**Proof:** The basic strategy is the following. First of all, we list up all elements in $(S_n)_{n-1}$ satisfying (Q1). These elements are called the members for clarity we then check whether each member satisfies (Q2) or not in these case of n = 3. In the case of n = 3 , the only member is $S_2 = (13)$.

$S_2 S_1^{-1} S_2 = (12) = S_1 S_2^{-1} S_1$ . Hence $S_2$, satisfies $Q_2$. This proves the first assertion.

**Proposition 4.3** we have $Q_5 = \{(1534), (1435)\}$

**Proof:** there are six members as for the set of $Q_5$;

$S_2 = (1345), (1354), (1543), (1435), (1534), (1453)$ One can observe that $(1534)$ and $(1435)$ satisfy Q2. We omit proof for the two cases. Therefore we show that the remaining four members do not satisfy (Q2).

Case (1); $S_2 := (1345)$, $S_1 = (2354)$ let m= -1 therefore $(1345); (1253 \neq 1432)$ $S_2 S_1^{-m} S_2 \neq S_1 S_2^{-m} S_1$

Case (2); $S_2 = (1354)$; *let* $m = -1$

$(1243) \neq (1532)$ ; $S_2 S_1^{-m} S_2 \neq S_1 S_2^{-m} S_1$

Case (3); $S_2 = (1543)$;

$(1532 \neq 2345)$ ; $S_2 S_1^{-1} S_2 \neq S_1 S_2^{-1} S_1$

Case (4); $S_2 = (1453)$

$(1235 \neq 1342)$; $S_2 S_1^{-1} S_2 \neq S_1 S_2^{-1} S_1$

This completes the proof of second assertion. When n = 3 the Latin quandles corresponding to $S_2 := (13)$ is the dihedral quandles with cardinality 3 (prime). When n = 5 , the Latin quandles corresponding to $S_2 = \{(1534),(1435)\}$ is pentahedron quandles. When $n \geq 5$; $n = p$ (prime) .

Lemma the following Lemma is useful to examine whether each cardinality satisfies (Q2) or not

**Lemma 4.1** [11], $S_2 \in Q_n$ and m=-1 satisfies $S_1^{-m} = S_2^{-l}$ then we have $S_2 S_1^{-m} S_2 = S_1 S_2^{-l} S_1$

**Proof:** since $Q_n = \{1, 2, ..., n-2\}$ *and* $S_2 \in Q_n$ satisfies (Q2) there exist $l \in \mathbf{Z}$ such that $l$= m then $S_2 S_1^{-m} S_2 = S_1 S_2^{-l} S_1$ .

Note that $S_2 S_1^{-m} S_2$ is a cyclic permutation of order n- 1, having the imagined fixed point $S_1^{-m}(2)$ similarly, $S_1 S_2^{-l} S_1$ has the imagine fixed point $S_2^{-l}(1)$. Hence combining with the assumption, one has $S_2(1) = S_2^{-m}(2) = S_2^{-l}(1)$

Since $S_2 \in (S_n)_{n-1}$ and it satisfies (Q1), we conclude $l = -1$ this completes the proof.

The above lemma is useful to determine the set $Q_n$ for any n = p ( prime). here we apply it to case of $n = 13$.

**Proposition 4.4** we have $Q_{13} = \begin{Bmatrix} (1\,9\,5\,7\,6\,13\,3\,8\,12\,10\,11\,4), (1\,8\,5\,10\,6\,4\,3\,9\,12\,7\,11\,13), \\ (1\,13\,11\,7\,12\,9\,3\,4\,6\,10\,5\,8), (1\,4\,11\,10\,12\,8\,3\,13\,6\,7\,5\,9) \end{Bmatrix}$

**Proof:** As for the set $Q_{13}$, there are four members. $S_{2=;}$ (1 9 5 7 6 13 3 8 12 10 11 4), (1 8 5 10 6 4 3 9 12 7 11 13), (1 13 11 7 12 9 3 4 6 10 5 8), (1 4 11 10 12 8 3 13 6 7 5 9) One can directly see that all four members satisfy (Q2). That ends the proof.

