Contents

Acknowledgements

I would like to express my gratitude to my advisor, Prof. Claudia Menini, for all the support she gave me during my PhD.

I wish to thank Prof. David Stanovskỳ and Prof. Petr Vojtěchovský for mentoring me during my visiting period at Charles University in Prague and at DU in Denver.

I would also like to thank Dr. Daniele Toller, my advisor and friend and Dr. Mattia Zanella for the long hours shared in the PhD students' office at the department.

My sincere gratitude goes to Dr. Giuliano Bianco, who helped and encouraged me in the last three years like no other. I wouldn't have finished my PhD without his outstanding and precious support.

Introduction

Quandles are non associative algebraic structures which arise very naturally in a lot of different areas of mathemathics. The most important probably are *knot theory*, ([6], [9], [10] and [22]) and the study of the solution of the (set-theoretical) *Quantum Yang Baxter Equation* (QYBE, [1], [14]) related to the classification of *pointed Hopf Algebras* ([1], [18]).

Quandles are also an interesting variety arising in universal algebra, since its axiomatization is given by very natural identities.

The main goal of the present work is to apply some tools of universal algebra and elements of tame congruence theory ([19]) to quandles, since they provide a very good example of an *idempotent* variety.

The core of this thesis is about *extension* theory of quandles, i.e., the description of the properties of a quandle starting from the properties of its congruences and the properties of its homomorphic images.

My work is a natural continuation of the work of Dr. Giuliano Bianco, who is a former PhD student at the department of Mathematics and Computer Sciences of the University of Ferrara. He was interested in the theory of quotient of quandles and into classifying quandles of order p^3 with p prime.

In the sequel we give a summary of the contents of this thesis.

Section 1 collects basic definitions, notations and known facts about *universal algebra*. In particular we introduce the notion of *congruence* of an algebra, of *Abelian, strongly Abelian* and *central* congruences (and algebras) and of *Maltsev conditions*.

The study of Maltsev conditions is one of the central topics in universal algebra, in view of its relation to *constraint satisfaction problems* (CSPs).

Section 2 is about Left-Qasigroups (LQGs) and *Quasigroups*. In Section 2.3 we introduce the notions of *connected* and *homogeneous* LQG and we define $\pi_0(\mathbf{X})$ to be the set of the orbits of the action of the Left multiplication group over $\mathbf{X}$ (denoted by $LMlt(\mathbf{X})$ from now on), endowed with the projection LQG structure. In Proposition 2.20 and Corollary 2.21 we show that a LQG $\mathbf{X}$ is connected if and only if $\mathbf{P}\text{-}\mathbf{LQ}_2 \notin \mathcal{H}(\mathbf{X})$. The definition of $\pi_0(\mathbf{X})$ and these results were already known for quandles ([13, Definition 2.28], [13, Proposition 2.30]) and we have extended them for LQGs.

Section 3 collects some known facts about quandles with a particular focus on homogeneous and connected quandles, which are the most studied and understood classes of quandles ([1], [4], [14], [17], [20], [25] and [33]).

Section 3.2 is about *coset representation* of homogeneous quandles (see Proposition 3.7) and in Section 3.3 we emphasize the role of the *transvection group* (in the following $Dis(\mathbf{X})$) in the theory of connected quandles. In particular it provides a *minimal representation* for connected quandles as has been proven in [20]. All the results of Section 3 were already known or are minor modifications of existing results.

Section 3.4 is about *faithful* quandles and collects some known facts about this class of quandles. The only original contribution in this Section is given in Proposition 3.24, where we adopt a categorical viewpoint. We define the functor L from the category of racks to the category of quandles and a natural transformation between

$\mathcal{U}L$ and I (where $\mathcal{U}$ is the forgetful functor from quandles to racks and I is the identity functor on racks).

Section 3.5 describes some interesting subclasses of the class of faithful quandles. We give a characterization of these classes by using universal algebra and we discuss the relations between them. These classes are:

(1) *Latin* quandles, defined as idempotent left-distributive quasigroups (already known and studied in literature, see [16], [27]).
(2) *Maltsev* quandles, defined as quandles admitting a *Maltsev term*. This is a class of algebras which can be defined in any variety (it was defined for the first time in [24], which is the first paper showing a connection between the congruence lattice of an algebra and the *clones* of the term operations). In the case of quandles there is no literature about it.
(3) *Taylor* quandles, defined as quandles admitting a *Taylor term*. The class of *Taylor* algebras arises very naturally in universal algebra, since it can be defined in any variety as the class of algebras which satisfy a non-trivial idempotent Maltsev condition ([26]).
(4) *Strongly faithful* quandles, defined as quandles such that any subquandle is faithful. This class has been defined for the first time by the author.

Note that the class of Latin quandles is a variety.

The class of *strongly faithful* quandles has been characterized in Proposition 3.33 in which we denote by $\mathbf{P\text{-}LQ}_2$ the projection LQG of size 2.

Proposition (3.33)**.** *Let $\boldsymbol{X}$ be a quandle. Then the following are equivalent:*

(1) *$\boldsymbol{X}$ is strongly faithful;*
(2) *$Fix(L_x) = \{x\}$ for every $x \in X$;*
(3) *$\boldsymbol{P\text{-}LQ}_2 \notin \mathcal{S}(\boldsymbol{X})$.*

In the finite case, we have the following characterization of Taylor quandles in Theorem 3.36.

Theorem (3.36)**.** *Let $\boldsymbol{X}$ be a finite quandle. Then the following are equivalent:*

(1) *$\boldsymbol{X}$ is a Taylor quandle;*
(2) *all the subquandles of $\boldsymbol{X}$ are connected.*

So, finite Taylor algebras have a really nice and natural characterization in the variety of quandles, since the class of quandles which has been studied deeper in the literature is for sure the class of connected quandles. The relations between these properties is the following

$$\text{Latin} \Rightarrow \text{Maltsev} \Rightarrow \text{Taylor} \Rightarrow \text{strongly faithful} \Rightarrow \text{faithful}$$

We also pointed out that the variety of Latin quandles is a proper subclass of the class of Maltsev quandles and that Taylor quandles form a proper subclass of strongly faithful quandles. This analysis yields to the following problems.

Problem. *Give a characterization of Maltsev quandles.*

Does the condition $\boldsymbol{P}_2 \notin \mathcal{S}(\boldsymbol{X})$ have some characterization in universal algebra?

Section 4 investigates the classes of *principal* and *affine* quandles. These classes correspond to quandles admitting a *regular* group of automorphisms (Proposition

4.1). In particular connected principal quandles correspond to quandles with regular transvection group (Proposition 4.2).

In Section 4.2 we prove that the subclasses of *principal Latin* quandles is a variety (Theorem 4.8), and therefore an equational class. This is a new result which leads to the following open problem.

Problem. *Find a equational axiomatization for the variety of principal Latin quandles.*

In Section 4.3, we go back to the classes studied in Section 3.5, and we show that under the assumption of principality, faithful and strongly faithful quandles coincide (Proposition 4.11). If we add finiteness to the picture, we get that all the classes defined above coincide (Proposition 4.14). In the affine case they also coincide with the class of connected quandles (Proposition 4.15).

We also prove that the class of Taylor quandles coincides with the class of Latin quandles in the affine case (Proposition 4.13). Therefore it coincides also with the class of affine Taylor quandles. Hence we formulate the following question.

Question. *Does the class of Taylor quandles and the class of Maltsev quandles coincide?*

We define *extensions* for LQGs in Section 5.1. This notion was already known for quandles and we performe the same construction of [1] in this more general setting and we reformulate some known results in this framework (Propositions 5.3 and 5.7). An extension of a LQG $\mathbf{X}$ by a set S is a LQG $(X \times S, \cdot)$ such that the canonical projection onto $\mathbf{X}$ is a morphism. The structure of $(X \times S, \cdot)$ is determined by the structure of $\mathbf{X}$ and by a map

$$\beta : \mathbf{X} \times \mathbf{X} \times S \longrightarrow \mathrm{Sym}(S)$$

since the multiplication is necessarily defined by

$$(x, s) \cdot (y, s) = (xy, \beta(x, y, s)(t)).$$

This structure is denoted by $\mathbf{X} \times_\beta S$. Whenever you have a *uniform* congruence of a LQG $\mathbf{X}$ (i.e. a congruence with all the blocks with the same cardinality), then $\mathbf{X}$ is an extension of $\mathbf{X}/\alpha$, up to isomorphism (Proposition 5.5). Moreover in the class of connected LQGs all the congruences are uniform and therefore, any LQG is an extension of any of its factors.

In the variety of quandles, β has to satify some further conditions, called *cocycle condition* (C) and *quandle condition* (Q), which reflect left-distributivity and idempotency. The maps satisfying (C) and (Q) are called *dynamical cocycles* and the set of dynamical cocycles of $\mathbf{X}$ is denoted by $Z^2(\mathbf{X}, S)$ (see Section 5.2).

In Section 5.3 we present the idea of *non-Abelian Cohomology*, which was already defined in Section 2 of [1]. The same extension can be described by different cocycles. Given two different cocycles, they are said to be *cohomologous* if the structure of the correspondent extension are obtain just by different labelling of the elements belonging to the same block. This condition define an equivalence relation on $Z^2(\mathbf{X}, S)$, therefore it is enough to consider the correspondent quotient. The quotient is called the *second Cohomology set of* $\boldsymbol{X}$ and denoted by $H^2(\mathbf{X}, S)$ (defined in 5.15).

Section 5.4 introduces a particular family of extensions of a quandle $\mathbf{X}$ which was studied indipendently and with different approaches in [1] and [13]. In [13] the elements of this family are called *coverings* and they are defined as pairs $(\mathbf{Y}, \rho)$, where $\mathbf{Y}$ is a quandle and $\rho : \mathbf{Y} \longrightarrow \mathbf{X}$ a surjective morphism, such that

$$\rho(x) = \rho(y) \;\Rightarrow\; L_x = L_y.$$

In [1] the family of *constant cocycles* is defined. Namely a cocycle β is constant if

$$\beta(x, y, s) = \beta(x, y, t), \text{ for every } x, y \in X \text{ and every } s, t \in S,$$

i.e. β is defined by a map from $X \times X$ to $\mathrm{Sym}(S)$. For this family of maps, cocycle condition and quandle condition are expressed by (CC) and (CQ).

The subset of constant cocycles is denoted by $Z^2_c(\mathbf{X}, S)$ and it is closed under the relation to be cohomologous. Therefore the correspondent subset of the second Cohomology set, is denoted by $H^2_c(\mathbf{X}, S)$.

Note that constant cocycle can be defined as mapping $\beta : X \times X \longrightarrow \Gamma$, where Γ is an arbitrary group and all the definitions above still make sense.

We show that the the family of coverings of a connected quandle $\mathbf{X}$ and the family of its extension by constant cocycles coincide. We also provide some examples of quandle coverings in the class of homogeneous quandles (Proposition 5.25).

In the variety of quandles there is a strong interplay between normal subgroups of the transvection group which are normal in the left multiplications group and congruences (see Lemma 4.2 of [4]). Section 6 is a further development of the subject of Section 4 of [4] and we claim that the results of this Section are brand new.

As a new contribution in Section 6.1, we show that there is a *Galois connection* between the congruence lattice of a quandle and the congruence lattice of subgroup of the transvection group which are normal in the left multiplication group. For every congruence α of a quandle $\mathbf{X}$ we define the subgroup $Dis_\alpha(\mathbf{X})$ as the subgroups generated by $L_x L_y^{-1}$ where $x \;\alpha\; y$. This definition leads to the following Theorem.

Theorem (6.9)**.** *Let $\boldsymbol{X}$ be a quandle and $[\{1\}, Dis(\boldsymbol{X})]$ be the interval between $\{1\}$ and $Dis(\boldsymbol{X})$ in the lattice of the normal subgroups of $LMlt(\boldsymbol{X})$. Then the assignment*

$$\begin{array}{rcl} Con(\boldsymbol{X}) & \longrightarrow & [\{1\}, Dis(\boldsymbol{X})] \\ \alpha & \mapsto & Dis_\alpha(\boldsymbol{X}) \\ \alpha_N & \leftarrow & N \end{array}$$

is a Galois connection.

Moreover, every normal subgroup $N \in [\{1\}, Dis(\mathbf{X})]$ sits in between $Dis_{\alpha_N}(\mathbf{X})$ and $Dis^{\alpha_N}(\mathbf{X})$. This condition together with the Galois connection is a powerful tool to infer informations about the congruence lattice of a quandle when the structure of the transvection group is known and vice versa. In order to exploit this interplay it is necessary to understand which is the relation between the subgroups $Dis_\alpha(\mathbf{X})$ and $Dis^\alpha(\mathbf{X})$.

Problem. *Under which assumption on $\boldsymbol{X}$ and α we have that $Dis_\alpha(\boldsymbol{X}) = Dis^\alpha(\boldsymbol{X})$?*

In Section 6.2 we give a characterization of Abelian, central and strongly Abelian congruences by group-theoretical properties of the correspondent subgroups of the transvection group. This result suggests that the role of this family of subgroups is very important. Moreover, we find that the definition of covering correspond to the universal algebraic concept of strong Abelianness.

Proposition (6.16)**.** *Let $\boldsymbol{X}$ be a quandle and α be its congruence. The following are equivalent:*

(1) *α is Abelian;*
(2) *$Dis_\alpha(\boldsymbol{X})$ is Abelian and α-semiregular.*

Proposition (6.19)**.** *Let $\boldsymbol{X}$ be a quandle and α its be congruence. Then the following are equivalent:*

(1) *α is central;*
(2) *$Dis_\alpha(\boldsymbol{X})$ is central in $Dis(\boldsymbol{X})$ and $Dis(\boldsymbol{X})$ is α-semiregular.*

Proposition (6.20)**.** *Let $\boldsymbol{X}$ be a quandle and α be its congruence. The following are equivalent:*

(1) *α is strongly Abelian;*
(2) *$Dis_\alpha(\boldsymbol{X}) = 1$;*
(3) *$(\boldsymbol{X}, \pi_\alpha)$ is a covering of $\boldsymbol{X}/\alpha$.*

In Section 6.3 we develop the ideas of Section 6.2 in connection to *Abelian extensions*. This family of extensions was already defined in [10]. In [1] and [6] the same construction was carried out under the name of *quandle modules*. We point out that this construction is a special case of a universal algebraic concept, i.e. we prove that Abelian congruences with connected blocks correspond to Abelian extensions (Proposition 6.30).

The largest central congruence of an algebra is said to be the *center* of the algebra. Thanks to Proposition 6.19, the center of a quandle is well understood (Corollary 6.34).

Solvable and *nilpotent* algebras are important subclasses of every variety. In Section 6.4 we show that solvable (nilpotent) quandles have solvable (nilpotent) transvection group (Propositions 6.36 and 6.37). Moreover solvable (nilpotent) Taylor quandles are completely characterized by the solvability (nilpotency) of their transvection groups (Theorems 7.14 and 6.40).

Since the class of Taylor quandles has a natural characterization and it behaves nicely with respect to solvability and nilpotency, one can be interested in their classification.

Problem. *Classify all the finite Taylor quandles (up to some size).*

The main future direction of research we want to follow is to understand better the features of the Galois correspondence between congruences and normal subgroups, and the characterization of Abelian and central congruences in order to solve some open problems as the following ones.

Problem. *Characterize connected quandles of size pq with p and q prime.*
Is any connected quandle of order $3p$ Latin?

Finally in Section 6.5 we characterize the connected extensions of a given quandle which preserve the transvection group (Proposition 6.42).

The original result of Section 7 is to show that no finite quandle satisfies *meet-semistributivity*. This is an interesting property of the congruence lattice of an algebra than can be characterized by a Maltsev condition ([2]).

First we show some general features of quandles with doubly transitive automorphism group (Section 7.1) and then we characterize *minimal* quandles (i.e. quandles with no proper subquandles) among the *simple* ones by several different conditions in Theorem 7.18 (references about simple and minimal quandles can be find in [22], [1] and [16]). This characterization leads to Theorem 7.19.

Section 8 is dedicated to define a combinatorial approach to the computation of the second cohomology set of Latin quandles. This is a brand new approach to this problem and our mail goal is to use it to extend Lemma 5.1 of [17], i.e., to provide some more examples of quandles with *trivial cohomology*, i.e. satisfying $H^2_c(\mathbf{X},\Gamma) = \{\mathbf{1}\}$ for every group Γ (where $\mathbf{1}$ denotes the constant map $(x, y) \mapsto 1$ for every $x, y \in X$).

First we define a special representative for each class of $H^2_c(\mathbf{X},\Gamma)$ with some special properties, called *normalized cocycle*. Namely, given an element $u \in X$, the normalization condition with respect to u is given by

$$\beta(x, u) = 1, \text{ for every } x \in X.$$

Showing that a quandle has trivial cohomology is equivalent to show that any normalized cocycle is trivial (Proposition 8.7).

It turns out that a u-normalized cocycle is invariant under the diagonal action of L_u (Proposition 8.9) and with respect to the action of the permutations f and ω acting on $X \times X$ (defined as in Propositions 8.10 and 8.11).

Section 8.3 is a technical Section about the properties of this action in general. The actions of f and ω on $X \times X$ induce an action on the set of the orbits with respect to the diagonal action of L_u.

In Section 9 we discuss several particular cases. In Section 9.1 we restrict to principal Latin quandles. In definition 9.7 we define a condition for the length of the orbits of f, called condition (F), namely

of all the (non-trivial) orbits of the action under f have size $|X| - 1$.

We came up to it by virtue of the reasoning in Remark 9.6, which shows that it is not arbitrary as it may seem at a first glance.

This condition turns out to be sufficient for a non-affine principal Latin quandle to have trivial cohomology (Proposition 9.8).

Section 9.2 collects some reformulation of the results of 9.1 for finite affine connected quandles. Moreover in the affine case we can compute explicitly the length of the orbits of f and ω (Propositions 9.12 and 9.13) and we can characterize quandles satisfying condition (F) (Proposition 9.18).

Then we apply the previous results to the class of affine quandles over *cyclic groups* and to the family of quandles with doubly transitive left multiplication group (for which there exists a characterization in [33]). It turns out that all quandles belonging to these families except those of size 4 have trivial cohomology.

Theorem (9.26)**.** *Let* $\boldsymbol{X} = \mathcal{Q}(\mathbb{Z}_m, \lambda_n)$ *be a connected quandle. Then* $\boldsymbol{X}$ *has trivial cohomology.*

Theorem (9.31)**.** *Let* $\boldsymbol{X} = \mathcal{Q}\left(\mathbb{Z}_p^n, \alpha\right)$ *be a doubly transitive quandle with* $p \geq 3$ *and* $n > 1$*. Then* $\boldsymbol{X}$ *has trivial cohomology.*

Theorem (9.32)**.** *Let* $\boldsymbol{X} = \mathcal{Q}\left(\mathbb{Z}_2^n, \alpha\right)$ *be a doubly transitive quandle with* $n \neq 2$*. Then* $\boldsymbol{X}$ *has trivial cohomology.*

The previous theorems show that the condition (F) is sufficient to have trivial cohomology for principal Latin quandles with size different than 4.

Corollary (9.34)**.** *Let* $\boldsymbol{X}$ *be a finite principal Latin quandle with* $|X| \neq 4$*. If* $\boldsymbol{X}$ *satisfies condition (F) then it has trivial cohomology.*

We claim that this combinatoral approach has some potential and that may be used to characterize Latin quandles with trivial cohomology.

Problem. *Give a characterization of Latin quandles with trivial cohomology.*

Is there any combinatorial characterization of this class in terms of the properties of the actions of f *and* ω*?*

In Section 10 we briefly present the categorical approach to coverings carried out by Eisermann in [13]. His approach relies on the properties of the *Adjoint group* (see [13] and [18]) and points out the relationship between coverings and central extensions of groups. Section 10.1 collects the main results from the paper of Eisermann and we just observe that in the finite case it is enough to deal with a proper finite quotient of the Adjoint group.

As new contributions, in Section 10.2 we show a characterization of *simply connected* quandles (i.e. quandles such that $H_c^2(\mathbf{X}, S) = \{\mathbf{1}\}$ for every S in the terminology of Eisermann) as a subclass of principal quandles (Theorem 10.17) and in Section 10.3 we show that the functor L preserves coverings (Corollary 10.24).

Finally, Section 11 collects all the questions and open problems we have already stated above with some more details.

In the development of the present work we used the software GAP in order to produce specific examples or non-examples of quandles.

Notations

In the present work the following notations will be used. If G is a group acting on a set X, the stabilizer of a point x under this action will be denoted by G_x and its orbit by $O_G(x)$. The centralizer of an element $g \in G$ will be denoted by $C_G(g)$ and the automorphism group of G by $Aut(G)$. The unit element of a group and the identity mapping will be denoted by 1.

The n^{th} element of the lower central series will be denoted by G^n, and the n^{th} element of the derived series by $G^{(n)}$. The order of an element $g \in G$ will be denoted by $o(g)$.

Groups defined by generators and relations are denoted by $\langle X \mid R \rangle$ and the surjective morphism from the free group generated by X and $\langle X \mid R \rangle$ by π_R.

The least common multiple of a and b will be denoted by L.C.M.$\{a, b\}$ and the greatest common divisor of a and b by G.C.D.$\{a, b\}$.