| N | $\#Q$ | $Q_n$ |
|---|---|---|
| 2 | 0 | 0 |
| 3 | 1 | $\{(13)\}$ |
| 5 | 2 | $\{(1534),(1435)\}$ |
| 7 | 2 | $\{(167354),(145376)\}$ |
| 11 | 4 | $\begin{Bmatrix} (111\,9\,5\,8\,3\,4\,6\,10\,7), (17\,10\,6\,4\,3\,8\,5\,9\,11), (1\,5\,4\,7\,9\,3\,10\,11\,8\,6), \\ (1\,6\,8\,11\,10\,3\,9\,7\,4\,5) \end{Bmatrix}$ |
| 13 | 4 | $\begin{Bmatrix} (1\,9\,5\,7\,6\,13\,3\,8\,12\,10\,11\,4), (1\,8\,5\,10\,6\,4\,3\,9\,12\,7\,11\,13), \\ (1\,13\,11\,7\,12\,9\,3\,4\,6\,10\,5\,8), (1\,4\,11\,10\,12\,8\,3\,13\,6\,7\,5\,9) \end{Bmatrix}$ |

**Table 1: Latin Quandles of cyclic type with prime cardinality up to 13**

The results are summarized in table 1, which gives a classification of Latin quandles of cyclic type with prime cardinality up to 13. Then note that $\#Q_n$ denotes the cardinality of $Q_n$ we note that table 1 agrees with some previous known results [11], [8]and[11]. By looking at the classification we conjecture the following,

**Conjecture 4.5:** let $n \geq 3$ then there exist a Latin quandles of cyclic type if and only if n is a power of a prime number.

## V. PROOF OF THE MAIN THEOREM

In this section we proof theorem 4.1, which gives a bijection from $Q_n$ onto $C_n$.

**Proof :**

For this proof, we define auxiliary sets $P_n$ and $R_n$, then we constructed bijections

$$g_3 : Q_n \to P_n \text{ , } g_2 : P_n, \; g_1 : R_n \to C_n \qquad (5.1)$$

In this subjection, we define a set $R_n$ and constructed bijection from on to $R_n$ onto $C_n$ (5.1) is a bijection from $R_n$ onto $C_n$ . Recall that $Q := \{1,...,n\}$, *and* $(S_n)_{n-1}$ is the subset of $S_n$ consisting of all cyclic permutations of order n-1.

Two subsets $\omega, \omega' \subset S_n$ are said to be conjugate if there exists $g \in S_n$ such that $g^{-1}\omega g = \omega^{-1}$.

**Definition 5.1** we denoted by $R_n^{\#}$ the set of $\omega \subset (S_n)_{n-1}$ satisfying

$(R1) \forall s \in \omega, S^{-1}\omega s \subset \omega,$ *and*

$(R2) \forall x \in Q;$ *there exist* $s \in \omega \; s(x) = x$

We also denoted by $R_n$ the set of conjugate classes $[\omega]$ of $\omega \in R_n^{\#}$. Firstly we study $R_n^{\#}$. Note that condition (R1) and (R2) are presented by conjugation. Namely; if $\omega \in R_n^{\#}$ and is conjugate o $\omega'$, then one has $\omega' \in R_n^{\#}$. Therefore, the following lemma yields that every $\omega \in R_n^{\#}$ satisfies $\#\omega = n$

**Lemma 5.2 Let** $\omega \in R_n^{\#}$ . for each $x \in Q,$ denote by $S_x^w \in \omega$ the unique element with $S_x^w(x) = x.$ Then, the obtained map $S^{\omega}; \; Q \to \omega$ is bijective.

**Proof**

We show that $S^w$ is surjective. Take any $S \in \omega$. Since $s \in (S_n)_{n-1}$, there exist $x \in Q$ such that $S(x) = x$ by definition. Thus x is the unique fixed point of $S_x^w \in (S_n)_{n-1}$. Similarly, y is the unique fixed point of $S_y^w$. This concludes x = y

**Lemma 5.3** the above defined map $S^\omega \circ Q \to (S_n)_{n-1}$ satisfies $S^\omega \in C_n^\#$, that is $(Q, S^\omega)$ is a Latin quandles of cyclic type.

**Proof:**

By definition $S^\omega$ Satisfies (S1). Hence we have only to show (S3). Take any $x, y \in Q$. Condition (R1) yields

$$S_y^w (S_x^\omega)^{-1} \circ S_y^w \in \omega \tag{5.2}$$

$$S_y^w \circ (S_x^\omega)^{-1} \circ S_y^\omega (S_x^\omega (y)) = S_y^\omega \circ S_x^\omega (y) = S_y^\omega (x) \tag{5.3}$$

Therefore from the uniqueness in (R2), we have;

$$S_y^w \circ (S_x^\omega)^{-1} \circ S_y^\omega = S^\omega (S_x^\omega (y))^{-1} = S^\omega_{s_x^\omega (y)} \tag{5.4}$$

This proves (S3). This completes the proof.

**Lemma 5.4: The following map is surjective**

$$\bar{g}_1 : R_n^\# \to C_n^\# : \omega \to S^\omega$$

**Proof:**

Take any $S \in C_n^\#$. let us put

$$\omega := \{ s_x \mid x \in Q \} \subset (S_n)_{n-1} \tag{5.5}$$

We prove that $\omega \in R_n^\#$ *and* $\bar{g}_1(\omega) = s$

We show that $\omega$ satisfies (R1). Take any $s_x, s_y \in \omega$ since $s_x^{-1}$ is an automorphism, one has

$$s_x \circ s_y^{-1} \circ s_x = S_{S_y^{-1}}(x) \in \omega \tag{5.6}$$

This proves $S_y^{-1} \omega s_y \subset \omega$

Next we show that $\omega$ satisfies (R2). Take any $x \in Q$. Since s satisfies (S1), $s_x \in \omega$ *satisfies* $s_x(x) = x$. Since $s \in C_n^{\#}$, one has $s_y \in (S_n)_{n-1}$.hence x is the unique fixed point of $s_y$. Thus (S1) yields that x = y which proves the uniqueness. By definition of $\bar{g}_1$, it is obvious to see that $\bar{g}_1(\omega) = s$ this completes the proof.

**Lemma 5.5** the following map is well-defined;

$g_1 : R_n \to C_n : [\omega] \to [s^{\omega}]$

**Proof:**

Let $\omega, \omega' \in R_n^{\#}$, and assume that $[\omega] = [\omega']$. Hence there exists $g \in S_n$ such that $\omega = g^{-1}\omega^{-1}g$. In order to show $[S^{\omega}] = [S^{\omega'}]$, it is enough to prove that the following map is a quandles Isomorphism;

$g : (Q, S^{\omega}) \to (Q, S^{\omega'})$ This is obvious bijective. We show that g is a quandles homomorphism. Take any $x \in Q$. By definition, one has

$$S^{\omega'}_{g(x)}(g(x)) = g(x) \tag{5.8}$$

This means that

$$S^{\omega'}_{y(x)} \circ g^{-1} \circ S^{\omega}_{y(x)} = x \tag{5.9}$$

on the other hand one has

$$S^{\omega'}_{y(x)} \circ g^{-1} \circ g \in \omega g^{-1} g = \omega \tag{5.10}$$

Hence , from the uniqueness in (R2). We have

$$S^{\omega'}_{g(x)} \circ g^{-1} g = S^{\omega}_{x} \tag{5.11}$$

This proves that g is a quandles homomorphism. We now show that the above defined map $g_1$ is bijective. The following is the main result of this subsection.

**Proposition 5.6** The map $g1 : R_n \to C_n$ is bijective

**Proof:**

Recall that g1 is surjective, since, so is $\bar{g}1$ from lemma (5.4). it remains to show that g1 is injective. Let $[\omega],[\omega'] \in R_n$, and assume that $([\omega]) = g1([\omega])$. By definition, one has $[S^{\omega}] = [S^{\omega'}]$, that is there exist a quandles isomorphism.