Further notations will be introducted whenever needed.

1. Universal Algebra

1.1. **Basics and Definitions.** There are many definitions of what is an *algebra structure* on a set X. The most natural way is to define it as a set endowed with a set of *operations*. In the sequel the universal algebraic viewpoint is adopted and in this Section some basics notions are summarized. For further references about universal algebra, see [3] and [5].

Definition 1.1. An *n-ary operation* f on a set X, is a function

$$f : X^n \longrightarrow X$$

The number n is called the *arity* of f. An *algebra* is a pair (X, F) where X is a set and F is a set of operations together with a map $\rho : F \longrightarrow \mathbb{N}$, which assigns to every $f \in F$ its arity. The map ρ is called the *type* or *signature* of X.

The algebra (X, F) will be denoted by $\mathbf{X}$ and the underlying set just by X.

Example 1.2. A set $\mathbf{X}$ is just an algebra with no operation. The one element set is called *trivial algebra*.

Any algebra has *projection operation* defined by setting

$$\pi_i^n : X^n \longrightarrow X, \quad (x_1, \dots, x_i, \dots, n_n) \mapsto x_i$$

for every $n \in \mathbb{N}$ and every $i \leq n$. An algebra on a set X with only projection operation is called *projection algebra* and denoted $\mathbf{P}_{|X|}$.

A subset $Y \subseteq X$ closed under every operation is called *subuniverse* of X. This means

$$y_1, \dots, y_n \in Y \implies f(y_1, \dots, y_n) \in Y$$

for every n-ary operation $f \in F$. A *subalgebra* of $\mathbf{X}$ is a pair (Y, F_Y) where Y is a subuniverse and F_Y denote the set of the restrictions of the elements of F to Y.

Definition 1.3. Let $\mathbf{X}$ be an algebra and S a subset of X. Then the smallest subalgebra containing X is called the *subalgebra generated by S* and denoted by $Sg(S)$.

Note that 0-ary operations are allowed, and they are constant mappings. An algebra with a finite number of operations is usually denoted by $(X, f_1, \dots, f_n)$ and its type by $(\rho(f_1), \dots, \rho(f_n))$.

For instance a group is an algebra $(G, \cdot, ^{-1}, 1)$ of type $(2, 1, 0)$, a monoid is an algebra $(M, \cdot, 1)$ of type $(2, 0)$ and so on.

The elements of F are usually called *basic operations*. Whenever it makes sense, they can be composed as functions.

Definition 1.4. [5, Definition 10.1] The set of *term operations* of the algebra $\mathbf{X}$ is the smallest set $T(\mathbf{X})$ such that it contains X and 0-ary operations on $\mathbf{X}$ and for every $f \in F$ an n-ary basic operation and every $t_1, \dots, t_n \in T(\mathbf{X})$, we have $f(t_1, \dots, t_n) \in T(\mathbf{X})$.

A term operation is then an arbitrary finite well defined composition of basic operations and therefore it is a function

$$t : X^n \longrightarrow X$$

where n is its arity. Two n-ary term operations t and s are the same if and only if

$$t(x_1, \dots, x_n) = s(x_1, \dots, x_n)$$

for every $x_1, \dots, x_n \in X$, or shortly $t \approx s$. The *subalgebra generated* by a subset is obtained by applying term operations to tuples of element of the subset.

Fact 1.5. *Let $\boldsymbol{X}$ be an algebra and $Y \subseteq \boldsymbol{X}$. Then*

$$Sg(Y) = \{t(y_1, \dots, y_n),\ y_i \in Y \text{ for every } 1 \le i \le n,\ t \in T(\boldsymbol{X})\}$$

In order to compare algebras of the same type the notion of *language* is needed. It is nothing but a labelling of basic operations which allows to identify corresponding operations of different algebras of the same type.

Definition 1.6. A *language* is a pair $(L, \mathbf{ar})$, where L is a set of symbols, ar is a map from L to $\mathbb{N}$. An algebra in a given language L is an algebra $\mathbf{X} = (X, F)$ of type ρ, together with a bijection

$$L \longrightarrow F, \quad \lambda \mapsto f_\lambda^{\mathbf{X}}$$

such that $\mathbf{ar}(\lambda) = \rho(f_\lambda^{\mathbf{X}})$. The symbol λ is called *n-ary symbol*.

This is essential in order to define *morphisms* between two algebras of the same type.

Definition 1.7. Let $\mathbf{X}$ and $\mathbf{Y}$ be algebras of the same type in a given language L. A map $\phi : X \longrightarrow Y$ is a *algebra morphism* if

$$\phi(f_\lambda^{\mathbf{X}}(x_1, \dots, x_n)) = f_\lambda^{\mathbf{Y}}(\phi(x_1), \dots \phi(x_n))$$

for every n-ary symbol $\lambda \in L$ and every $x_1, \dots, x_n \in X$. If ϕ is bijective then it is called *isomorphism*.

The image of an algebra morphism is a subalgebra of the codomain and it is called *homomorphic image* of X.

It is easy to verify that invertible morphisms of algebra from $\mathbf{X}$ to $\mathbf{X}$ form a group under composition. They are called *automorphisms* and the group is denoted by $Aut(\mathbf{X})$.

Let $\{\mathbf{X}_i,\ i \in I\}$ be a family of algebras of a given type. The cartesian product of the underlying sets of the family has a natural structure of algebra, given by operations defined component-wise. An element of the cartesian product will be denoted by (x_i) and its j-th components by x_j.

Definition 1.8. Let $\{\mathbf{X}_i,\ i \in I\}$ a family of algebras of a given type ρ, in a language L. For every n-ary symbol $\lambda \in L$, define

$$\left(f_\lambda((x_i^1),\dots,(x_i^n))\right)_j = f_\lambda^{\mathbf{X}_j}(x_j^1,\dots,x_j^n)$$

for every $j \in I$ and every $(x_i^k) \in \prod_{i\in I} X_i$. Then $\prod_{i\in I}\mathbf{X}_i$ is an algebra of type ρ and it is called the *product* of the family $\{\mathbf{X}_i,\ i \in I\}$.

Some classes of algebras play a central role in universal algebra. They are defined as the classes closed with respect to the class operators $\mathcal{H}, \mathcal{S}$ and $\mathcal{P}$.

Definition 1.9. Let $\mathcal{K}$ be a class of algebras of a given type. The class operators $\mathcal{H}, \mathcal{S}$ and $\mathcal{P}$ are defined by setting:

(a) $\mathbf{X} \in \mathcal{S}(\mathcal{K})$ if $\mathbf{X}$ is isomorphic to a subalgebra of some algebra $\mathbf{K} \in \mathcal{K}$;
(b) $\mathbf{X} \in \mathcal{H}(\mathcal{K})$ if $\mathbf{X}$ is a homomorphic image of some algebra $\mathbf{K} \in \mathcal{K}$;
(a) $\mathbf{X} \in \mathcal{P}(\mathcal{K})$ if $\mathbf{X}$ is isomorphic to a product of a family of algebras of $\mathcal{K}$;

Definition 1.10. A class of algebra of a given type $\mathcal{K}$ is a *variety* if and only if

$$\mathcal{H}(\mathcal{K}) = \mathcal{S}(\mathcal{K}) = \mathcal{P}(\mathcal{K}) = \mathcal{K}.$$

Let $\mathcal{K}$ be a class of algebras of a given type. The smallest variety containing $\mathcal{K}$ is called *variety generated by* $\mathcal{K}$ and it will be denoted by $\mathcal{V}(\mathcal{K})$.

Classes of algebras of the same type are often identified by a set of identities involving term operations (axioms). This turns out to be (one of) the characterizations of varierties.

Theorem 1.11. *A class of all algebras of a given type ρ is a variety if and only if it is the class of algebras of type ρ satisfying a certain set of identities for term operations.*

For instance the variety of groups is given by all algebras $(G, \cdot, ^{-1}, 1)$ of type $(2, 1, 0)$, satisfying

$$\begin{aligned} x\cdot(y\cdot z) &\approx (x\cdot y)\cdot z \\ x\cdot 1 &\approx 1\cdot x \approx x \\ x\cdot x^{-1} &\approx x^{-1}\cdot x \approx 1 \end{aligned}$$

Remark 1.12. *Any variety of algebras of a given type and its algebra morphisms form a category.*

For this reason some categorical notions and constructions will be used in the sequel for sake of convenience.

1.2. **Congruences.** A *congruence* of an algebra **X** is an equivalence relation which respects the algebra structure. Let α be an equivalence relation on X, an α-related pair of element $x, y \in X$ will be denoted by $x \ \alpha \ y$ and given $\bar{x}$ and $\bar{y}$ n-tuples, $\bar{x} \ \alpha \ \bar{y}$ means $x_i \ \alpha \ y_i$ for every $1 \leq i \leq n$. The class of x will be denoted by $[x]_\alpha$ (or simply by $[x]$). Classes are called *blocks*.

Definition 1.13. Let **X** be an algebra. An equivalence relation α on X is a *congruence* if

$$\bar{x} \ \alpha \ \bar{y} \implies t(x_1, \dots, x_n) \ \alpha \ t(y_1, \dots, y_n) \tag{1}$$

for every n-ary term operation t. A congruence is called *uniform* if all the blocks have the same cardinality. The set of all congruences of an algebra **X** will be denoted by $Con(\mathbf{X})$.

Obviously it is enough to check the implication (1) just for basic operations. The next is a very well know fact.

Fact 1.14. *The poset* $(Con(\boldsymbol{X}), \subseteq)$ *is a bounded algebraic lattice.*

In the sequel the biggest congruence, namely $\mathbf{X} \times \mathbf{X}$, will be denoted by $1_{\mathbf{X}}$, the smallest one, namely $\{(x, x), \ x \in X\}$, by $0_{\mathbf{X}}$ and the set $\{\gamma \in Con(\mathbf{X}), \ \alpha \leq \gamma \leq \beta\}$ by $[\alpha, \beta]$.

The quotient of X with respect to a congruence has a natural structure of algebra. This is uniquely determined by claiming that the canonical projection is an algebra morphism.

Lemma 1.15. [5, Theorem 6.10] *Let* α *be a congruence of the algebra* $\boldsymbol{X}$ *in a given language* L. *Then*

$$(f_\lambda^{\boldsymbol{X}/\alpha})([x_1]_\alpha, \dots, [x_n]_\alpha) = [f_\lambda^{\boldsymbol{X}}(x_1, \dots, x_n)]_\alpha$$

is well defined for every n*-ary symbol* $\lambda \in L$. *Then* $\boldsymbol{X}/\alpha$, *is an algebra of the same type of* $\boldsymbol{X}$ *and*

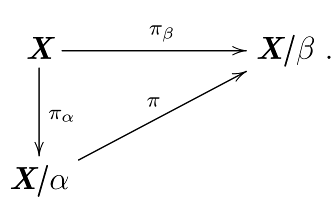
$$\pi_\alpha : \boldsymbol{X} \longrightarrow \boldsymbol{X}/\alpha, \quad x \longrightarrow [x]_\alpha$$

is an algebra morphism.

The following Proposition shows another very well known fact about congruences.

Proposition 1.16. *Let* $\boldsymbol{X}$ *be an algebra and* α, β *be its congruences. Then the following are equivalent:*

(1) $\alpha \leq \beta$;
(2) *there exists a unique surjective morphism* π *such that the following diagram is commutative*



Proof. The map π has to be necessarily defined as follows

$$\pi([x]_\alpha) = \pi(\pi_\alpha(x)) = \pi_\beta(x) = [x]_\beta$$

This map is well defined if and only $\alpha \leq \beta$. Let $\lambda \in L$ be a n-ary symbol, then

$$\begin{aligned} \pi((f_\lambda^{\mathbf{X}/\alpha}([x_1]_\alpha, \dots, [x_n]_\alpha)) &= \pi(\pi_\alpha(f_\lambda^{\mathbf{X}}(x_1, \dots, x_n)) = \\ &= \pi_\beta(f_\lambda^{\mathbf{X}}(x_1, \dots, x_n)) = \\ &= f_\lambda^{\mathbf{X}/\beta}([x_1]_\beta, \dots, [x_n]_\beta) = \\ &= f_\lambda^{\mathbf{X}/\beta}(\pi([x_1]_\alpha), \dots, \pi([x_n]_\alpha)) \end{aligned}$$

Therefore, π is a morphism. □

Algebras defined as in Lemma 1.15 are usually called *factor algebras*. It turns out that, up to isomorphism, factor algebras are all the homomorphic images of $\mathbf{X}$. Hence, there is a one to one correspondence between the set of congruences $Con(\mathbf{X})$ and the set of isomorphism classes of homomorphic images of $\mathbf{X}$, denoted by $\mathcal{H}(\mathbf{X})/\sim$.

Proposition 1.17. [5, Theorem 6.12] *Let $\boldsymbol{X}$ be an algebra and $\boldsymbol{Y}$ its homomorphic image under the morphism ϕ. Then $ker(\phi) = \{(x,y) \in X \times X,\ f(x) = f(y)\}$ is a congruence and $\boldsymbol{Y} \simeq \boldsymbol{X}/ker(\phi)$.*

Corollary 1.18. *Let $\boldsymbol{X}$ be an algebra. Then*

$$\begin{array}{rcl} Con(\boldsymbol{X}) & \longleftrightarrow & \mathcal{H}(\boldsymbol{X})/\sim \\ \alpha & \mapsto & [\boldsymbol{X}/\alpha] \\ ker(\phi) & \leftarrow\!\shortmid & [Im(\phi)] \end{array}$$

is a bijection.

In some cases congruences correspond to *subnormal objects*, as for groups and modules, but it is just a special feature of some varieties.

The congruence lattice of a factor algebra $\mathbf{X}/\alpha$ is determined by the congruence lattice of $\mathbf{X}$.

Lemma 1.19. [5, Lemma 6.14] *Let $\boldsymbol{X}$ be an algebra and $\alpha \leq \beta$ be its congruences. The relation β/α defined by setting*

$$[x]_\alpha\ \beta/\alpha\ [y]_\alpha \iff x\ \beta\ y$$

is a congruence of $\boldsymbol{X}/\alpha$.

The following theorem is called the corrispondence theorem.

Proposition 1.20. [5, Theorem 6.20] *Let $\boldsymbol{X}$ be an algebra and $\alpha \leq \beta$ be its congruences. Then*

$$[\alpha, 1_{\boldsymbol{X}}] \longrightarrow Con(\boldsymbol{X}/\alpha), \quad \beta \mapsto \beta/\alpha$$

is a lattice isomorphism.

As for normal subgroups of a group, congruences can be *Abelian* and *central*.

Definition 1.21. A congruence α of an algebra $\mathbf{X}$ is called

(a) *Abelian* if, for every term t, $x\ \alpha\ y$, $\bar{u}\ \alpha\ \bar{v}$,

$$t(x,\bar{u}) = t(x,\bar{v}) \iff t(y,\bar{u}) = t(y,\bar{v}) \tag{2}$$

(b) *central* if, for every term t, $x\ \alpha\ y$, $u_i, v_i \in X$,

$$t(x,\bar{u}) = t(x,\bar{v}) \iff t(y,\bar{u}) = t(y,\bar{v}) \tag{3}$$

(c) *strongly Abelian* if, for every term t, $x\ \alpha\ y$, $\bar{u}\ \alpha\ \bar{v}\ \alpha\ \bar{w}$,

$$t(x,\bar{u}) = t(y,\bar{v}) \implies t(x,\bar{w}) = t(y,\bar{w}) \tag{4}$$

An algebra is said to be

(d) *Abelian* if $1_{\mathbf{X}}$ is Abelian;
(e) *strongly Abelian* if $1_{\mathbf{X}}$ is strongly Abelian.

Remark 1.22. *It is enough to check condition 2, 3 and 4 just for certain type of terms operations. A term operation t is called slim with respect to a variable if there is only one occurrence of it in t, if this occurrence is in the lowest level of t, and if every node of t has at most one branch of length greater than 1.*

By Lemma 4.1 of [28], *α is Abelian (central, strongly Abelian) if and only if formula 2 (3, 4) holds for every slim term operation with respect to the first variable.*

Both centrality and strongly Abelianness are stronger than Abelianness.

Lemma 1.23. *Let $\boldsymbol{X}$ be an algebra and α be its congruence.*

(i) *If α is central, then it is Abelian.*
(ii) *If α is strongly Abelian then it is Abelian.*

Proof. Let assume that $x\ \alpha\ y$, $\bar{u}\ \alpha\ \bar{v}$ and $t(x,\bar{u}) = t(x,\bar{v})$ for some n-ary term.

(i) By centrality, $t(y,\bar{u}) = t(y,\bar{v})$ for every $\bar{u},\bar{v} \in X^{n-1}$. So it holds in particular whenever $\bar{u}\ \alpha\ \bar{v}$.

(ii) It follows by Proposition 3.11 of [19]. □

The following Lemma will be useful in the sequel.

Lemma 1.24. *Let $\alpha \le \beta \le \gamma$ be congruences of an algebra $\boldsymbol{X}$.*

(i) *γ/β is Abelian if and only if $(\gamma/\alpha)/(\beta/\alpha)$ is Abelian.*
(ii) *γ/β is central if and only if $(\gamma/\alpha)/(\beta/\alpha)$ is central.*
(iii) *γ/β is strongly Abelian if and only if $(\gamma/\alpha)/(\beta/\alpha)$ is strongly Abelian.*

Proof. Note that $t([x]_\alpha, \overline{[u]_\alpha}) = [t(x,\bar{u})]_\alpha$ and that

$$[t(x,\bar{u})]_\alpha\ \beta/\alpha\ [t(x,\bar{v})]_\alpha \iff t(x,\bar{u})\ \beta\ t(x,\bar{v})$$

(i) Let $\bar{u}\ \gamma\ \bar{v}$ and $x\ \gamma\ y$. Abelianness of γ/β, given by the condition

$$t(x,\bar{u})\ \beta\ t(x,\bar{v}), \iff t(y,\bar{u})\ \beta\ t(y,\bar{v})$$

is therefore equivalent to condition

$$t([x]_\alpha, \overline{[u]_\alpha})\ \beta/\alpha\ t([x]_\alpha, \overline{[v]_\alpha}) \iff t([y]_\alpha, \overline{[u]_\alpha})\ \beta/\alpha\ t([y]_\alpha, \overline{[v]_\alpha})$$

which states Abelianness of $(\gamma/\alpha)/(\beta/\alpha)$.

(ii) - (iii) The very same argument applies. □

1.3. **Maltsev Conditions.** A strong *Maltsev condition* S consists of a finite set of function symbols $\{f_i,\ i \in I\}$ of various arities along with a finite set of equations Σ, involving terms over the f_i. A Maltsev condition is said do be *trivial* if any algebra satisfies it.

A Maltsev condition is said to be *idempotent* if it involves *idempotent terms*, i.e., terms satisfying

$$t(x,\dots,x) \approx x$$

For instance, some properties of the congruence lattice of an algebra $\mathbf{X}$ are defineable by strong Maltsev conditions.

Theorem 1.25. [24] *Let $\mathcal{V}$ be a variety algebra. Then the following are equivalent:*

(1) *$\alpha\beta = \beta\alpha$ for every $\alpha, \beta \in Con(\boldsymbol{X})$ and every $\boldsymbol{X} \in \mathcal{V}$;*
(2) *there exists an idempotent ternary term m, such that*

$$m(x,y,y) \approx m(y,y,x) \approx x$$

called Maltsev term.

Algebras satisfying a non trivial idempotent Maltsev condition have a *Taylor term*, defined as follows.

Definition 1.26. [2, Definition 1.2.2] An n-ary idempotent term t is a *Taylor* term if, for every coordinate $i \le n$, t satisfies an identity of the form

$$t(x_1,...,x_n) \approx t(y_1,...,y_n),$$

where $x_1,...,x_n, y_1,...,y_n \in \{x,y\}$ and $x_i = x,\ y_i = y$.

An algebra with a Taylor term is called *Taylor* algebra. If it has a Maltsev term, then it is called *Maltsev* algebra.

Note that if $\mathbf{X}$ is Taylor (Maltsev) algebra, then $\mathbf{Y}$ is Taylor (Maltsev) for every $\mathbf{Y} \in \mathcal{V}(\mathbf{X})$. More generally if $\mathbf{X}$ satisfies any Maltsev condition, then any algebra in $\mathcal{V}(\mathbf{X})$ does.

Some strong Maltsev conditions have been characterized in [2] for finite idempotent algebras.

Theorem 1.27. [2, Theorem 1.1] *Let $\boldsymbol{X}$ be a finite idempotent algebra. Then the following are equivalent:*

(1) *$\boldsymbol{X}$ has a Taylor term;*
(2) *$\boldsymbol{P}_2 \notin \mathcal{HS}(\boldsymbol{X})$.*

The class of Taylor algebras in a variety contains all algebras satisfying some non trivial idempotent Maltsev condition.