$$g : (Q , S^{\omega'}) \to (Q , S^{\omega'}) \tag{5.12}$$

Since g is bijective, we have $g \in S_n$. Since g is a homomorphism, we have for any $x \in Q$ that

$$S_x^{\omega} = S_{y(x)}^{\omega} \circ g^{-1} \circ S_{y(x)}^{\omega}(x) \in \omega' g^{-1} \omega \tag{5.13}$$

this proves $\omega \subset \omega' g^{-1} g$. Recall that $\#\omega = n = \#\omega'$ holds from lemma 5.2. therefore, we have $\omega = \omega g^{-1} g$, and thus $[\omega] = [\omega']$. this concludes that g1 is injective. (5.2) is a bijection from $P_n$ onto $R_n$. We denoted by

$$S_n, (1,2) := \{u \in S_n \mid u(1) = 1, u(2) = 2\} \tag{5.14}$$

two elements $(u_1, u_2), (v_1, v_2) \in (S_n)_{n-1} \times (S_n)_{n-1}$ are said to be $S_n, (1,2)-$ conjugate if $(u_1, u_2) = (\lambda^{-1} v_1 \lambda, \lambda^{-1} v_2 \lambda)$ for some $\lambda \in S_n(1,2)$.

**Definition 5.7** we denote by $P_n^{\#}$ the set of $(u_1, u_2) \in (S_n)_{n-1} \times (S_n)_{n-1}$ satisfying.

(P1) $u_1(1) = 1, u_2(2) = 2$ and
(P2) $\{u_2 u_1^{-1} u_2\} = \{u_1 u_2^{-1} u_1\}$

We also denote by $p_n$ the set of $S_n(1,2)-$ conjugacy classes $[(u_1, u_2)]$ of $(u_1, u_2) \in P_n^{\#}$ firstly of all, we construct a map from $P_n^{\#}$ to $R_n^{\#}$.

**Lemma 5.8:** let $(u_1, u_2) \in P_n^{\#}$. Then one has

$$\omega_{(u_1,u_2)} := \{u_1, u_2\} \cup \{u_2 u_1^{-1} u_2\} \in R_n \tag{5.15}$$

**Proof :**

we need to show that $\omega_{(u_1,u_2)}$ satisfies (R1) and (R2). In order to show (R1), it is enough to prove

$$u_2 \omega_{(u_1,u_2)} u_2 \subset \omega_{(u_1,u_2)}, u^{-1} \omega_{(u_1,u_2)} u_1 \subset \omega_{(u_1,u_2)} \tag{5.16}$$

Note that $u_1$ has order n-1. Then one has

$$u_1 u_1^{-1} u_1 = u_1 \in \omega_{(u_1,u_2)}$$

$$u_2 u_1^{-1} u_2 = u_1 u_2^{-1} u_1 \in \omega_{(u_1,u_2)} \tag{5.17}$$

This proves (5.16) and (P2) yield that

$$\omega_{(u_1,u_2)} = \{u_1, u_2\} \cup \{u_2 u_1^{-1} u_2\} \tag{5.18}$$

Next (R2). Take any $x \in Q.$ *if* $x = 1,2,$ then it is fixed by $u_1, u_2 \in \omega_{(u_1,u_2)}$, respectively. Assume $x \neq 1,2,$ by (P1) and $u_1 \in (S_n)_{n-1}$, there exists -1 such that $x = u_1^{-1}(2).$ then one has

$$u_2 u_1^{-1} u_2(x) = u_2 u_1^{-1} u_2(u_2(1)) = u_2 u_1^{-1}(1) = u_1^{-1}(2) = x \tag{5.19}$$

This completes the proof of the existence. On the other hand, by definition, one has $\#\omega_{(u_1,u_2)} \leq n$.

This shows the uniqueness.

**Lemma 5.9:** the following map is defined

$$g2 : p_n \to R_n : [(u_1, u_2)] \to [\omega_{(u_1,u_2)}]$$

**Proof:** let $\left[(u_1, u_2)\right], \left[\left(u_1^{'}, u_2^{'}\right)\right] \in p_n$ and assume that $\left[(u_1, u_2)\right] = \left[\left(u_1^{'}, u_2^{'}\right)\right]$, then there exist $\lambda \in S_{n,(1,2)}$ such that

$$u_1 = u_1^{'} \lambda^{-1} \lambda \ , \ u_2 = u_2^{'} \lambda^{-1} \lambda \tag{5.20}$$

$$w_{(u_1,u_2)} \lambda^{-1} \lambda = w_{(u_1,u_2)} \tag{5.21}$$

Since $w_{\left(u_1^{'}, u_2^{'}\right)}, w_{(u_1,u_2)} \in R_n^{\#},$ hence $\#w_{\left(u_1^{'}, u_2^{'}\right)} = n = w_{(u_1,u_2)}$ by lemma (5.2). this complete the proof of $\left[w_{(u_1,u_2)}\right] = \left[w_{\left(u_1^{'}, u_2^{'}\right)}\right]$

Next we need to prove that g2 is bijective by constructing inverse map from $R_n^{\#}$ *to* $P_n^{\#}$. Recall that

$$g1 : R_n^{\#} \to C_n^{\#} \ ; w \to S^w \tag{5.22}$$

**Lemma 5.10:** Let $w \in R_n^{\#}$ then one has $\left(s_1^w, s_2^w\right) \in P_n$

**Proof:** we put $s_x := s_x^w$ for which $x \in Q$ by definition, $(s_1, s_2)$ obviously satisfies $(P1)$ we need to show $(P1)$

Firstly we claim that

$$\left\{s_2 s_1^{-1} s_2\right\} = \left\{s_x \middle| x = 3,4,...n\right\} \tag{5.23}$$

Since w satisfies $(R1)$ we have

$$s_2 s_1^{-1} s_2 = s_2 w s_2^{-1} \subset w \tag{5.24}$$

Thus, it follows from $s_2 s_1^{-1} s_2 (s_2(1)) = s_2(1)$ and the uniqueness in $(R2)$ *that*

$$s_2 s_1^{-1} s_2 = S_{s_2}(1) \tag{5.25}$$

Since $s_2(1) = 1$ *and* $s_2 \in (s_n)_{n-1}$ *then*

$$\left\{s_2(2)\right\} = \left\{3,4,...,n\right\} \tag{5.26}$$

This completes the proof of the claim. The above lemma gives a map from $R_n^{\#}$ *to* $P_n^{\#}$. Next is to show that the map induces a map from $R_n$ *to* $P_n$

**Lemma 5.11:** The following map is well-defined;

$$f_2 : R_n \to P_n : [w] \to \left[\left(s_1^w, s_2^w\right)\right] \tag{5.27}$$

**Proof:** let $[w], [w'] \in D_n$, and assume that $[w] = [w']$ by definition, there exist $g \in s_n$ such that $w = g^{-1} w' g$. It then follows from lemma 5.5 that

$$g : \left(Q, s^w\right) \to \left(Q, s^{w'}\right) \tag{5.28}$$

Is a quandles isomorphism. Note that $\left(Q, s^{w'}\right)$ is of cyclic type, and hence two points homogeneous. Therefore, since $g(1) \neq g(2)$, there exist $h \in Inn\left(Q, s^{w'}\right)$ such that

$$h \circ g(1), h \circ g(2) = (1,2). \tag{5.29}$$

These yields $h \circ g \in s_{n,(1,2)}$. note that $h \circ g$ is a Latin quandles isomorphism from $\left(Q, s^w\right)$ *onto* $\left(Q, s^{w'}\right)$. Thus we have

$$(h\circ g)\circ s_1^w\circ(h\circ g)^{-1}=s_{h\circ g(1)}^{w'}=s_1^{w'} \tag{5.30}$$

This completes the proof of $\left[\left(s_1^w,s_2^w\right)\right]=\left[\left(s_1^{w'},s_2^{w'}\right)\right]$ . By showing that $f_2$ is the inverse of $g_2$. We have the following main result of this subsection.