Corollary 1.28. [19, Lemma 9.4] *Let $\boldsymbol{X}$ be a finite idempotent algebra satisfying a non trivial idempotent Maltsev condition. Then $\boldsymbol{X}$ has a Taylor term.*

Proof. Assume that $\mathbf{P}_2 \in \mathcal{HS}(\mathbf{X})$. Then $\mathbf{P}_2$ satisfies the same non trivial Maltsev condition. Therefore, it is given by identities involving just projection operations, hence it is trivial. □

Another property which is defineable by a strong Maltsev condition is *meet-semidistributivity.*

Definition 1.29. Let $\mathbf{X}$ be an algebra. Then $\mathbf{X}$ satisfies the *meet-semidistributivity* property ($SD(\wedge)$) if

$$\alpha \wedge \beta = \gamma \wedge \beta \implies (\alpha \vee \gamma) \wedge \beta = \alpha \wedge \beta$$

for every $\alpha, \beta, \gamma \in Con(\mathbf{X})$. A variety $\mathcal{V}$ satisfies $SD(\wedge)$ if every algebra in $\mathcal{V}$ does.

This property is characterized by the following Proposition which shows that it is a strong Maltsev condition.

Proposition 1.30. *Let $\boldsymbol{X}$ be a finite idempotent algebra. Then the following are equivalent:*

(1) $\mathcal{V}(\boldsymbol{X})$ *satisfies* $SD(\wedge)$*;*
(2) $\mathcal{V}$ *has an* n*-ary term* t *which, for every* $i \leq n$*, satisfies an identity*

$$t(x_{i,1}, x_{i,2}, \dots, x_{i,n}) \approx t(y_{i,1}, y_{i,2}, \dots, y_{i,n})$$

where $(x_{i,j})$ *and* $(y_{i,j})$ *are* $\{x, y\}$*-matrices such that* $x_{i,j} = y_{i,j}$ *for every* $i \neq j$*, and* $x_{i,i} = x$*,* $y_{i,i} = y$ *for every* i*;*
(3) $\mathcal{HS}(\boldsymbol{X})$ *does not contain any simple Abelian algebra.*

The equivalence between (1) and (2) follows by Theorem 1.3 of [2] and the equivalence between (1) and (2) follows by the characterization of a meet-semidistributive variety ([19, Theorem 9.10]) by virtue of Proposition 3.1 of [31].

2. Left-Qasigroupss and Quasigroups

2.1. **Left-Quasigroups.** The variety of *Quandles* is a variety of algebras of type (2,2) which is contained in the variety of *Left-Qasigroups* (LQGs). Some of the results shown in this thesis will be developed in this bigger variety. Dually, quandles can be defined as *Right-quasigroups* (RQGs), as often happens in the literature. All the following statements about LQGs have a dual version holding for RQGs.

There are many equivalent ways to define LQGs. We start with a universal algebraic definition.

Definition 2.1. Let X be a set

(a) A *LQG* (LQG) is an algebra $\mathbf{X} = (X, \cdot, \backslash)$ of type (2,2) such that

$$x \cdot (x \backslash y) \approx y, \quad x \backslash (x \cdot y) \approx y \tag{5}$$

(b) A *Right-quasigroup* (RQG) is an algebra $\mathbf{X} = (X, \cdot, /)$ of type (2,2) such that

$$(y \cdot x)/x \approx y, \quad (y/x) \cdot x \approx y \tag{6}$$

The operation $\cdot$ is called *multiplication*, $\backslash, /$ respectively *left* and *right division.*

Remark 2.2. *Equation (5) is equivalent to have unique solution to the equation*

$$a \cdot x = b$$

for every $a, b \in X$*. This property is called unique left-division.*

Another equivalent way to characterize LQGs is claiming that *left multiplications* are bijections.

Proposition 2.3. *Let $\boldsymbol{X} = (X, \cdot, \backslash)$ be an algebra of type (2,2). Then the following are equivalent:*

(1) *$\boldsymbol{X}$ is a LQG;*
(2) *$\boldsymbol{X}$ has the unique left-division property;*
(3) *the map*

$$L_x : X \longrightarrow X, \quad y \mapsto x \cdot y$$

is bijective for every $x \in X$.

The map L_x is called *left multiplication by x*. Note that $L_x^{-1}(y) = x\backslash y$ for every $x, y \in X$ and in order to define a LQG structure on X it is enough to specify the set of left multiplications.

Example 2.4. (a) Let X be a set. Then $\mathbf{P\text{-}LQ}_{|X|} = (X, \pi_2^2)$ is a LQG, where $xy = y$ for every $x, y \in X$. It will be called *projection LQG.*

(b) Let X be a set and $L : X \longrightarrow \mathrm{Sym}(X)$ be any map. Then $\mathbf{X} = (X, \cdot, \backslash)$ where

$$x \cdot y = L(x)(y), \quad x\backslash y = L(x)^{-1}(y)$$

is a LQG.

Notation 2.5. *In the sequel the multiplication will be denoted just by juxtaposition. In order to avoid the use of parenthesis the following notation will be used*

$$\begin{aligned} x(yz) &\approx x \cdot yz \\ x \cdot y\backslash z &\approx x(y\backslash z) \\ (xy)\backslash(zu) &\approx xy\backslash zu \end{aligned}$$

Let us introduce some interesting subclasses of LQGs.

Definition 2.6. A LQG $\mathbf{X}$ is called

(a) *left-distributive* if

$$x \cdot yz \approx xy \cdot xz$$

(b) *right-distributive* if

$$xy \cdot z \approx xz \cdot yz$$

(c) *distributive* if it is both left and right-distributive;
(d) *idempotent* if

$$x \cdot x \approx x$$

(e) *medial* if

$$xy \cdot zt \approx xz \cdot yt$$

(e) *involutory* if

$$x \cdot xy \approx y$$

All these classes are subvarieties of the variety of LQGs, since they are defined by term identities.

Item (3) of Proposition 2.3, allows to define a subgroup of $\mathrm{Sym}(X)$ by using the left multiplications.

Definition 2.7. Let $\mathbf{X}$ be a LQG. The group $LMlt(\mathbf{X}) = \langle L_x,\ x \in X \rangle$ is called the *left multiplication group* of $\mathbf{X}$.

Note that $\mathbf{X}$ is left-distributive if and only if all the left multiplications are automorphisms. It follows by the following very well known fact.

Fact 2.8. *Let $\boldsymbol{X}$ be a LQG. Then $\alpha \in Aut(\boldsymbol{X})$ if and only if*

$$L_{\alpha(x)} = \alpha L_x \alpha^{-1}$$

for every $x \in X$.

Lemma 2.9. *A LQG $\boldsymbol{X}$ is left-distributive if and only if $LMlt(\boldsymbol{X})$ is a normal subgroup of $Aut(\boldsymbol{X})$.*

Proof. By Fact 2.8, $L_x \in Aut(\mathbf{X})$ if and only if $L_{xy} = L_x L_y L_x^{-1}$ for every $y \in X$. This identity is equivalent to have

$$xy \cdot xz = x \cdot yz$$

for every $x, y, z \in X$, which is the definition of left-distributivity.

Let $\alpha \in Aut(\mathbf{X})$, then $L_{\alpha(x)} = \alpha L_x \alpha^{-1}$ for every $x \in X$, therefore $LMlt(\mathbf{X})$ is a normal subgroup of $Aut(\mathbf{X})$. □

Corollary 2.10. *Let $\boldsymbol{X}$ be a left-distributive LQG. Then $\{L_x,\ x \in X\}$ is a union of conjugacy classes in $Aut(\boldsymbol{X})$.*

In the next Lemma we show that a surjective morphisms of LQGs induces a map between the respective left multiplication groups. This construction was already known in the quandle setting ([4, Theorem 1.27]), and it can be easily extended to LQGs.

Lemma 2.11. *Let $\boldsymbol{X}$ be a LQG and α be its congruence. Then the mapping*

$$\pi_\alpha^* : LMlt(\boldsymbol{X}) \longrightarrow LMlt(\boldsymbol{X}/\alpha), \quad L_{x_1}^{a_1} \dots L_{x_n}^{a_n} \mapsto L_{[x_1]}^{a_1} \dots L_{[x_n]}^{a_n}$$

is a surjective group morphism.

Proof. If the map is well defined then the claim follows by definition.
Let assume that $L_{x_1}^{a_1} \dots L_{x_n}^{a_n} = L_{x_1'}^{b_1} \dots L_{x_m'}^{b_m}$. Then

$$\begin{aligned} [L_{x_1}^{a_1} \dots L_{x_n}^{a_n}(y)] &= [L_{x_1'}^{b_1} \dots L_{x_m'}^{b_m}(y)] \\ L_{[x_1]}^{a_1} \dots L_{[x_n]}^{a_n}[y] &= L_{[x_1']}^{b_1} \dots L_{[x_m']}^{b_m}[y] \end{aligned}$$

for every $[y] \in \mathbf{X}/\alpha$. Therefore, the map is well defined. □

2.2. **Quasigroups.** *Quasigroup* are algebras which have a structure of LQG and of RQG at the same time.

Definition 2.12. Let X be a set. A *Quasigroup* (QG) is an algebra $\mathbf{X} = (X, \cdot, \backslash, /)$ of type (2,2,2) such that $(X, \cdot, \backslash)$ is a LQG and $(X, \cdot, /)$ is a RQG.

A characterization of quasigroups follows by Proposition 2.3.

Proposition 2.13. *Let $\boldsymbol{X} = (X, \cdot, \backslash, /)$ be an algebra of type $(2,2,2)$. The following are equivalent:*

(1) *$\boldsymbol{X}$ is a quasigroup;*
(2) *$\boldsymbol{X}$ has the unique left-division and the unique right-division properties;*

(3) *the maps defined by setting*

$$L_x : X \longrightarrow X, \qquad y \mapsto xy$$
$$R_x : X \longrightarrow X, \qquad y \mapsto yx$$

are bijections for every $x \in X$.

Finite quasigroups arise from well known combinatorial objects, called *Latin squares*.

Fact 2.14. *A finite algebra $\mathbf{X} = (X, \cdot, \backslash, /)$ of type (2,2,2) is a quasigroup if and only if the table of $\cdot$ is a Latin square.*

There is a set of permutations that can be defined for any quasigroup $\mathbf{X}$. These maps are defined both in [28] and [12] and we denote them as in [28].

Definition 2.15. [12, Section 1] Let $\mathbf{X}$ be a finite quasigroup. Let $x \in X$, Then the map M_x defined by setting

$$M_x : X \to X, \quad y \mapsto L_y^{-1}(x) = y\backslash x$$

is called *right middle translation*.

Remark 2.16. *It is easy to see that the map M_x is a permutation. Its inverse is given by*

$$M_x^{-1} : X \to X, \quad y \mapsto R_y^{-1}(x) = y/x$$

and it is called left middle translation (see Proposition 1.1 of [12]*).*

Proposition 2.17. [12, Proposition 2.3] *Let $\mathbf{X}$ be a finite quasigroup. Then the map $M_x M_y^{-1}$ has no fixed points whenever $x \neq y$.*

2.3. **Homogeneous and Connected LQGs.** Any LQG $\mathbf{X}$ partitions in the disjoint union of the orbits under the natural action of $Aut(\mathbf{X})$ or of $LMlt(\mathbf{X})$. The orbits under $LMlt(\mathbf{X})$ are subalgebras of $\mathbf{X}$ and in order to describe the structure of $\mathbf{X}$ we need to study the structure of these subalgebras and the way they act one on each other. For this reason a good starting point is to study LQGs for which this actions is transitive.

The original contribution of this Section is to extend Proposition 2.20, already known for quandles, to LQGs, and to give an universal algebraic characterization of connected LQGs (Corollary 2.21).

Definition 2.18. Let $\mathbf{X}$ be a LQG. Then

(a) it is *homogeneous* if $Aut(\mathbf{X})$ acts transitively;
(b) it is *connected* if $LMlt(\mathbf{X})$ acts transitively;
(c) the *connected component of* x is the orbit of x under the action of $LMlt(\mathbf{X})$.

The orbits with respect to these two groups can be very different. Let $\mathbf{P\text{-}LQ}_n$ be the projection LQG of size n, then $Aut(\mathbf{P\text{-}LQ}_n) = \mathrm{Sym}(n)$ and $LMlt(\mathbf{P\text{-}LQ}_n) = \{1\}$. Hence, it is homogeneous but totally disconnected. Examples of connected LQGs come from quasigroups.

Lemma 2.19. *Let $\mathbf{X} = (X, \cdot, \backslash, /)$ be a quasigroup. Then $\mathbf{X}_L = (X, \cdot, \backslash)$ is a connected LQG.*

Proof. Let $x, y \in X$. Then there exists a unique $z \in X$ such that $y = R_x(z) = L_z(x)$, since R_x is a bijection for every $x \in X$. Therefore, $\mathbf{X}$ is connected. □

The set of the connected components endowed with the projection LQG structure will be denoteby by $\pi_0(\mathbf{X})$. The map π_0 which assigns to every element x its connected component is a morphism. Indeed,

$$\begin{aligned} \pi_0(xy) &= \pi_0(y) = \pi_0(x) \cdot \pi_0(y) \\ \pi_0(x \backslash y) &= \pi_0(y) = \pi_0(x) \backslash \pi_0(y) \end{aligned}$$

Therefore, $\pi_0(\mathbf{X}) \simeq \mathbf{X}/ker(\pi_0)$. An analogous categorical construction was already known in Proposition 2.30 of [13] for quandles, but left-distributivity is not necessary.

The congruence $ker(\pi_0)$ is the smallest congruence of $\mathbf{X}$ with projection factor.

Proposition 2.20. *Let $\boldsymbol{X}$ be a LQG and α be its congruence. Then $\boldsymbol{X}/\alpha$ is a projection LQG if and only if $ker(\pi_0) \leq \alpha$.*

Proof. Let $ker(\pi_0) \leq \alpha$. By Proposition 1.16, there exists $\pi : \mathbf{X}/ker(\pi_0) \longrightarrow \mathbf{X}/\alpha$ and then $\mathbf{X}/\alpha$ is a projection LQG.

Let $\mathbf{X}/\alpha$ be a projection LQG and $x \ ker(\pi_0) \ y$, i.e. there exists $h \in LMlt(\mathbf{X})$ such that $y = h(x) \in \mathbf{X}$. Then

$$\pi_\alpha(y) = \pi_\alpha(h(x)) = \pi_\alpha^*(h)(\pi_\alpha(x)) = \pi_\alpha(x)$$

since $LMlt(\mathbf{X}/\alpha)$ is trivial. Therefore, $ker(\pi_0) \leq \alpha$. □

Corollary 2.21. *Let $\boldsymbol{X}$ be a LQG. Then the following are equivalent*

(1) *$\boldsymbol{X}$ is connected;*
(2) *$|\pi_0(\boldsymbol{X})| = 1$;*
(3) *$\boldsymbol{P}$-$\boldsymbol{LQ}_2 \notin \mathcal{H}(\boldsymbol{X})$.*

Proof. (1) ⇔ (2) It follows by definition of $\pi_0(\mathbf{X})$.

(2) ⇔ (3) By Propositions 1.16 and 2.20, $\mathbf{P}$-$\mathbf{LQ}_2 \in \mathcal{H}(\mathbf{X})$ if and only if $\mathbf{P}$-$\mathbf{LQ}_2 \in \mathcal{H}(\pi_0(\mathbf{X}))$, which is equivalent to have $|\pi_0(\mathbf{X})| \geq 2$. □

As a Corollary we get that the class of connected LQGs is closed under $\mathcal{H}$.

Corollary 2.22. *Every homomorphic image of a connected LQG is connected.*

Remark 2.23. *It is straightforward to see that the class of connected LQGs is also closed under $\mathcal{P}$.*

3. Racks and Quandles

3.1. **Definitions and Examples.** In this Section some well known facts about racks and quandles are shown. In particular we give a brief summary of the theory of connected quandles, which is the most studied class of quandles ([1], [4], [14], [17], [22], [20], [25] and [33]).

The class of racks and the class of quandles are subvarieties of the variety of LQGs defined as follows.

Definition 3.1. A LQG $\mathbf{X}$ is said to be

(a) a *rack* if it is left-distributive;

(b) a *quandle* if it is an idempotent rack;
(c) a *crossed set* if it is a quandle X and

$$xy = y \iff yx = x$$

for every $x, y \in X$;
(d) a *Latin* quandle if it is an idempotent left-distributive quasigroup.

All the previous classes but (c) are varieties (they are equational classes). Remarkable examples of quandles arise from groups setting.

Example 3.2. (i) Let X be a set and $\sigma \in \mathrm{Sym}(X)$. Define

$$x \cdot y = L_x(y) = \sigma(y)$$

for every $x, y \in X$. Then $\mathbf{X} = (X, \cdot)$ is a rack called *permutation rack*. Note that $\mathbf{X}$ is a quandle if and only if $\sigma = 1$, therefore, $\mathbf{X} = \mathbf{P\text{-}LQ}_{|X|}$.

(ii) Let G be a group and $H \subseteq G$ a subset closed under conjugation. Let us define

$$x \cdot y = xyx^{-1}$$

for every $x, y \in H$. Then $\mathbf{H}$ is a quandle. It will be called *conjugation quandle* and denoted by $Conj(H)$. Note that every conjugation quandle is a crossed set.

(iii) Let G be a group, $\alpha \in Aut(G)$ and $H \leq Fix(\alpha)$. Consider the set G/H of left cosets with respect to H and define the multiplication by setting

$$xH \cdot yH = x\alpha(x^{-1}y)H$$

The algebra $\mathbf{G/H}$ is a quandle. It will be called *coset* or *Galkin quandle* and denoted by $\mathcal{Q}(G, H, \alpha)$.
If $H = \{1_G\}$, the quandle is called *principal coset quandle* and denoted by $\mathcal{Q}(G, \alpha)$.

(iv) Let $\mathbf{X}$ be a rack and let $L(\mathbf{X})$ be the set of all the left multiplications of $\mathbf{X}$. Then $Conj(L(X))$ is a quandle (see Corollary 2.10). Moreover the map

$$L_{\mathbf{X}} : \mathbf{X} \longrightarrow L(\mathbf{X}), \quad x \mapsto L_x$$

is a surjective morphism of racks.

Properties of an algebra depend on its term operations. Quandle term operations have a standard representation.

Lemma 3.3. *Let $t(x_1, \dots, x_n)$ be a quandle term operation. Then there are $y_1, \dots, y_m, y \in \{x_1, \dots, x_n\}$ and $k_i \in \{\pm 1\}$ such that*

$$t(x_1, \dots, x_n) = L_{y_1}^{k_1} \dots L_{y_m}^{k_m}(y)$$

is an identity valid in every quandle.

Proof. Let n be the number of occurrences of variables in the term t. If $n = 1$, then $t(x) = x$. Let $t(x_1, \dots, x_n)$ be a quandle term. Then there exists terms s, r such that

$$t(x_1, \dots, x_n) = L_{s(x_{i_1}, \dots x_{i_k})}^{\pm 1}(r(x_{j_1}, \dots, x_{j_l}))$$

and the number of occurrences of the variables in r and s is less then n and $\{x_{i_1},\dots x_{i_k},x_{j_1},\dots,x_{j_l}\}\subseteq\{x_1,\dots,x_n\}$. By induction,

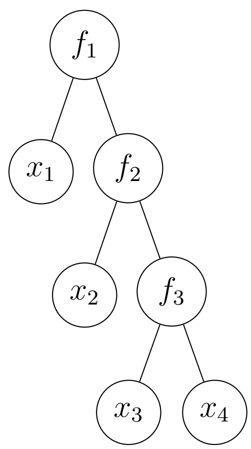
$$\begin{aligned} s(x_{i_1},\dots x_{i_k}) &= L_{x_{s_1}}^{a_1}\dots L_{x_{s_p}}^{a_p}(x_s) \\ r(x_{j_1},\dots,x_{j_l}) &= L_{x_{r_1}}^{b_1}\dots L_{x_{r_q}}^{b_q}(x_r) \end{aligned}$$

where $\{x_{s_1},\dots x_{s_p},x_s,x_{r_1},\dots,x_{r_q},x_r\}\subseteq\{x_1,\dots,x_n\}$ and a_i and b_j are ±1. Therefore,

$$\begin{aligned} t(x_1,\dots,x_n) &= L^{\pm1}_{s(x_{i_1},\dots x_{i_k})}(r(x_{j_1},\dots,x_{j_l})) = \\ &= L_{x_{s_1}}^{a_1}\dots L_{x_{s_p}}^{a_p}L_{x_s}^{\pm1}(L_{x_{s_1}}^{a_1}\dots L_{x_{s_p}}^{a_p})^{-1}L_{x_{r_1}}^{b_1}\dots L_{x_{r_q}}^{b_q}(x_r) \end{aligned}$$

□

The previous Lemma shows that every quandle term can be written as the following one



where $f_i\in\{\cdot,\backslash\}$.

3.2. **Homogeneous and Connected Quandles.** The classes of homogeneous quandles and of connected quandles has been studied a lot in the literature.

The most important result we show in this Section is that any homogeneous quandle is isomorphic to a coset quandles, as has been proved by Joyce in Theorem 7.1 of [22].

All properties but labels are shared by elements belonging to the same orbits of $Aut(\mathbf{X})$.

Proposition 3.4. *Let $\boldsymbol{X}$ be a rack and let $x,y\in X$ belong to the same orbit under the action of $Aut(\boldsymbol{X})$. Then L_x and L_y have the same cycle structure as permutations.*

If $\boldsymbol{X}$ is a homogeneous, then all the left multiplications have the same cycle structure.

The main examples of homogeneous quandles are given by coset quandles.