**Proposition 5.12:** The map $g_2:P_n\to R_n$ is bijective

**Proof:** we show that $f_2$ is the inverse map of $g_2$. It is clear that the composition $f_2\circ g_2$ is identity mapping. Consider $g_2\circ f_2:R_n\to R_n,$ and take any $[w]\in R_n$ then one has $f_2([w])=\left[\left(s_1^w,s_2^w\right)\right]$. One also has $g_2\circ f_2([w])=\left[w'\right]$ where

$$w:=\left\{s_1^w,s_2^w\right\}\cup\left\{s_2^w\left(s_1^w\right)^{-1}s_2^w\right\} \tag{5.31}$$

Since $s^w$ is a quandles structure, one can see $w'\subset w$ thus we have $w'=w$ for cardinality reason. This shows that $g_2\circ f_2$ is the identity mapping. Recall (5.3) is a bijection from $Q_n$ *onto* $R_n$. We lastly construct a bijection from $Q_n$ *onto* $P_n$, let $s_1:=(2,3,...n)$ and recall that $Q_n$ Is the set of $s_2\in(s_n)_{n-1}$ satisfying $Q(1)$ *and* $(Q2)$

**Proposition 5.13:** the following map is bijective

$$g_3:Q_n\to P_n:S_2\to\left[(s_1,s_2)\right]$$

**Proof:** we show that $g_3$ is surjective. Take any $\left[(u_1,u_2)\right]\in P_n$ since $u_1\in(s_n)_{n-1}$ *and* $u_1(1)=1$ we can write $u_1=(2a_3a_4...a_n)$. Let us define $g\in s_n,(1,2)$ by

$$g:\begin{pmatrix}1&2&3&\dots&n\\1&2&a_3&\dots&a_n\end{pmatrix} \tag{5.32}$$

An easy computation show $g\circ g^{-1}u_1=s_1$ let $s_2:=g\circ g^{-1}u_2$. Then $s_2$ obviously satisfies $(Q1)$. Furthermore, since $(u_1,u_2)$ satisfies $(Pn)$. One can see that $s_2$ satisfies $(Q2)$. We thus have $s_2\in Q_n$. This concludes that $g_3$ is surjective since

$g_3(s_2)=\left[(s_1,s_2)\right]=\left[\left(g\circ g^{-1}\circ u_1,g\circ g^{-1}\circ u_2\right)\right]=\left[(u_1,u_2)\right]$ we show that $g_3$ is injective. Let $s_2,s_2'\in Q_n$ and suppose that $g_3(s_2)=g_3\left(s_2'\right)$. Hence there exist $h\in s_n,(1,2)$ such that

$$\left(s_1,s_2'\right)=\left(h^{-1}\circ s_1\circ h,h^{-1}\circ s_2\circ h\right) \tag{5.33}$$

By definition one has $h(1)=1$ and $h(2)=2$ then it follows from $h(2)=2$ that

$$3 = s_1(2) = h \circ s_1^{-1} \circ h(2) = h^2 \circ s_1^{-1}(2) = h(3) \tag{5.34}$$

Similarly, this yields that

$$4 = s_1(3) = h \circ s_1^{-1} \circ h(3) = h^2 \circ s_1^{-1}(3) = h(4) \tag{5.35}$$

One can show inductively that $x = h(x)$ for $x = any\ x \in Q$ this means that $h = id, and\ thus\ s_2^{'} = s_2$ this shows that $g_3$ is injective.

**a. CONSTRUCTING QUANDLES OF CYCLIC TYPE FROM Qn**

In the previous subsections. We have constructed the following bijections

$$g_3 : Q_n \to P_n,\ \ g_2 : P_n \to R_n, g_1 : R_n \to C_n \tag{5.36}$$

In this subsection, we describe $g_1 \circ g_2 \circ g_3(s_2)$ for each $s_2 \in Q_n$. Take any $s_2 \in Q_n$. Recall that $s_1 := (2,3...n)$ and

$$w_{(s_1,s_2)} := \{s_1, s_2\} \cup \{s_2 s_1^{-1} s_2\} \tag{5.37}$$

Then one has $g_2 \circ g_3(s) = \left[ w_{(s_1,s_2)} \right]$. We put

$$\psi(s_2) := s^w(s_1, s_2) \in C_n^{\#} \tag{5.38}$$

This means $g_1 \circ g_2 \circ g_3(s_2) = [\psi(s_2)]$. Note that $(\psi(s_2))_i \in w_{(s_1,s_2)}$ is defined as the unique element fixing $i \in Q$. This immediately yields

$$(\psi(s_2))_1 = s_1, (\varphi(s_2))_2 = s_2 \tag{5.39}$$

Let $i \in \{3,...n\}$. Then one has $i = s_1^{-1}(2)$ and hence

$$s_2 s_1^{-1} s_2 = s_1 s_2^{-1} s_1 = s_3 \tag{5.40}$$

This concludes that

$$(\psi(s_2))_i = s_2 s_1^{-1} s_2 \tag{5.41}$$

This concludes the proof of theorem 4.1.