Remark 3.5. *Let $\boldsymbol{X}=\mathcal{Q}(G,H,\alpha)$ be a coset quandle and λ be the canonical left action of G on G/H. Note that*

$$\begin{aligned} \lambda(g)(xH\cdot yH) &= g(xH\cdot yH)=gx\alpha(x^{-1}y)H= \\ &= gx\alpha(x^{-1}g^{-1}gy)H=gxH\cdot gyH \end{aligned}$$

$$= \quad \lambda(g)(xH)\cdot\lambda(g)(yH)$$

Then λ *is an action by automorphisms and it is transitive. Therefore,* $\boldsymbol{X}$ *is homogeneous. Left and right multiplications are determined by the automorphism* α *and by the action* λ*:*

$$L_{xH} = \lambda(x)L_H\lambda(x)^{-1}, \quad R_{xH} = \lambda(x)R_H\lambda(x)^{-1}$$

for every $x \in G$*, where*

$$L_H(xH) = \alpha(x)H, \quad R_H(xH) = x\alpha(x^{-1})H = t(x)H$$

for every $x \in G$*.*

The following theorem shows how a transitive action by automorphisms on a quandles provides a representation of the quandle as a coset quandle.

Theorem 3.6. [22, Theorem 7.1] *Let* $\boldsymbol{X}$ *be a quandle,* $x \in X$ *and* G *be a group acting transitively on* X *and such that* $L_x G L_x^{-1} = G$*. Then*

$$\boldsymbol{X} \simeq \mathcal{Q}(G, G_x, \widehat{L_x})$$

where $\widehat{L_x}(g) = L_x g L_x^{-1}$*.*

The existence of a coset representation is actually a characterization of homogenous quandles, since any coset quandles is homogeneous as we have seen in Remark 3.5.

Proposition 3.7. *A quandle* $\boldsymbol{X}$ *is homogeneous if and only if* $\boldsymbol{X} \simeq \mathcal{Q}(G, H, \alpha)$ *for some group* G*,* $\alpha \in Aut(G)$ *and* $H \leq Fix(\alpha)$*.*

Because of this characterization, a coset representation is also called *homogenous representation.*

Remark 3.8. *Canonical representations for a homogeneous quandle* $\boldsymbol{X}$ *is given by* $\boldsymbol{X} \simeq \mathcal{Q}(Aut(\boldsymbol{X}), Aut(\boldsymbol{X})_x, \widehat{L_x})$ *for every* $x \in X$*. If* $\boldsymbol{X}$ *is connected then* $\boldsymbol{X} \simeq \mathcal{Q}(LMlt(\boldsymbol{X}), LMlt(\boldsymbol{X})_x, \widehat{L_x})$ *for every* $x \in X$*.*

A homogeneous representation allows us to do concrete computations as follows.

Proposition 3.9. *Let* $\boldsymbol{X} = \mathcal{Q}(G, H, \alpha)$*, then*

$$x_0 H \cdot (x_1 H \cdot (\ldots \cdot (\ldots \cdot (x_{n-1}H \cdot x_n H)))) = x_0 \prod_{k=1}^{n} \alpha^k \left(x_{k-1}^{-1} x_k\right) H$$

for every $x_0, \ldots, x_n \in G$*.*

Proof. It follows easily by an inductive argument. □

A homogeneous representation is called *principal* if the coset quandle is principal and *affine* if the group G is Abelian.

Definition 3.10. Let $\mathbf{X}$ be a quandle. It is said to be

(a) *principal* if it has a principal coset representation;
(b) *affine* if it has an affine coset representation.

The homogeneous representation is not unique. For instance, any connected quandles have at least two homogeneous represention, given by $Aut(\mathbf{X})$ and by $LMlt(\mathbf{X})$.

Remark 3.11. *By Lemma 3.3 of* [4], $\mathcal{Q}(G, H, \alpha)$ *is somorphic to* $\mathcal{Q}(G/N, H/N, \alpha_N)$, *for every* $N \trianglelefteq G$, $N \leq H$, *where* $\alpha_N(xN) = \alpha(x)N$ *for every* $x \in G$. *If* G *is Abelian then*

$$\mathcal{Q}(G, H, \alpha) \simeq \mathcal{Q}(G/H, \alpha_H)$$

The previous remark says that normal subgroups of G in H can be factored out in order to get a new homogeneous representation. This fact shows that every affine quandle is principal and leads to the following definition of reduced representation.

Definition 3.12. [4, Definition 3.4] Let $\mathbf{X} = \mathcal{Q}(G, H, \alpha)$ be a homogeneous quandle. If $\mathrm{Core}_G(H) = \{1\}$, then the representation is called *reduced*.

Lemma 3.13. *Every homogeneous quandle has a reduced representation.*

Proof. Let $\mathcal{Q}(G, H, \alpha)$ be a homogeneous representation and $K = \mathrm{Core}_G(H)$. By Remark 3.11,

$$\mathcal{Q}(G/K, H/K, \alpha_K) \simeq \mathcal{Q}(G, H, \alpha)$$

and H/K is core-free. ☐

3.3. **Transvection group and Minimal Homogeneous Representation.** A subgroup of the left multiplications group which play a very important role in the theory is the *transvection group*. Its most important feature is to provide a *minimal* homogeneous representation for connected quandles (see Theorem 4.1 of [20]). The minimality of this representation yields to the characterization of several classes of connected quandles through the properties of the transvection group (see for instance Proposition 4.2 and Corollary 4.4).

The transvection group is a powerful tool in the theory of quandles in general. A lot of quandle-theoretical properties can be translated to group-theoretical properties of the transvection group. For instance mediality has been characterized through Abelianness of the transvection group in Proposition 2.1 of [21].

The transvection group is defined as follows.

Definition 3.14. Let $\mathbf{X}$ be a rack, then

$$Dis(\mathbf{X}) = \langle L_x L_y^{-1},\ x, y \in X\rangle$$

is called *transvection group* or *displacements group* of $\mathbf{X}$.

The main features of the transvection group are summarized in the next Proposition.

Proposition 3.15. [20, Proposition 2.1] *Let* $\boldsymbol{X}$ *be a rack then:*

(i) $Dis(\boldsymbol{X}) = \langle L_y^{-1} L_x,\ y \in X\rangle$ *for every* $x \in X$*;*
(ii) $Dis(\boldsymbol{X}) = \{L_{x_1}^{a_1} \dots L_{x_n}^{a_n},\ x_i \in X,\ n, a_i \in \mathbb{N}$ *such that* $\sum_{i=1}^{n} a_i = 0\}$*;*
(iii) $Dis(\boldsymbol{X})$ *is a normal subgroup of* $Aut(\boldsymbol{X})$*;*
(iv) $LMlt(\boldsymbol{X}) = Dis(\boldsymbol{X})\langle L_x\rangle$ *for every* $x \in X$*;*
(v) $Dis(\boldsymbol{X})$ *and* $LMlt(\boldsymbol{X})$ *have the same orbits;*
(vi) *if* $\boldsymbol{X}$ *is connected then* $Dis(\boldsymbol{X}) = LMlt(\boldsymbol{X})^{(1)}$*.*

The induced morphism of groups showed in Proposition 2.11, restricts to a morphism of groups between transvection groups.

Proposition 3.16. [4, Theorem 1.27] *Let* $\boldsymbol{X}$ *be a rack and* α *be its congruence. Then* π_α^* *restricts to a surjective morphism of groups between* $Dis(\boldsymbol{X})$ *and* $Dis(\boldsymbol{X}/\alpha)$*.*

Remark 3.17. *By item (v) of Proposition 3.15, the transvection group provides a homogeneous representation for connected quandles. Then*

$$\boldsymbol{X} \simeq \mathcal{Q}(Dis(\boldsymbol{X}), Dis(\boldsymbol{X})_x, \widehat{L_x})$$

for any connected quandle $\boldsymbol{X}$*.*

This representation allows to characterize some classes of quandles. Furthermore it fulfils a minimality condition among the homogeneous representations in the following sense.

Proposition 3.18. [20, Theorem 4.1] *Let* $\boldsymbol{X} \simeq \mathcal{Q}(G, H, \alpha)$ *be a connected quandle. Then* $Dis(\boldsymbol{X})$ *embeds in a quotient of* G*.*

The homogeneous representation of a connected quandle given by the transvection group is then called *minimal.*

Corollary 3.19. *Let* $\boldsymbol{X}$ *be a finite connected quandle. Then the minimal homogeneous representation is reduced.*

Proof. Let $K \leq Dis(\mathbf{X})_x$ be a normal subgroup of $Dis(\mathbf{X})$. Then

$$\mathcal{Q}(Dis(\mathbf{X})/K, Dis(\mathbf{X})_x/K, (\widehat{L_x})_K)$$

is a homogeneous representation of $\mathbf{X}$. By Corollary 3.18, $Dis(\mathbf{X})$ embeds into a quotient of $Dis(\mathbf{X})/K$, hence K is trivial. □

In the sequel, the following notation will be used

Notation 3.20. *Let* G *be a group and* $\alpha \in Aut(G)$*, then*

$$[G, \alpha] = \langle x\alpha(x^{-1}),\ x \in G\rangle$$

Proposition 3.21. *Let* G *be a group,* $\alpha \in Aut(G)$ *and* $Fix(\alpha)$ *be a core-free subgroup. Then* $Dis(\mathcal{Q}(G, H, \alpha)) \simeq [G, \alpha]$ *for every* $H \leq Fix(\alpha)$*.*

Proof. If $Fix(\alpha)$ is core-free, then $\mathcal{Q}(G, H, \alpha)$ is a reduced homogeneous representation for every $H \leq Fix(\alpha)$. Then by Proposition 3.12 of [4], it follows that

$$Dis(\mathcal{Q}(G, H, \alpha)) \simeq [G, \alpha]$$

for every $H \leq Fix(\alpha)$. □

Remark 3.22. *Accordingly to Lemma 3.11 of* [4]*, the action of the transvection group of a coset quandle* $\boldsymbol{X} = \mathcal{Q}(G, H, \alpha)$ *is given by the left action of* $[G, \alpha]$ *on the set* G/H*. Therefore, if* $\boldsymbol{X} = \mathcal{Q}(Dis(\boldsymbol{X}), Dis(\boldsymbol{X})_x, \widehat{L_x})$ *is connected, then* $\boldsymbol{Y}_H = \mathcal{Q}(Dis(\boldsymbol{X}), H, \widehat{L_x})$ *is connected for every* $H \leq Dis(\boldsymbol{X})_x$*.*

3.4. **Faithful Quandles.** The class of *faithful* quandles is an important class of quandles and its definition is quite natural in quandle setting. All the results of this Section but Lemma 3.23 and Proposition 3.24 are just a restatement of some known facts about faithful quandles.

Every variety of algebras of a given type with its algebra morphisms form a category. So racks together with morphisms of racks form a category, and quandles with morphisms of quandles form a subcategory of it.

The set of the left multiplications of a LQG is a subset of a permutations group. In general it has no natural algebraic structure. If $\mathbf{X}$ is a rack, as noticed in example 3.2 (iv), the set of all left multiplications has a structure of conjugation quandle and the map $L_{\mathbf{X}}$ is a surjective morphism of rack. Therefore, $Conj(L(\mathbf{X})) \simeq \mathbf{X}/ker(L_{\mathbf{X}})$ and it will be denoted simply by $L(\mathbf{X})$.

Lemma 3.23. *Let $\boldsymbol{X}$ and $\boldsymbol{Y}$ be racks and $\phi : \boldsymbol{Y} \longrightarrow \boldsymbol{X}$ be a rack morphism. Then there exists a unique quandle morphism $L(\phi) : L(\boldsymbol{Y}) \longrightarrow L(\boldsymbol{X})$ such that the following diagram is commutative*

(7)
$$\begin{array}{ccc} \boldsymbol{Y} & \xrightarrow{\phi} & \boldsymbol{X} \\ \downarrow{\scriptstyle L_{\boldsymbol{Y}}} & & \downarrow{\scriptstyle L_{\boldsymbol{X}}} \\ L(\boldsymbol{Y}) & \xrightarrow{L(\phi)} & L(\boldsymbol{X}) \end{array}$$

Proof. In order to make the diagram to commute, $L(\phi)$ has to be defined by setting $L(\phi)(L_y) = L_{\phi(y)}$ for every $x \in Y$. This map is a quandle morphism, since

$$\begin{aligned} L(\phi)(L_x \cdot L_y) &= L(\phi)(L_{xy}) = L_{\phi(xy)} = L_{\phi(x)\phi(y)} = \\ &= L_{\phi(x)} \cdot L_{\phi(y)} = L(\phi)(L_x) \cdot L(\phi)(L_y) \end{aligned}$$

for every $x, y \in y$. □

This Lemma allows to define the following functor between the category of racks (**Racks**) and the category of quandles (**Qnd**). Let $\mathcal{U}$ be the forgetful functor from **Qnd** to **Racks** and I be the identity functor on **Racks**. Then we can define a natural transformation from I to $\mathcal{U}L$.

Proposition 3.24. *Let L : **Racks** $\longrightarrow$ **Qnd**, defined by setting*

$$\boldsymbol{X} \mapsto L(\boldsymbol{X}), \qquad \phi : \boldsymbol{Y} \longrightarrow \boldsymbol{X} \mapsto L(\phi) : L(\boldsymbol{Y}) \longrightarrow L(\boldsymbol{X})$$

*is a covariant functor and the family of morphisms $\{L_{\boldsymbol{X}},\ \boldsymbol{X} \in$ **Racks**$\}$ is a natural transformation from I to $\mathcal{U}L$.*

Proof. It is easy to show that $L(\phi \circ \psi) = L(\phi) \circ L(\psi)$ and that $L(id_X) = id_{L(\mathbf{X})}$. The second claim follows by the commutativity of diagram (7). □

The map defined in Lemma 3.23 in general does not extend to a group morphism between $LMlt(\mathbf{Y})$ and $LMlt(\mathbf{X})$ (which means that the functor L does not lift to a functor from **Racks** to **Grps**). Let $\mathbf{X}$ be a quandle and $\mathbf{P}$-$\mathbf{LQ}_1$ be the trivial quandle. Let $x \in X$ such that $L_x \neq 1$. The map $i_x : \mathbf{P\text{-}LQ}_1 \longrightarrow \mathbf{X}$, with range $\{x\}$ is a quandle morphism, but

$$\{1\} \longrightarrow LMlt(\mathbf{X}), \quad L_x \mapsto L_{i(x)}$$

is not a group morphism.

Remark 3.25. *Proposition 2.11 shows that this assignment is well defined for surjective morphism. Then we can define a functor LMlt between the categories of racks (LQGs) and surjective morphisms and the category of groups and surjective morphisms, given by*

$$\begin{array}{rcl} \boldsymbol{X} & \mapsto & LMlt(\boldsymbol{X}) \\ \pi_\alpha : \boldsymbol{X} \longrightarrow \boldsymbol{X}/\alpha & \mapsto & \pi_\alpha^* : LMlt(\boldsymbol{X}) \longrightarrow LMlt(\boldsymbol{X}/\alpha) \end{array}$$

In general the map $L_{\mathbf{X}}$ is not injective.

Definition 3.26. A quandle $\mathbf{X}$ is said to be *faithful* if $ker(L_{\mathbf{X}}) = 0_{\mathbf{X}}$.

Since $L_{\mathbf{X}}$ is always surjective, faithful quandles are those for which it is injective. The definition is restricted to quandle, since any faithful rack would necessarily be a quandle. Actually, since any faithful quandle is isomorphic to a conjugation quandle, it is also a crossed sets.

Proposition 3.27. *Any faithful quandle is a crossed set.*

Let $\mathbf{X}$ be a quandle and $h \in LMlt(\mathbf{X})_x$. Then

$$hL_x h^{-1} = L_{h(x)} = L_x$$

Hence, $LMlt(\mathbf{X})_x \leq C_{LMlt(\mathbf{X})}(L_x)$ for every $x \in X$. The equality holds for faithful quandles.

Proposition 3.28. *Let $\boldsymbol{X}$ be a faithful quandle. Then $LMlt(\boldsymbol{X})_x = C_{LMlt(\boldsymbol{X})}(L_x)$ for every $x \in X$ and $LMlt(\boldsymbol{X})$ has trivial center.*

Proof. Let $h \in LMlt(\mathbf{X})$, then $L_{h(x)} = hL_x h^{-1}$. So h centralizes L_x if and only if $L_{h(x)} = L_x$. Since $\mathbf{X}$ is faithful this is equivalent to have $h(x) = x$. Central elements of $LMlt(\mathbf{X})$ are given by

$$Z(LMlt(\mathbf{X})) = \bigcap_{x \in X} C_{LMlt(\mathbf{X})}(L_x) = \bigcap_{x \in X} LMlt(\mathbf{X})_x = \{1\}.$$

□

Remark 3.29. *The last Proposition holds for the automorphism group. Let $\boldsymbol{X}$ be a faithful quandle, then $Aut(\boldsymbol{X})_x = C_{Aut(\boldsymbol{X})}(L_x)$ for every $x \in X$.*

The converse is not true. For instance the quandle SmallQuandle(12,1) from the GAP database has centerless left multiplication group but it is not faithful. The following Proposition gives a criterion for faithfulness of reduced representation.

Proposition 3.30. [4, Proposition 3.9] *Let $\boldsymbol{X} = \mathcal{Q}(G, H, \alpha)$ be a reduced homogeneous representation. Then $\boldsymbol{X}$ is faithful if and only if $H = Fix(\alpha)$.*

Connected faithful quandles are characterized by the properties of the stabilizers in $LMlt(\mathbf{X})$. Note that stabilizers of the points (and centralizers of generators of $LMlt(\mathbf{X})$) are pairwise conjugate whenever $\mathbf{X}$ is connected.

Proposition 3.31. *Let $\boldsymbol{X}$ be a connected quandle. Then the following are equivalent*

(1) *$\boldsymbol{X}$ is faithful;*
(2) *$LMlt(\boldsymbol{X})_x = C_{LMlt(\boldsymbol{X})}(L_x)$ for every $x \in X$;*
(3) *$Dis(\boldsymbol{X})_x = C_{LMlt(\boldsymbol{X})}(L_x) \cap Dis(\boldsymbol{X})$ for every $x \in X$.*

Proof. (1) $\Leftrightarrow$ (2) The right implication follows from Proposition 3.28.

Let assume that $LMlt(\mathbf{X})_x = C_{LMlt(\mathbf{X})}(L_x)$ for every $x \in X$ and that $L_x = L_y$. Since $\mathbf{X}$ is connected, $y = h(x)$ for some $h \in LMlt(\mathbf{X})$. Hence,

$$L_x = L_y = hL_xh^{-1} \iff h \in C_{LMlt(\mathbf{X})}(L_x) = LMlt(\mathbf{X})_x$$

and therefore $x = y$.

(1) $\Leftrightarrow$ (3) It follows by Proposition 3.30, since the minimal representation is reduced. □

3.5. **Some subclasses of Faithful quandles.** This Section is about some subclasses of faithful quandles which can be captured by universal algebraic definition. All the contents of the Section are original contributions of the author. In any variety the class of Taylor algebras and the class of Maltsev algebra are worthy of attention. Every quasigroup has a Maltsev term ([19, Lemma 4.6]), then it has a Taylor term. In particular it is true for Latin quandles.

Fact 3.32. *Latin quandles are Maltsev (and thefore Taylor).*

The class of connected quandles is not a variety since it is not closed under $\mathcal{S}$. For instance, there are many examples of connected quandles with projection subquandles. The class of quandle with no projection subquandles can be characterized as follows.

Proposition 3.33. *Let $\boldsymbol{X}$ be a quandle. Then the following are equivalent:*

(1) *$Fix(L_x) = \{x\}$ for every $x \in X$;*
(2) *every projection subquandle of $\boldsymbol{X}$ is trivial;*
(3) *$\boldsymbol{P}\text{-}\boldsymbol{LQ}_2 \notin \mathcal{S}(\boldsymbol{X})$;*
(4) *all the subquandles of $\boldsymbol{X}$ are faithful.*

Proof. (1) $\Rightarrow$ (2) Let Q be a projection subquandle and $x, y \in Q$. Since $xy = y$ implies $y = x$, then $Q = \{x\}$.

(2) $\Rightarrow$ (3) It follows since every subset of a projection quandle is a projection subquandle.

(3) $\Rightarrow$ (4) Let $\mathbf{Y} \in \mathcal{S}(\mathbf{X})$ be non faithful. Then the blocks of $ker(L_{\mathbf{Y}})$ are projection subquandles, i.e. $\mathbf{P}\text{-}\mathbf{LQ}_2 \in \mathcal{S}(\mathbf{Y}) \subset \mathcal{S}(\mathbf{X})$, contradiction.

(4) $\Rightarrow$ (1) The quandle $\mathbf{X}$ is faithful , therefore it is a crossed set by Lemma 3.27. If there exists $x, y \in X$ such that $xy = y$, Then $\{x, y\}$ is a projection subquandle, since it $\mathbf{X}$ is a crossed set. Therefore $\{x, y\}$ is not faithful, contradiction. □

Definition 3.34. A quandle $\mathbf{X}$ is said to be a *strongly faithful* quandle if any subquandle of $\mathbf{X}$ is faithful.

Corollary 3.35. *Let $\boldsymbol{X}$ be a strongly faithful quandle. Then $LMlt(\boldsymbol{X})_x$ is a self-normalizing subgroup.*

Proof. Let assume that h normalizes $LMlt(\mathbf{X})_x$. Then $hL_xh^{-1} = L_{h(x)} \in LMlt(\mathbf{X})_x$. By Proposition 3.33, $h(x) = x$. □

Note that the class of strongly faithful quandles is closed under $\mathcal{S}$ and it is a proper subclass of faithful quandles. For instance, the quandle SmallQuandle(6,1) in the database of the RIG package of software GAP, is faithful but it has projection subquandles of size 2 (more generally any non-simple connected quandle of size $2p$ for some prime p is faithful but have subquandles of size 2 which are projection).

Finite Taylor Quandles have a nice characterization is terms of the properties of subquandles.

Theorem 3.36. *Let $\boldsymbol{X}$ be a finite quandle. Then the following are equivalent:*

(1) *$\boldsymbol{X}$ is a Taylor quandle;*
(2) *all the subquandles of $\boldsymbol{X}$ are connected.*

Proof. Item (1) is equivalent to have $\mathbf{P\text{-}LQ_2} \notin \mathcal{HS}(\mathbf{X})$, by Theorem 1.27.

By Proposition 2.20, $\mathbf{P\text{-}LQ_2} \in \mathcal{HS}(\mathbf{X})$ if and only if some subquandle of $\mathbf{X}$ is not connected. □

This Theorem holds also for idempotent LQGs, since Theorem 1.27 holds for every finite idempotent algebra and the construction of $\pi_0(\mathbf{X})$ can be carried out in this setting.

Remark 3.37. *An idempotent algebra $\boldsymbol{X}$ is Taylor if and only if $\boldsymbol{P}_2$ does not belong to the variety generated by $\boldsymbol{X}$ (*[26, Corollary 5.3]*). Then in particular $\boldsymbol{P}_2 \notin \mathcal{HS}(\boldsymbol{X})$. Therefore, if a quandle is Taylor, then all its subquandles are connected, without any finitess assumption. Moreover $\boldsymbol{P\text{-}LQ}_2 \notin \mathcal{S}(\boldsymbol{X})$, hence all subquandles of $\boldsymbol{X}$ are faithful.*

By virtue of the previous Remark, the class of Taylor quandles is intermediate between Maltsev quandles and strongly faithful quandles. Therefore, for any quandle $\mathbf{X}$, we have

$$\text{Latin} \Rightarrow \text{Maltsev} \Rightarrow \text{Taylor} \Rightarrow \text{strongly faithful} \Rightarrow \text{Faithful} \Rightarrow \text{Crossed Set}$$

The class of Latin quandles is a proper class of Maltsev quandles and Taylor quandles form a proper subclass of strongly faithful quandles.

Remark 3.38. *Let $\boldsymbol{X} = \mathcal{Q}(\mathbb{Z}, \alpha)$, where $\alpha(x) = -x$ for every $x \in \mathbb{Z}$. It satisfies the property $Fix(L_x) = \{x\}$ for every $x \in \mathbb{Z}$ but it is not even connected, since $Im(1-\alpha) = 2\mathbb{Z}$.*

SmallQuandles (28,3), (28,4), (28,5) and (28,6) from the RIG database are Taylor and solvable. Then they are Maltsev but not Latin, by virtue of Corollary 1.6 of [2].

From the analysis of these classes of quandles some natural questions arise.

Problem 1. Give a characterization of Maltsev quandles.

Problem 2. Does the class of Taylor quandles and the class of Maltsev quandles coincide?

4. Principal and Affine Quandle

4.1. **Connected principal quandles.** A subclass of homogeneous quandles is given by principal quandles. They can be found in the literature under different names as *generalized Alexander quandles* ([9]). In this Section we characterize connected principal quandles (Proposition 10.16) which generalizes Corollary 3.20 of [4] dropping the finiteness assumption.

In the following the quandle operation is denoted by $\cdot$ and the group operation just by juxtaposition.

Principal representations correspond to regular actions by automorphism groups invariant under $\widehat{L_x}$.

Proposition 4.1. *Let $\mathbf{X}$ be a quandle and $G \leq Aut(\mathbf{X})$. Then the following are equivalent:*

1. *G acts regularly and it is invariant under $\widehat{L_x}$;*
2. *$\mathbf{X} \simeq \mathcal{Q}(G, \widehat{L_x})$.*

Proof. (1) $\Rightarrow$ (2) The group G is regular and provides a homogeneous representation given by $\mathbf{X} \simeq \mathcal{Q}(G, \widehat{L_x})$, since $G_x = \{1\}$.

(2) $\Rightarrow$ (1) The canonical left action of G on $\mathbf{X}$ is regular. □

The transvection group gives also a characterization of principal and affine connected quandles.

Proposition 4.2. *Let $\mathbf{X}$ be a connected quandle. Then the following are equivalent:*

1. *$Dis(\mathbf{X})$ is regular;*
2. *$\mathbf{X}$ is principal.*

Proof. (1) $\Rightarrow$ (2) If $Dis(\mathbf{X})$ is regular, then $\mathbf{X} \simeq \mathcal{Q}(Dis(\mathbf{X}), \widehat{L_x})$.

(2) $\Rightarrow$ (1) Let $\mathbf{X} \simeq \mathcal{Q}(G, \alpha)$. The left action of G on G is regular. The action of $Dis(\mathbf{X})$ is given by the left action of $[G, \alpha] \leq G$, then it is semiregular. Since $\mathbf{X}$ is connected, then $Dis(\mathbf{X})$ is regular. □

Remark 4.3. *Let $\mathbf{X}$ be a connected quandle. Up to isomorphism, the only regular automorphism group is $Dis(\mathbf{X})$. Indeed, let $\mathbf{X} \simeq \mathcal{Q}(G, \alpha)$ and $Dis(\mathbf{X}) \simeq [G, \alpha] \leq G$. The left action of $[G, \alpha]$ is regular if and only if $[G, \alpha] = G$. Hence $Dis(\mathbf{X}) \simeq G$.*

Corollary 4.4. [4, Corollary 3.21] *A connected quandle $\mathbf{X}$ is affine if and only if $Dis(\mathbf{X})$ is Abelian.*

4.2. **Principal Latin quandles.** The structure of principal quandles is determined by the underlying group structure and by the properties of the automorphism α.

In this Section we investigate the interplay between the group structure and the quandle structure in the Latin case. We investigate the nature of subquandles of principal Latin quandles and the structure of the automorphism group. The results of this Section are original. The main one is Theorem 4.8, which states that the class of principal Latin quandles is a variety.

Lemma 4.5. *Let $\mathbf{X}$ be a Latin quandle. Then the following are equivalent:*

1. *$\mathbf{X}$ is principal;*

(2) *$Dis(\boldsymbol{X}) = \{L_y L_x^{-1},\ y \in X\}$ for every $x \in X$.*

Proof. (1) $\Rightarrow$ (2) Assume that $\mathbf{X}$ is principal and let $x \in X$. The assignment

$$X \longrightarrow Dis(\mathbf{X}), \quad y \longrightarrow L_{y/x} L_x^{-1}$$

is bijective. Its inverse is given by $h \mapsto h(x)$.

(2) $\Rightarrow$ (1) Assume that $Dis(\mathbf{X}) = \{L_y L_x^{-1},\ y \in X\}$, and that $L_y L_x^{-1}(x) = yx = x$ for some y. Since $\mathbf{X}$ is Latin, $y = x$, therefore $L_y L_x^{-1} = 1$. Thus, $\mathbf{X}$ is principal by Proposition 4.2. □

Corollary 4.6. *Let $\boldsymbol{X}$ be a principal Latin quandle, β be its congruence. Then $\boldsymbol{X}/\beta$ is a principal Latin quandle.*

Proof. It follows by Lemma 4.5, since $Dis(\mathbf{X}/\beta) = \{L_{[y]} L_{[x]}^{-1},\ [y] \in \mathbf{X}/\beta\}$ and since $\mathbf{X}/\beta$ is Latin. □

Lemma 4.7. *Let $\boldsymbol{X} = \mathcal{Q}(G,\alpha)$ be a principal Latin quandle. Then the following are equivalent:*

(1) *$Q \subset X$ is a subquandle;*
(2) *Q is a coset with respect a subgroup invariant under α.*

Proof. The quandles multiplication is defined by $x \cdot y = x\alpha(x^{-1}y)$. It is easy to check that

$$xy = x/1 \cdot 1\backslash y, \quad x^{-1} = 1 \cdot ((x/1)\backslash 1) \tag{8}$$

for every $x, y \in G$.

Since $\mathbf{X}$ is principal and Latin, then every subquandle is given by xQ where $x \in G$ and Q is a subquandle containing 1. Therefore it is enough to consider a subset Q containing 1.

By virtue of formulas (8) and the definition of the quandle multiplication, Q is a subquandle containing 1 if and only if it is subgroup invariant under α. □

Theorem 4.8. *The class of principal Latin quandle is a variety.*

Proof. It is easy to see that that it is closed under $\mathcal{P}$. Corollary 4.6 implies that it is is closed under $\mathcal{H}$ and Lemma 4.7 implies that it is closed under $\mathcal{S}$. □

The automorphism group of principal Latin quandles have a nice structure. The following Proposition, was already known for finite connected affine quandles (see Corollary 1.25 of [1]). It can be extended to principal Latin quandles.

Proposition 4.9. *Let $\boldsymbol{X} = \mathcal{Q}(G,\alpha)$ be a principal Latin quandle, then*

$$\begin{aligned} Aut(\boldsymbol{X}) &\simeq G \rtimes C_{Aut(G)}(\alpha) \\ LMlt(\boldsymbol{X}) &\simeq G \rtimes \langle\alpha\rangle \\ Dis(\boldsymbol{X}) &\simeq G \end{aligned}$$

Proof. Let f be an automorphism of $\mathbf{X}$, such that $f(1) = b$. In general $b \neq 1$. Define:

$$g = \lambda_{b^{-1}} f$$

where $\lambda_{b^{-1}}$ is the translation by b^{-1}. It is an automorphism of quandle and $g(1) = 1$. Therefore

$$\begin{aligned} g(xy) &= g(x/1 \cdot 1\backslash y) = g(x)/g(1) \cdot g(1)\backslash g(y) = \\ &= g(x)/1 \cdot 1\backslash g(y) = \\ &= g(x)g(y) \end{aligned}$$

and then g is a group automorphism. Moreover $g \in Aut(\mathbf{X})_1 \cap Aut(G) = C_{Aut(G)}(\alpha)$, by Remark 3.29. Moreover, $C_{Aut(G)}(\alpha) \leq Aut(\mathbf{X})$.

Let $f, g \in Aut(\mathbf{X})$, then there exists $a, b \in G$ and $f', g' \in C_{Aut(G)}(\alpha)$ such that $f = \lambda_a f'$ and $g = \lambda_b g'$, then

$$\begin{aligned} fg(x) &= \lambda_a f' \lambda_b g'(x) = \lambda_{af'(b)} f' g'(x) = \\ &= \lambda_a \left(f' \lambda_b f'^{-1} \right) f' g'(x) \end{aligned}$$

Then, the map Φ defined by setting,

$$\Phi : Aut(\mathbf{X}) \longrightarrow G \rtimes C_{Aut(G)}(\alpha), \quad f \mapsto \left(f(1), \lambda^{-1}_{f(1)} f \right)$$

is a surjective morphism of groups. Moreover $f \in ker(\Phi)$ if and only if $f(1) = 1$ and $\lambda_{f(1)^{-1}} f = 1$. So that Φ is an isomorphism.

Since $\mathbf{X}$ is principal and connected, then by Remark 4.3, $Dis(\mathbf{X}) \simeq G$. Since $\mathbf{X}$ is principal, $Dis(\mathbf{X}) \cap \langle \alpha \rangle = \{1\}$, hence $LMlt(\mathbf{X}) \simeq G \rtimes \langle \alpha \rangle$ by virtue of Proposition 3.15 (v). □

Remark 4.10. *Note that if $\boldsymbol{X}$ is principal, then $Aut(\boldsymbol{X})^{(1)} \leq Dis(\boldsymbol{X}) \simeq G$. In particular $Aut(\boldsymbol{X})$ is solvable or rank $n+1$ if and only if G is solvable of rank n. Therefore, if $\boldsymbol{X}$ is affine $Aut(\boldsymbol{X})$ is two-step solvable.*

4.3. **Some subclasses of principal quandles.** Some of the classes defined in the previous Section coincide for principal quandles. In this Section we investigate the classes defined in Section 3.5, as subclasses of the class of (finite) principal quandles or of the class of (finite) affine quandles. It turns out that under different assumptions some of these classes are actually the same.

Proposition 4.11. *Let $\boldsymbol{X} = \mathcal{Q}(G, \alpha)$ be a principal quandle. Then it is a crossed set. Moreover $\boldsymbol{X}$ is faithful if and only if it is strongly faithful.*

Proof. It is easy to see that

$$x \cdot y = t(x)\alpha(y) = y \;\Leftrightarrow\; t(x) = t(y) \;\Leftrightarrow\; L_x = L_y$$

Therefore, $\mathbf{X}$ is a crossed set and if it is faithful then it is strongly faithful. □

In the class of affine quandles the subclass of Latin quandles coincide with the class of Taylor quandles.

Lemma 4.12. *Let $\boldsymbol{X}$ an affine quandle. Then it is Latin if and only if it is faithful and connected.*

Proof. The quandle $\mathbf{X}$ is homogeneous, then it is enough to show that $R_0 = 1 - \alpha$ is bijective.

Since $\mathbf{X}$ is faithful if and only if $1 - \alpha$ is injective and it is connected if and only if it is surjective, these conditions together are equivalent to latinity. □

Proposition 4.13. *Let* $\mathbf{X}$ *be an affine quandle. Then the following are equivalent*

(1) $\mathbf{X}$ *is Taylor;*
(2) $\mathbf{X}$ *is Maltsev;*
(3) $\mathbf{X}$ *is Latin.*

Proof. If $\mathbf{X}$ is Taylor, then in particular it is connected and faithful. Therefore it is Latin. □

If we consider the class of finite principal quandles, all the classes defined in Section 3.5 are actually the same class.

Proposition 4.14. *Let* $\mathbf{X} = \mathcal{Q}(G,\alpha)$ *a principal finite quandle, then the following are equivalent:*

(1) $t = R_1$ *is a permutation;*
(2) $Fix(L_1) = Fix(\alpha) = \{1\}$*;*
(3) $\mathbf{X}$ *is faithful;*
(4) $\mathbf{X}$ *is strongly faithful;*
(5) $\mathbf{X}$ *is Taylor;*
(6) $\mathbf{X}$ *is Maltsev;*
(7) $\mathbf{X}$ *is Latin.*

Proof. The implications (7) ⇒ (6) ⇒ (5) ⇒ (4) ⇒ (3) hold in general.

(1) ⇔ (2) ⇔ (3) Since

$$\alpha(x^{-1}y) = x^{-1}y \iff t(x) = t(y) \iff L_x = L_y$$

then t is injective if and only if $Fix(L_1) = \{1\}$ if and only if $\mathbf{X}$ is faithful.

(1) ⇒ (6) Let $t = R_1$ be a permutation and λ_x denote the left action of $x \in G$ on G. Then $R_x = \lambda_x R_1 \lambda_x^{-1}$ is a permutation for every $x \in X$. □

Propositions 4.11 and 4.14 show that there exist non faithful crossed sets (any principal quandle $\mathcal{Q}(G,\alpha)$ with $Fix(\alpha) \neq \{1\}$). Moreover any of items of Proposition 4.14 implies connectedness. For affine quandles connectedness is equivalent to Latinity.

Proposition 4.15. [1, Section 1.3.8] *Let* $\mathbf{X} = \mathcal{Q}(A,\alpha)$ *be a finite affine quandle. Then the following are equivalent:*

(1) $\mathbf{X}$ *is connected;*
(2) $\mathbf{X}$ *is Latin.*

Proof. It is straightforward to see that $O_{LMlt(\mathbf{X})}(x) = x + Im(1-\alpha)$. Then $\mathbf{X}$ is connected if and only if $1-\alpha$ is surjective. Since $\mathbf{X}$ is finite, $\mathbf{X}$ is connected if and only if it is an automorphism of A. □

5. Extensions

5.1. **Extensions of LQGs.** This Section is about *extensions* of LQGs. All these results have been inspired by Section 2 of [1], where the same constructions are performed for racks and quandles.

Proposition 5.1. *Let* $\mathbf{X}$ *be a LQG and* α *be its congruence.*

(i) *The blocks of α are subalgebras if and only if $\boldsymbol{X}/\alpha$ is idempotent.*
(ii) *If $\boldsymbol{X}/\alpha$ is connected then α is uniform.*
(iii) *If $\boldsymbol{X}$ is a quandle and $\boldsymbol{X}/\alpha$ is connected, then the blocks are pairwise isomorphic subalgebras of $\boldsymbol{X}$.*

Proof. (i) Let $x, y \in [x]$, then the block $[x]$ is a subalgebra if and only if

$$[L_x^{\pm 1}(y)] = L_{[x]}^{\pm 1}([x]) = [x].$$

So it holds for every block if and only if $\mathbf{X}/\alpha$ is idempotent.

(ii) Let $[x], [y] \in \mathbf{X}/\alpha$, then there exists $h \in LMlt(\mathbf{X}/\alpha)$ such that $[y] = h([x])$. By Lemma 2.11, there exists $h' \in LMlt(\mathbf{X})$ such that $h = \pi_\alpha^*(h')$ and

$$[h'(z)] = h([z])$$

for every $z \in X$. So h' maps the $[x]$ to the block $h([(x)]) = [y]$, and its restriction to the block $[x]$ is bijective.

(iii) It follows from the previous items using the fact that left multiplications are automorphisms. □

Remark 5.2. *Item (i) of Proposition 5.1 holds for algebras of any type. Indeed, if $x_1 \ \alpha \ x_2 \ \alpha \ \ldots \ \alpha \ x_n$, then*

$$[t^{\boldsymbol{X}}(x_1, \ldots, x_n)] = t^{\boldsymbol{X}/\alpha}([x_1], \ldots, [x_1]) = [x_1]$$

for every term t if and only if $\boldsymbol{X}/\alpha$ is idempotent.

Let $\mathbf{X}$ be a LQG and let S be a non-empty set. Then the set $X \times S$ can be endowed by a LQG structure such that the canonical projection

$$\pi : X \times S \longrightarrow X, \quad (x, s) \longmapsto x$$

is an algebra morphism. Note that in such a case $ker(\pi)$ is uniform.

Proposition 5.3. *Let S be a non-empty set and $\boldsymbol{X}$, $(X \times S, \cdot)$ be LQGs. Then the projection onto $\boldsymbol{X}$ is an algebra morphism if and only if there exists*

$$\beta : X \times X \times S \longrightarrow \mathrm{Sym}(S), \quad (x, y, s) \mapsto \beta(x, y, s)$$

such that

$$(x, s) \cdot (y, t) = (xy, \beta(x, y, s)(t)) \tag{9}$$

for every $x, y \in \boldsymbol{X}$ and $s, t \in S$.

Proof. If the operation $\cdot$ is defined as in formula (9), then $(X \times S, \cdot)$ is a LQG and π is a morphism.

Let assume that

$$\pi\left((x, s) \cdot (y, t)\right) = \pi\left((x, s)\right) \pi\left((y, t)\right) = xy$$

Then $(x, s) \cdot (y, s) = (xy, u)$ for some $u \in S$, for every $x, y \in X$ and every $s, t \in S$. In order to define a bijection on $X \times S$, $L_{(x,s)}$ has to be a bijection between $\{y\} \times S$ and $\{xy\} \times S$ for every $x, y \in X$ and every $s \in S$, Then there exists $\beta(x, y, s) \in \mathrm{Sym}(S)$ such that

$$(x, s) \cdot (y, t) = (xy, \beta(x, y, s)(t)$$

for every $t \in S$. Then a map β is defined by setting

$$\beta : X \times X \times S \longrightarrow \mathrm{Sym}(S), \quad (x, y, s) \mapsto \beta(x, y, s)$$

for every $x, y \in X$ and every $s \in S$. □

The LQG structure defined in Proposition 5.3 will be denoted by $\mathbf{X} \times_\beta S$.

Definition 5.4. A LQG isomorphic to $\mathbf{X} \times_\beta S$ for some non-empty set S and some map $\beta : X \times X \times S \longrightarrow \mathrm{Sym}(S)$ is said to be an *extension of* $\boldsymbol{X}$.

Extensions correspond to uniform congruences.