## VI. CONCLUSION

Theorem 4.1 presents abstract construction of Latin quandles of prime order which gave rise to Latin quandles of cyclic type. These constructions help to established the concept of isomorphism in definition 2.3 between any given Latin quandles of the same order . The Latin quandle order structure is also presented on table 1 using cyclic permutation of order n-1 as shown in $Q_n$ which is the inner automorphism. Note that $s_x \left( x \in Q \right)$ is an automorphism of (Q,s) the subgroup of Aut (Q,s) generated by $\left\{ s_x \middle| x \in Q \right\}$ is called the inner automorphism group of (Q,s) and denoted by Inn(Q,s).

The results are summarized in table 1, which gives a classification of Latin quandles of cyclic type with prime cardinality up to 13. All Latin quandles presented were thoroughly verified using Maple software.

However, the classification of Latin quandle of cyclic type of order p > 13 up to isomorphism is still very open for future research especially for its fruitful application on cryptography.



## REFERENCE

[1]. Ugbolo Cletus, Ezurike Ugochi Julia, Ononogbo Chibuike Benjamin and Airemen Ikhuoria Edward: Connected Quandles of Order 3N and their Concept of Quandles Isomorphism. International Advanced Research Journal in Science, Engineering and Technology Vol. 7, Issue 9, September 2020 DOI 10.17148/IARJSET.2020.7911

[2]. Burstin, C.and Mayer, W. : Distributive Gruppen, J. Reine Angew . math.160,(1929)111-130.

[3]. Elhamdadi, M. Mac Quarrie J. and Restrepo, R. : Automorphism Group of Quadles, J. Algebra Appl.11,1(2012), 125008(9 pages).

[4]. Isere A.O. Akinleye, S. A and Adeniran, J.O: On Osborn loops of order 4n, Acta Universityatis Apulensis. No. 37,(2014)31-44.

[5]. Takasaki, M.: Abstractions of symmetric functions. Tohoku math. J.49(1943) 143-307(Japanese), Math.Rev.9 pages 8.

[6]. Isere A.O.: A quandles of order 2N and their concept of quandles isomorphism. Nigerian Mathematical society Journal vol. 39, Issue 2 pp. 155-166(2020).

[7]. Kamada, S. Tamaru, H. and Wads, K : On classification of quandles of cyclic type, Tokyo Journal of mathematics 39 1(2016) 151-171

[8]. Lopes, P. and Roseman D. : On finite racks and quandles, comm.. Algebra 34(2006). No. 1.371-406

[9]. Vendramin I. : On the classification of quandles of low order J. Knot Theorey Ranifications 21 (2012). No. 9, 1250088.10 pp.

[10]. Hayashi C.: Canonical forms for operation tables of finite connected quandles. Comm. Algebra 41(2013). 3340-3349.
[11]. Sehchi Kamada, Hiroshi Tamaru and Koshiro Wads: On classification of quandles of cyclic Type. Arxiv:1312.6917v [math.GT] 25 Dec 2013
[12]. Isere, A.O. Adeniran J. and Jaiyela, T.G.: On Latin quandles and Application to Cryptography. Preprint (2020).

[13]. Edwin Clerk W.; Mohamed Elhamdadi, Masahico Saito and Timothy Yeatman: On quandles colourings of Knots and applications arxi:1312.3307v2 [math.GT] 2014.
[14]. Mac Quarrie J : Automorphism Groups of quandles of order 3,4 and 5, Graduate Thesis and Dissertation, University of south floride available at https//Scoholar Commons. Usf.edu/etd/3226(2011).
[15]. Tamaru H. : Two point homogeneous quandles with prime cardinality, J.Math.Soc Japan 65(2013), No 4, 1117-1134.
[16]. David Stanovsky: A guide to self-distributive quasigroups, or Latin Quandles preprint