Proposition 5.5. *Let* $\boldsymbol{X}$ *be a LQG and* α *be its congruence. Then* $\boldsymbol{X}$ *is an extension of* $\boldsymbol{X}/\alpha$ *if and only if* α *is a uniform congruence.*

Proof. If $\mathbf{X} \simeq \mathbf{X}/\alpha \times_\beta S$ then the blocks and S have the same cardinality.
If the blocks of α have all the same size, there exists a set S and a family of bijections $h_{[x]} : [x] \longrightarrow S$. The map β is defined by setting

$$\beta(x, y, s) = h_{[xy]} L_{h^{-1}_{[x]}(s)} h^{-1}_{[y]} \tag{10}$$

The mapping

$$\mathbf{X} \longrightarrow \mathbf{X}/\alpha \times S, \quad x \mapsto ([x], h_{[x]}(x)) \tag{11}$$

is an isomorphism. □

Remark 5.6. *Let* $\boldsymbol{X}$ *be a LQG, and* α *be its congruence such that* $\boldsymbol{X}/\alpha$ *is connected. Then* $\boldsymbol{X}$ *is an extension of* $\boldsymbol{X}/\alpha$ *since by Proposition 5.1 (ii),* α *is uniform.*
If $\boldsymbol{X}$ *is connected LQG, then any congruence* $\alpha \in Con(\boldsymbol{X})$ *is uniform and* $\boldsymbol{X}$ *is an extension of* $\boldsymbol{X}/\alpha$*.*

Connectedness of an extension $\mathbf{X} \times_\beta S$ of a connected quandle $\mathbf{X}$ depends on the properties of the preimage of the stabilizers of $\mathbf{X}$ under the map $\pi^*_{ker(\pi)}$.

Proposition 5.7. *Let* $\boldsymbol{X}$ *be a LQG and* α *be its congruence. Then* $\boldsymbol{X}$ *is connected if and only if* $\boldsymbol{X}/\alpha$ *is connected and*

$$Dis(\boldsymbol{X})_{[x]} = \{h \in Dis(\boldsymbol{X}), \text{ such that } [h(x)] = [x]\} = (\pi^*_\alpha)^{-1}(Dis(\boldsymbol{X}/\alpha)_{[x]})$$

is transitive on $[x]$ *for every* $x \in \boldsymbol{X}$*.*

Proof. Let $\mathbf{X}$ be connected, then $\mathbf{X}/\alpha$ is connected and clearly $Dis(\mathbf{X})_{[x]}$ is transitive on $[x]$ for every $x \in \mathbf{X}$.
Let $([x], s)$, $([y], t) \in \mathbf{X} \simeq \mathbf{X}/\alpha \times_\beta S$. Since $\mathbf{X}/\alpha$ is connected, then there exists $h = \prod_{i=1}^n L^{a_i}_{[x_i]}$ such that $[y] = h([x])$. Therefore,

$$\prod_{i=1}^n L^{a_i}_{([x_i],s)}([x], s) = ([y], t')$$

for some $t' \in S$. By transitivity of $Dis(\mathbf{X})_{[x]}$ on $[x]$, there exists $g \in Dis(\mathbf{X})_{[x]}$ such that $gh([x], s) = g([y], t') = ([y], t)$. Therefore, $\mathbf{X}$ is connected. □

Remark 5.8. *Note that* $Dis(\boldsymbol{X})_{[x]}$ *and* $Dis(\boldsymbol{X})_{[y]}$ *are conjugate whenever* $\boldsymbol{X}/\alpha$ *is connected. Then it is enough to have that one of them is transitive.*

5.2. **Extensions for Racks and Quandles.** In this Section we just restate some of the results given in Section 2 of [1].

Let $\mathbf{X}$ be a rack and $\mathbf{X}\times_\beta S$ an extension of $\mathbf{X}$ as LQG. In order to define a rack structure on $\mathbf{X}\times S$, the map β has to satisfy one more condition, which corresponds to left-distributivity. This condition is given in the following definition.

Definition 5.9. [1, Definition 2.2] Let β be a map:

$$\beta : X \times X \times S \to \mathrm{Sym}(S)$$

The map β is called a *(dynamical) cocycle* if it satisfies the following condition

$$\text{(C)} \qquad \beta(xy, xz, \beta(y,z,s)(t))\beta(x,z,s) = \beta(x,yz,s)\beta(y,z,t)$$

for every $x,y,z \in X$, $s,t \in S$. This condition is called *cocycle condition.*

In addition, if $\mathbf{X}$ is a quandle, β is a *quandle cocycle* if it satysfies following condition

$$\text{(Q)} \qquad \beta(x,x,s)(s) = s$$

for every $x \in X$ and every $s \in S$. This condition is called *quandle* condition.
Then

$$Z^2(\mathbf{X}, \mathrm{Sym}(S)) = \{\beta : X \times X \times S \to \mathrm{Sym}(S), \text{ such that } (C) \text{ and } (Q) \text{ hold}\}$$

is the *set of the non-Abelian dynamical 2-cocycles.*

A result analogous to Proposition 5.3 holds for racks and quandles.

Proposition 5.10. [1, Lemma 2.1] *Let S be a non-empty set and $\boldsymbol{X}$, $(X\times S,\cdot)$ be quandles. Then the canonical projection onto $\boldsymbol{X}$ is a quandle morphism if and only if $(X\times S,\cdot)\simeq \boldsymbol{X}\times_\beta S$ for some $\beta\in Z^2(\boldsymbol{X},\mathrm{Sym}(S))$.*

Proof. The map β is defined as in formula 10. It has to be necessarily a dynamical cocycles in order to satisfy left-distributivity. □

Remark 5.11. *Proposition 5.10 can be stated for racks, and in this case β need to satisfy just condition (C).*

Proposition 5.5 and Remark 5.6 hold for racks and quandles, too.

Example 5.12. The map defined by setting

$$\mathbf{1} : X \times X \longrightarrow \mathrm{Sym}\,(S)\,, \quad (x,y) \mapsto 1$$

is a cocycle. It is called the *trivial cocycle.* It is easy to see that $\mathbf{X}\times_{\mathbf{1}} S = X\times\mathbf{P\text{-}LQ}_{|S|}$. The extension $\mathbf{Y} = \mathbf{X}\times_{\mathbf{1}} S$ is called *trivial extension* of $\mathbf{X}$ and $O_{LMlt(\mathbf{Y})}(x,s) = \mathbf{X}\times\{s\}$. Therefore $\mathbf{Y}$ is connected if and only if $|S| = 1$.

5.3. **Non Abelian Cohomology.** The contents of this Section are again taken from Section 2 of [1]. The same construction can be develop in a more general setting but we focus on quandles.

Let $\mathbf{X}$ be an extension of $\mathbf{X}/\alpha$. The isomorphism defined in formula (11) is defined up to the choice of a family of bijections between S and the blocks of α. Cohomologous cocycles, defined as follows, correspond to different choices of family of bijections in (11).

Definition 5.13. [1, Definition 2.6] Let $\mathbf{X}$ be a rack, β, β' be dynamical cocycles. They are said to be *cohomologous* if there exists

$$\gamma : X \to \mathrm{Sym}(S), \quad x \mapsto \gamma(x)$$

such that

$$\beta'(x,y,s) = \gamma(xy)\beta(x,y,\gamma(x)^{-1}(s))\gamma(y)^{-1} \tag{12}$$

for every $x, y \in X$ and every $s \in S$.

Remark 5.14. *The map defined in formula (12) is a quandle cocycle whenever β is a quandle cocycle. So the relation defined in 5.13 is an equivalence relation on $Z^2(\boldsymbol{X}, \mathrm{Sym}(S))$.*

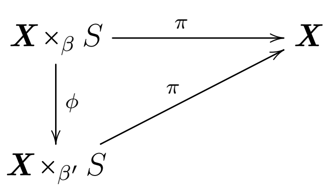
Definition 5.15. Let $\mathbf{X}$ be a rack, S be a non empty set, then

$$H^2(\mathbf{X}, \mathrm{Sym}(S)) = Z^2(\mathbf{X}, \mathrm{Sym}(S))/\sim$$

is called *second cohomology set* of $\mathbf{X}$.

Proposition 5.16. [1, Section 2] *Let $\beta, \beta' \in Z^2(\boldsymbol{X}, \mathrm{Sym}(S))$ be dynamical cocycles. Then the following are equivalent:*

(1) *there exists an isomorphism $\phi : X \times_\beta S \longrightarrow \boldsymbol{X} \times_{\beta'} S$ such that*



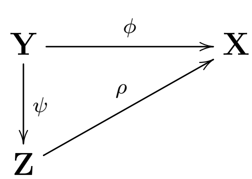
is commutative;

(2) *β and β' are cohomologous.*

5.4. **Quandle Coverings.** The goal of this Section is to show that the categorical approach to coverings given in [13] and the construction of extensions by constant cocycles given in Section 2.2 of [1] are equivalent.

Definition 5.17. [13, Definition 1.4], [13, Definition 4.1] Let $\mathbf{X}, \mathbf{Y}$ be racks and $\phi : \mathbf{Y} \longrightarrow \mathbf{X}$ be a surjective morphism such that $ker(\phi) \leq ker(L_{\mathbf{Y}})$. Then the pair $(\mathbf{Y}, \phi)$ is said to be a *covering of $\boldsymbol{X}$*.

Let $\mathbf{X}$ be a quandle and $(\mathbf{Y}, \phi)$, $(\mathbf{Z}, \rho)$ be coverings of $\mathbf{X}$. They are said to be *isomorphic* if there exists an isomorphism ψ such that the following diagram is commutative



Remark 5.18. *The property $ker(\phi) \leq ker(L_{\boldsymbol{Y}})$ can be written as*

$$\phi(x) = \phi(y) \;\Rightarrow\; L_x = L_y \tag{13}$$

Note that if $(\boldsymbol{X},\phi)$ is a covering then the blocks of $ker(\phi)$ are projection subquandles, since the blocks of $ker(L_{\boldsymbol{X}})$ are projection subquandles. Moreover $\boldsymbol{X}$ is not faithful, unless ϕ is an isomorphism.

Extensions satisfying the property (13) correspond to cocycles such that $\beta(x,y,s) = \beta(x,y,t)$ for every $x,y \in X$ and every $s,t \in S$. Cocycles satisfying this property are called constant cocycle.

Definition 5.19. [1, Definition 2.2] Let $\mathbf{X}$ be a quandle and S be a non-empty set. A map $\beta : X \times X \to \mathrm{Sym}(S)$, is called a *constant quandle cocycle* if it satisfies the following conditions

$$\beta(xy,xz)\beta(x,z) = \beta(x,yz)\beta(y,z) \tag{CC}$$

$$\beta(x,x) = 1 \tag{CQ}$$

for every $x,y,z \in X$, $s,t \in S$. The set

$$Z^2_c(\mathbf{X},\mathrm{Sym}(S)) = \{\beta : X \times X \to \mathrm{Sym}(S), \text{ such that } (CC) \text{ and } (CQ) \text{ hold}\}$$

is the set of the *constant non-Abelian 2-cocycles with coefficients in* $\mathrm{Sym}(S)$. Two constant cocycles β and β' are *cohomologous* if

$$\beta'(x,y) = \gamma(xy)\,\beta(x,y)\,\gamma(y)^{-1}$$

for every $x,y \in X$, for some $\gamma : X \longrightarrow \mathrm{Sym}(S)$. The set

$$H^2_c(\mathbf{X},\mathrm{Sym}(S)) = Z^2_c(\mathbf{X},\mathrm{Sym}(S))/\sim$$

is *the second constant cohomology set of $\boldsymbol{X}$ with coefficient in* $\mathrm{Sym}(S)$.

Remark 5.20. *The constant cocycle condition implies that*

$$\beta(xy,xz) = \beta(x,yz) \Longleftrightarrow \beta(x,z) = \beta(y,z) \tag{WCC}$$

for every $x,y,z \in X$. This condition will be called weaker cocycle condition.

Remark 5.21. *Constant cocycles with coefficients in groups different from permutation groups still make sense and they have applications to other problems (see* [1] *Section 5). So the sets $Z^2_c(\boldsymbol{X},\Gamma)$ and $H^2_c(\boldsymbol{X},\Gamma)$ can be defined for any group Γ in the very same way.*

We say that $\boldsymbol{X}$ has trivial cohomology if $H^2_c(\boldsymbol{X},\Gamma)$ for every group Γ.

Remark 5.22. *A quandle $\boldsymbol{X}$ has trivial cohomology if and only if*

$$\beta(yx,y) = \beta(y,xy)$$

for every $x,y \in X$, since from (CC) you can obtain that

$$\beta(x,y) = 1_\Gamma \Longleftrightarrow \beta(yx,y) = \beta(y,xy)$$

The correspondence between coverings and constant cocycles is given by the following Proposition.

Proposition 5.23. *Let $\boldsymbol{X}$ be a quandle, S be a non-empty set. Then $(\boldsymbol{X} \times_\beta S, \pi)$ is a covering of $\boldsymbol{X}$ if and only if $\beta \in Z^2_c(\boldsymbol{X},\mathrm{Sym}(S))$.*

Proof. The pair $((\mathbf{X} \times_\beta S, \cdot), \pi)$ a covering if and only if

$$(x,s)\cdot(y,t) = (xy, \beta(x,y,s)(t)) = (xy, \beta(x,y,r)(t)) = (x,r)\cdot(y,t)$$

for every $x, y \in X$ and $r, s, t \in S$. This condition holds if and only if

$$\beta(x,y,s) = \beta(x,y,r)$$

for every $x, y \in X$ and every $s, r \in S$, i.e. if and only if $\beta \in Z^2_c(\mathbf{X}, \mathrm{Sym}(S))$. □

Remark 5.24. *Proposition 5.23 shows that the notion of covering and the notion of constant cocycles are basically the same. The only difference is that in the definition of a covering is not claimed that the correspondent congruence to be uniform. In the class of connected quandles, they are actually the very same thing.*

Some examples of coverings can be found in the class of homogeneous quandles.

Proposition 5.25. *Let G be a group, $H_1 \leq H_2 \leq G$ and $\boldsymbol{X}_1 = \mathcal{Q}(G, H_1, \alpha)$, $\boldsymbol{X}_2 = \mathcal{Q}(G, H_2, \alpha)$. Then $(\boldsymbol{X}_1, \pi)$ is a covering of $\boldsymbol{X}_2$, where*

$$\pi : \boldsymbol{X}_1 \longrightarrow \boldsymbol{X}_2, \quad xH_1 \mapsto xH_2$$

Proof. The map π is a morphism, since

$$\begin{aligned} \pi(xH_1 \cdot yH_1) &= \pi(x\alpha(x^{-1}y)H_1) = x\alpha(x^{-1}y)H_2 = \\ &= xH_2 \cdot yH_2 = \pi(xH_1)\cdot\pi(yH_1) \end{aligned}$$

for every $x, y \in G$. Let xH_1 and yH_1 be such that $xH_2 = yH_2$. Therefore $x = yh$ for some $h \in H_2$. Then

$$\begin{aligned} xH_1 \cdot zH_1 &= yhH_1 \cdot zH_1 = yh\alpha\left(h^{-1}y^{-1}z\right)H_1 = \\ &= yhh^{-1}\alpha\left(y^{-1}z\right)H_1 = y\alpha\left(y^{-1}z\right)H_1 = \\ &= yH_1 \cdot zH_1 \end{aligned}$$

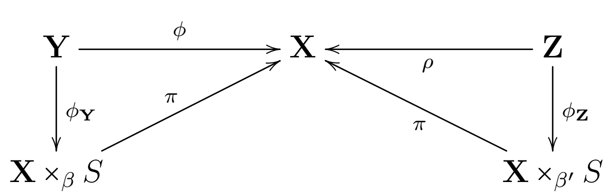
for every $z \in G$. Hence $ker(\pi) \leq ker(L_{\mathbf{X}_1})$, so $(\mathbf{X}_1, \pi)$ is a covering. □

Moreover isomorphic coverings correspond to cohomologous constant cocycles.

Proposition 5.26. *Let $\boldsymbol{X}$ be a connected quandle, $(\boldsymbol{Y}, \phi) \simeq \boldsymbol{X} \times_\beta S$ and $(\boldsymbol{Z}, \rho) \simeq \boldsymbol{X} \times_{\beta'} S$ be coverings of $\boldsymbol{X}$. Then the following are equivalent:*

(1) *$(\boldsymbol{Y}, \phi) \simeq (\boldsymbol{Z}, \rho)$;*
(2) *$\beta \sim \beta'$.*

Proof. Let $\phi_{\mathbf{Y}}$ be the isomorphism defined by setting $\phi_{\mathbf{Y}}(y) = (\phi(y), f_y(y))$ where f_y is a bijection between $[y]_{ker(\phi)}$ and S and let $\phi_{\mathbf{Z}}$ be defined in analogously (as in Proposition 5.5). Since the following diagram is commutative,



then (1) and (2) are equivalent. □

6. Congruences and transvection group

6.1. **Galois Connection.** In the variety of quandles there is a strong interplay between normal subgroups of the transvection group which are normal in the left multiplications group and congruences (see Lemma 4.2 of [4]). This Section is a further development of the subject of Section 4 of [4]. As a new contribution we show that there is a *Galois connection* between the congruence lattice of a quandle and the congruence lattice of subgroup of its transvection group which are normal in the left multiplication group.

In the sequel the kernel of $\pi_\alpha^*|_{Dis(\mathbf{X})}$ will be denote by $Dis^\alpha(\mathbf{X})$. It has the following characterization.

Lemma 6.1. *Let $\boldsymbol{X}$ be a quandle and α be its congruence. Then*

$$Dis^\alpha(\boldsymbol{X}) = \{h \in Dis(\boldsymbol{X}),\ [h(x)]_\alpha = [x]_\alpha,\ \text{for every } x \in \boldsymbol{X}\} = \bigcap_{x\in X} Dis(\boldsymbol{X})_{[x]}$$

If $\boldsymbol{X}/\alpha$ is connected, then

$$Dis^\alpha(\boldsymbol{X}) = Core_{LMlt(\boldsymbol{X})}(Dis(\boldsymbol{X})_{[x]})$$

Proof. Since

$$[h(x)]_\alpha = \pi_\alpha^*(h)[x]_\alpha = [x]_\alpha$$

holds for every $x \in \mathbf{X}$ if and only $\pi_\alpha^*(h) = 1$, then

$$Dis^\alpha(\mathbf{X}) = \{h \in Dis(\mathbf{X}),\ [h(x)]_\alpha = [x]_\alpha,\ \text{for every } x \in \mathbf{X}\} = \bigcap_{x\in X} Dis(\mathbf{X})_{[x]}$$

Assume that $\mathbf{X}/\alpha$ is connected. Then for every $[x],[y]$ there exists $\pi_\alpha^*(h)$ such that $[y] = \pi_\alpha^*(h)([x])$ and $Dis(\mathbf{X})_{[y]} = hDis(\mathbf{X})_{[x]}h^{-1}$. Therefore

$$Dis^\alpha(\mathbf{X}) = \bigcap_{h\in LMlt(\mathbf{X})} hDis(\mathbf{X})_{[x]}h^{-1} = Core_{LMlt(\mathbf{X})}(Dis(\mathbf{X})_{[x]})$$

□

Remark 6.2. *Note that if $\boldsymbol{X}/\alpha$ is a principal quandle then $Dis(\boldsymbol{X}/\alpha)_{[x]} = \{1\}$. Therefore*

$$Dis^\alpha(\boldsymbol{X}) = (\pi_\alpha^*)^{-1}(\{1\}) = Dis(\boldsymbol{X})_{[x]}$$

The group $Dis^\alpha(\mathbf{X})$ embeds in the product of the automorphism groups of the blocks with respect to α, as a Corollary of this general result.

Lemma 6.3. *Let G be a group of permutations acting on a set X. Let $X = \bigcup_{i\in I} X_i$ where $\{X_i,\ i \in I\}$ is a family of invariant subsets with respect to the action of G. Then G embeds in $\prod_{i\in I} G|_{X_i}$.*

Proof. The map

$$G \longrightarrow \prod_{i\in I} G|_{X_i}, \quad h \mapsto \{h|_{X_i},\ i \in I\}$$

is a injective group morphism. □

Corollary 6.4. *Let $\boldsymbol{X}$ be a quandle and α be its congruence. Then $Dis^\alpha(\boldsymbol{X})$ embeds in $\prod_{[x]\in \boldsymbol{X}/\alpha} Aut([x])$.*

Proof. It follows by Lemma 6.3, since every block is invariant under the action of $Dis^\alpha(\mathbf{X})$ and it acts by automorphism. □

Every subgroup of $Dis(\mathbf{X})$ normal in $LMlt(\mathbf{X})$ defines a congruence. The following result was already known (see Proposition 4.6 of [4]).

Lemma 6.5. *Let $\boldsymbol{X}$ be a quandle and $Dis(\boldsymbol{X}) \geq N \trianglelefteq LMlt(\boldsymbol{X})$. The relation*

$$x \ \alpha_N \ y \iff L_x L_y^{-1} \in N$$

is a congruence.

Proof. Let $x \ \alpha_N \ y$ and $z \in X$. Then

$$L_{L_z^{\pm 1}(x)} L_{L_z^{\pm 1}(y)}^{-1} = L_z^{\pm 1} L_x L_y^{-1} L_z^{\mp 1} \in N$$

since it is normal. Therefore $L_z^{\pm 1}(x) \ \alpha_N \ L_z^{\pm 1}(y)$. Since $L_y L_x^{-1} = (L_x L_y^{-1})^{-1} \in N$ and $L_x^{-1} L_y = L_x^{-1} L_y L_x^{-1} L_x \in N$, then

$$L_{xz} L_{yz}^{-1} = L_x L_z L_x^{-1} L_y L_z^{-1} L_y^{-1} = L_x L_y^{-1} L_y L_z L_x^{-1} L_y L_z^{-1} L_y^{-1} \in N$$

Therefore, $xz \ \alpha_N \ yz$ and then α_N is a congruence. □

On the other hand, to any congruence α corresponds a subgroup of $Dis(\mathbf{X})$ which is normal in $LMlt(\mathbf{X})$.

Definition 6.6. Let $\mathbf{X}$ be a quandle and α be its congruence. Then

$$Dis_\alpha(\mathbf{X}) = \langle L_x L_y^{-1}, \ x \ \alpha \ y \rangle$$

Proposition 6.7. *Let $\boldsymbol{X}$ be a quandle and α be its congruence. Then $Dis_\alpha(\boldsymbol{X})$ is a normal subgroup of $LMlt(\boldsymbol{X})$ and*

$$Dis_\alpha(\boldsymbol{X}) = \{ L_{x_m}^{-a_m} \dots L_{x_1}^{-a_1} L_{y_1}^{a_1} \dots L_{y_m}^{a_m}, \ \bar{x}, \bar{y} \in X^m, \bar{x} \ \alpha \ \bar{y}, \ a_i = \pm 1, \ m \in \mathbb{N} \}$$

Proof. Since α is a congruence, then $xy \ \alpha \ xz$ whenever $y \ \alpha \ z$. Then

$$L_x L_y L_z^{-1} L_x^{-1} = L_{xy} L_{xz}^{-1} \in Dis_\alpha(\mathbf{X})$$

for every $x \in X$. Therefore $Dis_\alpha(\mathbf{X})$ is normal in $LMlt(\mathbf{X})$.

Let $h = L_{x_n}^{-a_n} \dots L_{x_1}^{-a_1} L_{y_1}^{a_1} \dots L_{y_n}^{a_n}$ and $g = L_{z_m}^{-b_m} \dots L_{z_1}^{-b_1} L_{u_1}^{b_1} \dots L_{u_m}^{b_m}$ such that, $\bar{x} \ \alpha \ \bar{y}$ and $\bar{z} \ \alpha \ \bar{u}$. Let $f = L_{z_m}^{-b_m} \dots L_{z_1}^{-b_1}$, then

$$\begin{aligned} hg &= L_{x_n}^{-a_n} \dots L_{x_1}^{-a_1} L_{y_1}^{a_1} \dots L_{y_n}^{a_n} L_{z_m}^{-b_m} \dots L_{z_1}^{-b_1} L_{u_1}^{b_1} \dots L_{u_m}^{b_m} \\ &= L_{z_m}^{-b_m} \dots L_{z_1}^{-b_1} L_{f^{-1}(x_n)}^{-a_n} \dots L_{f^{-1}(x_1)}^{-a_1} L_{f^{-1}(y_1)}^{a_1} \dots L_{f^{-1}(y_n)}^{a_n} L_{u_1}^{b_1} \dots L_{u_m}^{b_m} \\ h^{-1} &= L_{y_n}^{-a_n} \dots L_{y_1}^{-a_1} L_{x_1}^{a_1} \dots L_{x_n}^{a_n} \end{aligned}$$

Since α is a congruence then $f^{-1}(x_i) \ \alpha \ f^{-1}(y_i)$ for every $1 \leq i \leq n$, so the right handside is a subgroup. Clearly it contains $Dis_\alpha(\mathbf{X})$ since it contains its generators.

For the other inclusion, let proceed by induction on $k = \sum_{i=1}^m |a_i|$. If $k = 1$ then it holds, since $L_x^{-1} L_y = L_{x \backslash y} L_x^{-1} \in Dis_\alpha(X)$ and $x \backslash y \ \alpha \ x$. Let

$$\begin{aligned} h &= L_{x_{n+1}}^{\pm 1} \dots L_{x_1}^{-a_1} L_{y_1}^{a_1} \dots L_{y_{n+1}}^{\mp 1} = \\ &= L_{L_{x_{n+1}}^{\pm 1}(x_n)}^{-a_n} \dots L_{L_{x_{n+1}}^{\pm 1}(x_1)}^{-a_1} L_{L_{x_{n+1}}^{\pm 1}(y_1)}^{a_1} \dots L_{L_{x_{n+1}}^{\pm 1}(y_n)}^{a_n} L_{x_{n+1}}^{\pm 1} L_{y_{n+1}}^{\mp 1} = \\ &= g L_{x_{n+1}}^{\pm 1} L_{y_{n+1}}^{\mp 1} \end{aligned}$$

By induction, g and $L_{x_{n+1}}^{\pm 1} L_{y_{n+1}}^{\mp 1}$ belong to $\in Dis_\alpha(\mathbf{X})$, since $L_{x_{n+1}}^{\pm 1}(x_i) \ \alpha \ L_{x_{n+1}}^{\pm 1}(y_i)$ for every $1 \leq i \leq n$. Therefore, $h \in Dis_\alpha(\mathbf{X})$. □

Remark 6.8. *Note that $ker(L_{\boldsymbol{X}}) \leq \alpha_N$ for every N, since $1 \in N$. And moreover*

$$\alpha \leq \alpha \vee ker(L_{\boldsymbol{X}}) \leq \alpha_{Dis_\alpha(\boldsymbol{X})}$$

since both α and $ker(L_{\boldsymbol{X}})$ are contained in $\alpha_{Dis_\alpha(\boldsymbol{X})}$.

The correspondence between congruences and subgroups is monotone, since

$$\begin{aligned} N \leq H &\implies \alpha_N \leq \alpha_H \\ \alpha \leq \beta &\implies Dis_\alpha(\boldsymbol{X}) \leq Dis_\beta(\boldsymbol{X}) \end{aligned}$$

The previous remark suggests that there exists a Galois connection between congruences and normal subgroups of the left multiplication group contained in the transvection group.

Theorem 6.9. *Let $\boldsymbol{X}$ be a quandle and $[\{1\}, Dis(\boldsymbol{X})]$ be the interval between $\{1\}$ and $Dis(\boldsymbol{X})$ in the lattice of the normal subgroups of $LMlt(\boldsymbol{X})$. The assignment*

$$\begin{aligned} Con(\boldsymbol{X}) &\longrightarrow [\{1\}, Dis(\boldsymbol{X})] \\ \alpha &\mapsto Dis_\alpha(\boldsymbol{X}) \\ \alpha_N &\leftarrow N \end{aligned}$$

is a Galois connection.

Proof. Let $Dis_\alpha(\mathbf{X}) \leq N$. Then $\alpha \leq \alpha_{Dis_\alpha(\mathbf{X})} \leq \alpha_N$, since the assignment $N \mapsto \alpha_N$ is monotone.

If $\alpha \leq \alpha_N$, then $L_x L_y^{-1} \in N$ whenever $x\ \alpha\ y$. Thus $Dis_\alpha(\mathbf{X}) \leq N$. □

Remark 6.10. *Note that these mapping are neither injective nor surjective in general. For instance no congruence $\alpha \leq ker(L_{\boldsymbol{X}})$ is given by a normal subgroup.*

Any normal subgroup inducing a congruence α sits in between the group $Dis_\alpha(\mathbf{X})$ and $Dis^\alpha(\mathbf{X})$. This is a powerful result in order to understand the structure of $Con(\mathbf{X})$ given the structure of $Dis(\mathbf{X})$ and vice versa.

Proposition 6.11. *Let $\boldsymbol{X}$ be a quandle, $Dis(\boldsymbol{X}) \geq N \trianglelefteq LMlt(\boldsymbol{X})$. Then*

$$Dis_{\alpha_N}(\boldsymbol{X}) \leq N \leq Dis^{\alpha_N}(\boldsymbol{X}).$$

Proof. Clearly since $x\ \alpha_N\ y$ if and only if $L_x L_y^{-1} \in N$, then $Dis_{\alpha_N}(\mathbf{X}) \leq N$.
Let $x \in \mathbf{X}$ and $h \in N$. Since N is normal, then

$$L_{h(z)} L_z^{-1} = h L_z h^{-1} L_z^{-1} \in N$$

therefore $[h(x)]_{\alpha_N} = [x]_{\alpha_N}$. By Proposition 6.1, $N \leq Dis^{\alpha_N}(\mathbf{X})$. □

Lemma 6.12. *Let $\boldsymbol{X}$ be a quandle. Then $Dis^{\alpha_N}(\boldsymbol{X})$ is a normal subgroup of $LMlt(\boldsymbol{X})$, and $\boldsymbol{X}/\alpha_{Dis^\alpha(\boldsymbol{X})} = L(\boldsymbol{X}/\alpha)$.*

Proof. The subgroup $Dis^\alpha(\mathbf{X})$ is normal since it is the intersection of $Dis(\mathbf{X})$ and $ker(\pi_\alpha^*)$ which are normal subgroups. Moreover

$$x\ \alpha_{Dis^\alpha(X)}\ y \iff L_x L_y^{-1} \in Dis^\alpha(X) \iff L_{[x]} = L_{[y]}$$

And then $\mathbf{X}/\alpha_{Dis^\alpha(\mathbf{X})} = L(\mathbf{X}/\alpha)$. □

Remark 6.13. *Let $\boldsymbol{X}$ be a quandle and α be its congruence Then $\boldsymbol{X}/\alpha$ is faithful if and only if $\alpha = \alpha_{Dis_\alpha(\boldsymbol{X})} = \alpha_{Dis^\alpha(\boldsymbol{X})}$. Indeed, by Lemma 6.12, $\boldsymbol{X}/\alpha$ is faithful if and only if*

$$x \ \alpha_{Dis^\alpha(\boldsymbol{X})} \ y \iff L_{[x]} = L_{[y]} \iff [x] = [y] \iff x \ \alpha \ y$$

This is equivalent to $\alpha = \alpha_{Dis_\alpha(\boldsymbol{X})} = \alpha_{Dis^\alpha(\boldsymbol{X})}$. Therefore we have that

$$L_x L_y^{-1} \in Dis_\alpha(\boldsymbol{X}) \iff L_x L_y^{-1} \in Dis^\alpha(\boldsymbol{X}).$$

If $\boldsymbol{X}$ is a Taylor quandle, then $\alpha = \alpha_{Dis^\alpha(\boldsymbol{X})}$ since all its homomorphic images are Taylor and therefore faithful.

If $\boldsymbol{X}$ is a principal Latin quandle then $Dis_\alpha(\boldsymbol{X}) = Dis^\alpha(\boldsymbol{X})$ for every $\alpha \in Con(\boldsymbol{X})$ by virtue of Lemma 4.5.

The following Lemma restates Lemma 4.10 of [4] by using the subgroup $Dis_\alpha(\mathbf{X})$.

Lemma 6.14. *Let $\boldsymbol{X}$ be a quandle and α be its congruence. Then $LMlt(\boldsymbol{X}), Dis^\alpha(\boldsymbol{X})] \leq Dis_\alpha(\boldsymbol{X})$. In particular $Dis^\alpha(\boldsymbol{X})/Dis_\alpha(\boldsymbol{X})$ is Abelian.*

Proof. Let $h = L_{x_1}^{a_1} \dots L_{x_n}^{a_n} \in LMlt(\mathbf{X})$, $g \in Dis^\alpha(\mathbf{X})$. Then

$$[h, g] = hgh^{-1}g^{-1} = L_{x_1}^{a_1} \dots L_{x_n}^{a_n} L_{g(x_n)}^{-a_n} \dots L_{g(x_1)}^{-a_1}$$

Since $g \in Dis^\alpha(\mathbf{X})$ then $g(x_i) \ \alpha \ x_i$ for every $1 \leq i \leq n$, hence $[h, g] \in Dis_\alpha(\mathbf{X})$. In particular $[Dis^\alpha(\mathbf{X}), Dis^\alpha(\mathbf{X})] \leq Dis_\alpha(\mathbf{X})$. □

Problem 3. The groups $Dis_\alpha(\mathbf{X})$ and $Dis^\alpha(\mathbf{X})$ in general induce different congruences, but even when the respective congruences are the same (as for Taylor quandles), they can be different.

Under which assumptions on $\mathbf{X}$ and α the equality holds?

A partial answer is given in Lemma 4.10 of [4], since it concernes just congruences corresponding to normal subgroups.

6.2. **Abelian, central and strongly Abelian congruences.** The properties of the group $Dis_\alpha(\mathbf{X})$ determines the nature of the congruence α. In this Section we show an original characterization of *Abelian*, *central* and *strongly Abelian* congruences through the properties of the correspondent subgroups (see Propositions 6.16, 6.19 and 6.20). In particular it turns out that coverings correspond to strongly Abelian congruences, and then they have a natural universal algebraic characterization.

Definition 6.15. Let $\mathbf{X}$ be a quandle and α be its congruence. A group G is called *α-semiregular* if it acts semiregularly on each of the blocks of α, i.e. for every $h \in G$ and every $x \ \alpha \ y$, then

$$h(x) = y \iff h(y) = y.$$

Proposition 6.16. *Let $\boldsymbol{X}$ be a quandle and α be its congruence. The following are equivalent:*

(1) *α is Abelian;*
(2) *$Dis_\alpha(\boldsymbol{X})$ is Abelian and α-semiregular.*

Proof. Let t be a term operation given by $t(\bar{x}) = L_{x_1}^{k_1} \dots L_{x_{i_m}}^{k_m}(x_{m+1})$ and let $\bar{x}\ \alpha\ \bar{y}$. According to Lemma 6.7, $\omega = L_{x_{i_m}}^{-k_m} \dots L_{x_{i_1}}^{-k_1} L_{y_{i_1}}^{k_1} \dots L_{y_{i_m}}^{k_m} \in Dis_\alpha(\mathbf{X})$. Note that the following equations are equivalent

$$t(x_0, \bar{x}) = t(x_0, \bar{y}) \tag{14}$$
$$\omega(x_{m+1}) = y_{m+1} \tag{15}$$

By Remark 1.22, it is enough to consider just slim terms with respect to the first variable to check Abelianness of α, hence without loss of generality $x_0 \in \{x_m, x_{m+1}\}$.

Case $x_0 = x_{m+1}$: by the equivalence between (14) and (15), we have

$$\omega(x_0) = x_0 \iff t(x_0, \bar{x}) = t(x_0, \bar{y}).$$

Then $Dis_\alpha(\mathbf{X})$ is semiregular if and only if t satisfies formula (2) of definition 1.21.

Case $x_0 = x_m$: note that $L_{x_0}^{-1}\omega L_{x_0} \in Dis_\alpha(\mathbf{X})$, then $L_{x_0}^{-1}\omega L_{x_0}(x) = y\ \alpha\ x$ for every $x \in X$.

Hence, let $s(x_0, \bar{x}) = L_{x_1}^{k_1} \dots L_{x_{i_m}}^{k_m} L_{x_0}(x) = L_{x_1}^{k_1} \dots L_{x_{i_m}}^{k_m} L_{x_0}(y) = s(x_0, \bar{y})$. Thereafore s satysfies formula (2) of definition 1.21 if and only if $L_{x_0}^{-1}\omega L_{x_0}(x) = y = L_{y_0}^{-1}\omega L_{y_0}(x)$ for every $x \in X$. Thus, $L_{y_0} L_{x_0}^{-1} \omega (L_{y_0} L_{x_0}^{-1})^{-1} = \omega$, for every $x_0\ \alpha\ y_0$ and $\omega \in Dis_\alpha(\mathbf{X})$, i.e. $Dis_\alpha(\mathbf{X})$ is Abelian.

Therefore, α is Abelian if and only if $Dis_\alpha(\mathbf{X})$ is Abelian and α-semiregular. □

Corollary 6.17. *Let $\boldsymbol{X}$ be a quandle. Then $\boldsymbol{X}$ is Abelian if and only if it $Dis(\boldsymbol{X})$ is Abelian and semiregular. If $\boldsymbol{X}$ is connected, then it is affine.*

Corollary 6.18. *Let $\boldsymbol{X}$ be a connected quandle and α be its congruence. Then the following are equivalent:*

(1) *$\boldsymbol{X}/\alpha$ is Abelian;*
(2) *$\alpha_{Dis(\boldsymbol{X})^{(1)}} \leq \alpha$.*

Proposition 6.19. *Let $\boldsymbol{X}$ be a quandle and α be its congruence. Then the following are equivalent:*

(1) *α is central;*
(2) *$Dis_\alpha(\boldsymbol{X})$ is central in $Dis(\boldsymbol{X})$ and $Dis(\boldsymbol{X})$ is α-semiregular.*

Proof. The proof is the same of Proposition 6.16. Let $\bar{x}$ and $\bar{y}$ be any n-tuples and $x_0\ \alpha\ y_0$. The same argument shows that formula (3) of definition 1.21 for slim terms is now equivalent to centrality of $Dis_\alpha(\mathbf{X})$ and α-semiregularity of $Dis(\mathbf{X})$. □

The following Proposition shows that coverings correspond to strongly Abelian congruences. As a Corollary, the only strongly Abelian quandles are the projection quandle.

Proposition 6.20. *Let $\boldsymbol{X}$ be a quandle and α be its congruence. The following are equivalent:*

(1) *α is strongly Abelian;*
(2) *$Dis_\alpha(\boldsymbol{X}) = 1$;*
(3) *$(\boldsymbol{X}, \pi_\alpha)$ is a covering of $\boldsymbol{X}/\alpha$.*

Proof. (1) ⇒ (3) Let $x\ \alpha\ y$ and $z \in X$. Then $u = L_x^{-1}L_y(z)\ \alpha\ z$. This is equivalent to

$$t(x,z) = xz = yu = t(y,u)$$

Then, by strongly Abelianness

$$t(x,z) = t(y,u) \implies t(x,z) = xz = xu = t(x,u)$$

i.e. $u = z$. Therefore $L_x = L_y$, whenever $x\ \alpha\ y$.

(2) ⇔ (3) The group $Dis_\alpha(\mathbf{X})$ is trivial if and only if $L_x L_y^{-1} = 1$ whenever $x\ \alpha\ y$. This is equivalent to have $\alpha \leq ker(L_{\mathbf{X}})$ and therefore $(\mathbf{X}, \pi_\alpha)$ is a covering of $\mathbf{X}/\alpha$.

(3) ⇒ (1) Let $t(x_0, \bar{x}) = L_{x_1}^{k_1} \dots L_{x_{i_m}}^{k_m}(x_{m+1})$ and let $\bar{x}\ \alpha\ \bar{y}$. Since

$$t(x_0,\bar{x}) = t(y_0,\bar{y}) \iff x_{m+1} = y_{m+1}$$

formula (4) of definition 1.21 holds for every $\bar{z}\ \alpha\ \bar{x}$. □

Corollary 6.21. *Let $\boldsymbol{X}$ be a quandle. Then $\boldsymbol{X}$ is strongly Abelian if and only if it is projection. If $\boldsymbol{X}$ is connected, then it is trivial.*

Proof. By definition 5.17, $\mathbf{X}$ is strongly Abelian if and only if $1_{\mathbf{X}} \leq ker(L_{\mathbf{X}})$. This is equivalent to have $L(\mathbf{X}) = \{1\}$ i.e. $\mathbf{X}$ is a projection quandle. A projection quandle is connected if and only if it is trivial. □

By the characterization of congruences through the properties of $Dis_\alpha(\mathbf{X})$, we can get some informations on the subgroup $Dis^\alpha(\mathbf{X})$.

Corollary 6.22. *Let $\boldsymbol{X}$ be a quandle and α be its congruence.*

(i) *If α is Abelian, then $Dis^\alpha(\boldsymbol{X})$ is solvable of rank 2.*
(ii) *If α is central, then $Dis^\alpha(\boldsymbol{X})$ is nilpotent of rank 2.*
(iii) *If α is strongly Abelian, then $Dis^\alpha(\boldsymbol{X})$ is central in $LMlt(\boldsymbol{X})$.*

Proof. (i) By Proposition 6.16, $Dis_\alpha(\mathbf{X})$ is Abelian. Accordingly to Lemma 6.14, we have $Dis^\alpha(\mathbf{X})^{(2)} \leq Dis_\alpha(\mathbf{X})^{(1)} = \{1\}$.

(ii) By Proposition 6.19, $Dis_\alpha(\mathbf{X})$ is central. Accordingly to Lemma 6.14, we have $Dis^\alpha(\mathbf{X})^2 \leq Dis_\alpha(\mathbf{X})^1 = \{1\}$.

(iii) By Proposition 6.20, $Dis_\alpha(\mathbf{X}) = \{1\}$. Accordingly to Lemma 6.14, we have $[LMlt(\mathbf{X}), Dis^\alpha(\mathbf{X})] = \{1\}$. □

If the quandle $\mathbf{X}$ is faithful, then α-regularity of the action on blocks of certain subgroups of the transvection group is for free.

Remark 6.23. *Let $\boldsymbol{X}$ be a faithful quandle and $Dis(\boldsymbol{X}) \geq N \trianglelefteq LMlt(\boldsymbol{X})$. by Proposition 3.28, $h(x) = x \iff hL_xh^{-1} = L_x$. Assume that $h(x) = x$, i.e.*

$$L_x = hL_xh^{-1} = hL_xL_y^{-1}L_yh^{-1}$$

for some $h \in N$. If N is Abelian, then it is α_N-regular.

The same argument show that if N is central, then $Dis(\boldsymbol{X})$ is α_N-regular.

Thus, since $\alpha \leq \alpha_{Dis_\alpha(\boldsymbol{X})}$ for every $\alpha \in Con(\boldsymbol{X})$

(i) *α is Abelian if and only if $Dis_\alpha(\boldsymbol{X})$ is Abelian;*
(ii) *α is central if and only if $Dis_\alpha(\boldsymbol{X})$ is central.*

whenever $\boldsymbol{X}$ is faithful.

6.3. **Abelian Extensions.** Some examples of Abelian congruences are given by *Abelian extensions*. This family of extensions was already defined in [10]. In [1] and [6] the same construction was carried out under the name of *quandle modules*. This family of extensions describes the structure of quandles admitting an Abelian congruence with connected blocks (Theorem 6.30). Therefore, they characterize Abelian congruences in the case of Taylor quandles (Corollary 6.31). All the contents of this Section are new results.

Let $\mathbf{X}$ be a quandle and A be an Abelian group. Then consider the algebra $(X \times A, \cdot)$ defined by setting

$$(x,a)\cdot(y,b) = (xy, \phi(x,y)(a) + \psi(x,y)(b) + \theta(x,y)) = (xy, \beta(x,y,a)(b))$$

for every $x, y \in X$ and $a, b \in A$, where

$$\begin{aligned} \phi : X \times X &\longrightarrow End(A,+) \\ \psi : X \times X &\longrightarrow Aut(A,+) \\ \theta : X \times X &\longrightarrow A \end{aligned}$$

The following Lemma gives the conditions under which $(X \times S, \cdot)$ is a quandle (i.e. the conditions under which the triple $\beta = (\phi, \psi, \theta)$ defines a quandle cocycle).

Lemma 6.24. *Let* $\boldsymbol{X}$ *be a quandle and* A *an Abelian group. Then the triple* (ϕ, ψ, θ) *defines a quandle cocycle if and only if*

$$\begin{aligned} \psi(x,yz)(\theta(y,z)) + \theta(x,yz) &= \psi(xy,xz)(\theta(x,z)) + \phi(xy,xz)(\theta(x,y)) + \theta(xy,xz) \\ \psi(x,yz)\psi(y,z) &= \psi(xy,xz)\psi(x,z) \\ \psi(x,yz)\phi(y,z) &= \phi(xy,xz)\psi(x,y) \\ \phi(x,yz) &= \phi(xy,xz)\phi(x,y) + \psi(xy,xz)\phi(x,z) \\ \theta(x,x) &= 0 \\ \phi(x,x) + \psi(x,x) &= 1 \end{aligned}$$

for every $x, y, z \in X$.

Proof. They follow from left-distributivity and idempotency. □

Extensions defined in this way are called *Abelian*.

Definition 6.25. Let $\mathbf{X}$ be a quandle, A an Abelian group and the maps

$$\begin{aligned} \phi : X \times X &\longrightarrow End(A,+) \\ \psi : X \times X &\longrightarrow Aut(A,+) \\ \theta : X \times X &\longrightarrow A \end{aligned}$$

The extension $\mathbf{X} \times_\beta A$, where β is defined by setting

$$\beta(x,y,a)(b) = \phi(x,y)(a) + \psi(x,y)(b) + \theta(x,y) \tag{16}$$

for every $x, y \in X$ and every $a, b \in A$, is called *Abelian extension of* $\boldsymbol{X}$. The cocycles β will be denoted by (ϕ, ψ, θ).

Remark 6.26. *Modules over a rack, introduced in Definition 2.16 of* [1], *correspond to quandle cocycles given by* $\beta = (\phi, \psi, 0)$.

Remark 6.27. *An Abelian extension $\boldsymbol{X} \times_\beta A$ is Latin if and only if $\boldsymbol{X}$ is Latin and*

$$\phi : X \times X \longrightarrow Aut(A)$$

Indeed, right division has to be defined necessarily by

$$(x,s)/(y,t) = (x/y, \phi^{-1}_{x/y,x}(s - \psi_{x/y,y}(t) - \theta_{x/y,x}))$$

for every $x, y \in X$ and every $s, t \in A$.

The blocks of an Abelian congruences are Abelian quandles and to Abelian extensions correspond Abelian congruences.

Lemma 6.28. *Let $\boldsymbol{X}$ be a quandle and α its Abelian congruence. Then the blocks are Abelian quandles.*

Proof. It follows directly from formula (2), choosing all the variables from the same block of α. □

Lemma 6.29. *Let $\boldsymbol{X}$ be a quandle, $\boldsymbol{X} \times_\beta A$ be an Abelian extension and π the canonical projection over $\boldsymbol{X}$. Then $ker(\pi)$ is an Abelian congruence.*

Proof. It is enough to prove that $Dis_\alpha(\mathbf{X})$ is Abelian and α-semiregular by virtue of 6.16 (ii). Since

$$L_{(x,a)} L^{-1}_{(x,b)}(y,c) = (y, c + \phi(x, x\backslash y)(a-b))$$

for every $x, y \in X$ and every $a, b \in A$, $Dis_\alpha(\mathbf{X})$ acts by translations on every block. Therefore, it is Abelian and α-semiregular. □

The blocks of an Abelian congruences α are Abelian quandles. If they are connected, they are affine (Corollary 6.17), and therefore, they have an induced structure of Abelian group. In this case $\mathbf{X}$ is an Abelian extension of $\mathbf{X}/\alpha$.

Theorem 6.30. *Let $\boldsymbol{X}$ be a quandle and α its Abelian congruence such that $\boldsymbol{X}/\alpha$ is connected. If the blocks of α are connected quandles, then $\boldsymbol{X}$ is an Abelian extension of $\boldsymbol{X}/\alpha$.*

Proof. Let α be Abelian and let the blocks of α be connected. By Corollary 6.17, the blocks are isomorphic to some connected affine quandle $\mathcal{Q}(A,\alpha)$. Let $e \in [x]$, then $([x], +)$ is an Abelian group, where

$$x + y = x/e \cdot e\backslash y$$

So + is a term operation and moreover the maps

$$h_{[x]} : A \longrightarrow [x]$$

can be chosen to be group isomorphisms by Corollary 4.2 of [21].

It is enough to prove that the cocycle β defined as in formula (10), splits as in formula (16) of definition 6.25.

The first step is to prove that

$$\beta(x,y)(a,b) = \beta(x,y)(a,0) + \beta(x,y)(0,b) - \beta(x,y)(0,0), \tag{17}$$

which is equivalent to the identity involving term operations given by

$$h_{[x]}(a)h_{[y]}(b) + h_{[x]}(0)h_{[y]}(0) = h_{[x]}(a)h_{[y]}(0) + h_{[x]}(0)h_{[y]}(b). \tag{18}$$

Equation (18) holds for $a = 0$, therefore, by Abelianness, it holds for every $a \in A$.

Let define $\psi(x,y)(b) = \beta(x,y)(0,b) - \beta(x,y)(0,0)$, hence $\psi(x,y)(0) = 0$. The identity

$$\psi(x,y)(a+b) = \psi(x,y)(a) + \psi(x,y)(b) \tag{19}$$

is equivalent to the equality involving term operations given by

$$h_{[x]}(0)h_{[y]}(a+b) - h_{[x]}(0)h_{[y]}(0) = h_{[x]}(0)h_{[y]}(a) + h_{[x]}(0)h_{[y]}(b) - 2h_{[x]}(0)h_{[y]}(0).$$

The last equality holds for $a = 0$, then by Abelianness it holds for every $a \in A$.

Therefore, identity (19) holds, i.e. $\psi(x,y)$ is a group morphism.

A similar argument shows that $\phi(x,y)(a) = \beta(x,y)(a,0) - \beta(x,y)(0,0)$ is a group morphism. Setting $\beta(x,y)(0,0) = \theta(x,y)$, from equation (17) it follows that

$$\beta(x,y)(a,b) = \phi(x,y)(a) + \psi(x,y)(b) + \theta(x,y)$$

Since left multiplications are bijective, then $\psi(x,y) \in Aut(A)$. □

Corollary 6.31. *Let* $\boldsymbol{X}$ *be a Taylor quandle and* α *be its congruence. Then the following are equivalent:*

(1) α *is Abelian;*
(2) $Dis_\alpha(\boldsymbol{X})$ *is Abelian;*
(3) $\boldsymbol{X}$ *is an Abelian extension of* $\boldsymbol{X}/\alpha$.

Proof. By Remark 6.23 and Lemma 6.29, we just need to prove (1) ⇒ (3).

Since all the subquandles of **X** are connected, then the blocks of α are connected. Therefore, by Theorem 6.30, if α is Abelian then **X** is an Abelian extension of $\mathbf{X}/\alpha$. □

6.4. **Solvable and Nilpotent Quandles.** Connected Abelian quandles are characterized by Corollary 6.17. In a variety other interesting classes of algebras are the classes of *solvable* and *nilpotent* algebras, which are defined in an analogous way to solvable and abelian groups.

In this Section we investigate the relationship between the solvability of a quandle and the solvability of its transvection group. In class of Taylor quandles solvability (nilpotency) of a quandle is characterized by the solvability (nilpotency) of its transvection group (Theorems 6.38 and 6.40).

We also characterize the *center* of a quandle. All the results of this Section are original.

Definition 6.32. [15, Lemma 5.2] Let **X** be a quandle. Then the center of **X** is the largest central congruence. It is denoted by $\mathcal{Z}(\mathbf{X})$.

Remark 6.33. *By Proposition 6.19 it follows that* $\mathcal{Z}(\boldsymbol{X})$*, as any other central congruence, has to be contained in* $\alpha_{Z(Dis(\boldsymbol{X}))}$ *and in the equivalence defined by*

$$x \sim y \iff Dis(\boldsymbol{X})_x = Dis(\boldsymbol{X})_y$$

Proposition 6.34. *Let* $\boldsymbol{X}$ *be a quandle. Then*

$$\mathcal{Z}(\boldsymbol{X}) = \alpha_{Z(Dis(\boldsymbol{X}))} \cap \{(x,y) \in X \times X,\ Dis(\boldsymbol{X})_x = Dis(\boldsymbol{X})_y\} \tag{20}$$

Proof. By remark 6.33, it is enough to show that the right hand side of (20) is a central congruence. Let call it β.

Let $(x, y) \in \beta$ and $z \in \mathbf{X}$. Since $\alpha_{Z(Dis(\mathbf{X}))}$ is a congruence, it is enough to check if the second condition holds for (zx, zy), $(z\backslash x, z\backslash y)$ and (xz, yz) to prove that β is a congruence. Then

$$Dis(\mathbf{X})_{L_z^{\pm 1}(x)} = L_z^{\pm 1} Dis(\mathbf{X})_x L_z^{\mp 1} = L_z^{\pm 1} Dis(\mathbf{X})_y L_z^{\mp 1} = Dis(\mathbf{X})_{L_z^{\pm 1}(y)}$$

Note that the second condition is equivalent to

$$\forall h \in Dis(\mathbf{X}),\ h(x) = x \iff h(y) = y \tag{21}$$

Let $h \in Dis(\mathbf{X})$, and assume that $h(xz) = xz$, which is equivalent to $L_x h L_x^{-1}(z) = z$. Then

$$L_y h L_y^{-1}(z) = L_y h L_y^{-1} L_x h L_x^{-1}(z) \overset{L_y^{-1} L_x \in Z(Dis(\mathbf{X}))}{=} L_x h L_x^{-1} L_x h L_x^{-1}(z) = z$$

therefore $h(yz) = yz$. Hence, β is a congruence and it is central by Proposition 6.19. ☐

Let us introduce the class of solvable and nilpotent algebras.

Definition 6.35. An algebra $\mathbf{X}$ is said to be

(a) *solvable* if there exists a chain of congruences

$$0_{\mathbf{X}} = \alpha_0 \leq \alpha_1 \leq \ldots \leq \alpha_n = 1_{\mathbf{X}}$$

such that α_k/α_{k-1} is Abelian for every $1 \leq k \leq n$;

(b) *nilpotent* if there exists a chain of congruences

$$0_{\mathbf{X}} = \alpha_0 \leq \alpha_1 \leq \ldots \leq \alpha_n = 1_{\mathbf{X}}$$

such that α_k/α_{k-1} is central for every $1 \leq k \leq n$.

In general, solvability and nilpotency of a quandle is a stronger property than to have solvable or nilpotent transvection group.

Proposition 6.36. *Let $\mathbf{X}$ be a solvable quandle. Then $Dis(\mathbf{X})$ is solvable.*

Proof. Let proceed by induction on the length of the chain of congruences

$$0_{\mathbf{X}} \leq \alpha_1 \leq \ldots \leq \alpha_k \leq 1_{\mathbf{X}}$$

where α_{i+1}/α_i is Abelian.

If $k = 1$, then $Dis(\mathbf{X})$ is Abelian (Corollary 6.17). If $k > 1$, then

$$0_{\mathbf{X}/\alpha_1} \leq \alpha_2/\alpha_1 \leq \ldots \leq \alpha_k/\alpha_1 \leq 1_{\mathbf{X}/\alpha_1}$$

is a chain of congruences in $\mathbf{X}/\alpha_1$ and $(\alpha_{i+1}/\alpha_1)/(\alpha_i/\alpha_1)$ is Abelian by Lemma 1.24 (i). By induction, $Dis(\mathbf{X}/\alpha_1)$ is solvable and $Dis^{\alpha_1}(\mathbf{X})$ is solvable by Corollary 6.22 (i). Since

$$Dis(\mathbf{X}/\alpha_1) \simeq Dis(\mathbf{X})/Dis^{\alpha_1}(\mathbf{X})$$

then $Dis(\mathbf{X})$ is solvable. ☐

Proposition 6.37. *Let $\mathbf{X}$ be a nilpotent quandle. Then $Dis(\mathbf{X})$ is nilpotent.*

Proof. Let prove the statement by induction on the length of the chain of congruences

$$0_{\mathbf{X}} \leq \alpha_1 \leq \ldots \leq \alpha_k \leq 1_{\mathbf{X}}$$

where α_{i+1}/α_i is central.

If $k = 1$, by Corollary 6.17, $Dis(\mathbf{X})$ is Abelian. If $k > 1$, then

$$0_{\mathbf{X}/\alpha_1} \leq \alpha_2/\alpha_1 \leq \ldots \leq \alpha_k/\alpha_1 \leq 1_{\mathbf{X}/\alpha_1}$$

is a chain of congruences in $\mathbf{X}/\alpha_1$ such that $(\alpha_{i+1}/\alpha_1)/(\alpha_i/\alpha_1)$ is central by Lemma 1.24 (ii). By induction, $Dis(\mathbf{X}/\alpha_1)$ is nilpotent, then $Dis(\mathbf{X})^n \leq Dis^{\alpha_1}(\mathbf{X})$ for some n. Therefore,

$$Dis(\mathbf{X})^{n+1} = [Dis(\mathbf{X})^n, Dis(\mathbf{X})] \leq [Dis^{\alpha_1}(\mathbf{X}), Dis(\mathbf{X})] \leq Dis_{\alpha_1}(\mathbf{X})$$

Since $Dis_{\alpha_1}(\mathbf{X})$ is central, then $Dis(\mathbf{X})^{n+2}$ is trivial. □

The converse holds in the class of Taylor quandles.

Theorem 6.38. *Let* $\boldsymbol{X}$ *be a Taylor quandle and* $Dis(\boldsymbol{X})$ *be solvable. Then* $\boldsymbol{X}$ *is a solvable quandle.*

Proof. Let prove the statement by induction on the length of the derived series.

If the length is 1 then $\mathbf{X}$ is affine and then Abelian by Corollary 6.17.

Let assume that the length is $n+1$, i.e. $Dis(\mathbf{X})^{(n+1)} = \{1\}$. Then $Dis(\mathbf{X})^{(n)}$ is Abelian and normal in $LMlt(\mathbf{X})$. By item (i) of Remark 6.31, $\alpha = \alpha_{Dis(\mathbf{X})^{(n)}}$ is an Abelian congruence of $\mathbf{X}$. Since $Dis(\mathbf{X}/\alpha) = Dis(\mathbf{X})/Dis^{\alpha}(\mathbf{X})$ and $Dis(\mathbf{X})^{(n)} \leq Dis^{\alpha}(\mathbf{X})$, then it is solvable of rank n. The factor $\mathbf{X}/\alpha$ is Taylor, hence by induction there exists a chain of congruences

$$0_{\mathbf{X}/\alpha} \leq \beta_1 \leq \ldots \leq \beta_k \leq 1_{\mathbf{X}/\alpha}$$

where $\beta_i = \alpha_i/\alpha$ for some congruences α_i of $\mathbf{X}$ containing α and β_{i+1}/β_i is Abelian.

In the correspondent sequence of congruences of $\mathbf{X}$,

$$0_{\mathbf{X}} \leq \alpha \leq \alpha_1 \leq \ldots \leq \alpha_k \leq 1_{\mathbf{X}}$$

α_{i+1}/α_i is Abelian since β_{i+1}/β_i is Abelian for every $1 \leq i \leq k$ by Lemma 1.24 (i). □

Corollary 6.39. *Let* $\boldsymbol{X}$ *be a Latin quandle. Then it is a solvable quandle.*

Proof. It follows by Theorem 6.38, since $\mathbf{X}$ is Taylor and $Dis(\mathbf{X})$ is solvable by Theorem 1.4 of [29]. □

Theorem 6.40. *Let* $\boldsymbol{X}$ *be a Taylor quandle and* $Dis(\boldsymbol{X})$ *be nilpotent. Then* $\boldsymbol{X}$ *is a nilpotent quandle.*

Proof. Let prove the statement by induction on the length of the central series.

If the length is 1 then $\mathbf{X}$ is affine and then Abelian by Corollary 6.17.

Let assume that the length is $n+1$, i.e. $Dis(\mathbf{X})^{n+1} = \{1\}$. Then $Dis(\mathbf{X})^n$ is central and normal in $LMlt(\mathbf{X})$. By item (ii) of Remark 6.23, $\alpha = \alpha_{Dis(\mathbf{X})^n}$ is a central congruence of $\mathbf{X}$. Since $Dis(\mathbf{X}/\alpha) = Dis(\mathbf{X})/Dis^{\alpha}(\mathbf{X})$ and $Dis(\mathbf{X})^n \leq Dis^{\alpha_n}(\mathbf{X})$, then it is nilpotent of rank n. Since $\mathbf{X}/\alpha$ is Taylor, then by induction there exists a chain of congruences

$$0_{\mathbf{X}/\alpha} \leq \beta_1 \leq \ldots \leq \beta_k \leq 1_{\mathbf{X}/\alpha}$$

where $\beta_i = \alpha_i/\alpha$ for some congruences α_i of $\mathbf{X}$ containing α and β_{i+1}/β_i is central.

In the correspondent sequence of congruences of $\mathbf{X}$

$$0_{\mathbf{X}} \leq \alpha \leq \alpha_1 \leq \ldots \leq \alpha_k \leq 1_{\mathbf{X}}$$

α_{i+1}/α_i is central for every $1 \leq i \leq k$, since β_{i+1}/β_i is central, by Lemma 1.24 (ii). □

6.5. **Extensions preserving Transvection Group.** This Section is about finite connected extensions preserving the transvection group. First we show that an extension preserves the transvection group only if it is a covering and then we give a complete characterization of finite coverings with this property.

Lemma 6.41. *Let $\boldsymbol{X}$ be a finite quandle and α be its congruence. If $Dis(\boldsymbol{X}) \simeq Dis(\boldsymbol{X}/\alpha)$ then $(\boldsymbol{X}, \pi_\alpha)$ is a covering of $\boldsymbol{X}/\alpha$.*

Proof. If $Dis(\mathbf{X}) \simeq Dis(\mathbf{X}/\alpha)$, then they have the same size. Since π_α^* is surjective then it is an isomorphism. Therefore, $Dis_\alpha(\mathbf{X}) \leq Dis^\alpha(\mathbf{X}) = \{1\}$. By Proposition 6.20, $(\mathbf{X}, \pi_\alpha)$ is a covering of $\mathbf{X}/\alpha$. □

The following Proposition characterizes the finite connected extensions preserving the transvection group. By virtue of Lemma 6.41, it is not restrictive to consider just coverings.

Proposition 6.42. *Let $(\boldsymbol{X}, \pi_\alpha)$ be a finite connected covering of $\boldsymbol{X}/\alpha$. Then the following are equivalent:*

(1) $Dis(\boldsymbol{X}) \simeq Dis(\boldsymbol{X}/\alpha)$;
(2) $\boldsymbol{X} \simeq \mathcal{Q}(Dis(\boldsymbol{X}/\alpha), H, \widehat{L_{[x]}})$ *for some* $H \leq Dis(\boldsymbol{X}/\alpha)_{[x]}$.

Proof. (1) $\Rightarrow$ (2) Let $(\mathbf{X}, \pi_\alpha)$ be a connected covering of $\mathbf{X}/\alpha$, and assume that $Dis(\mathbf{X}) \simeq Dis(\mathbf{X}/\alpha)$. Since $|Dis(\mathbf{X})| = |Dis(\mathbf{Y})|$, the group morphism

$$\pi_\alpha^* : Dis(\mathbf{X}) \longrightarrow Dis(\mathbf{X}/\alpha)$$

is an isomorphism. Let $h \in Dis(\mathbf{X})_x$, then

$$\pi_\alpha^*(h)([x]) = [h(x)] = [x]$$

and then $H = \pi_\alpha^*(Dis(\mathbf{X})_x) \leq Dis(\mathbf{X}/\alpha)_{[x]}$. Then the map

$$\phi : \mathcal{Q}(Dis(\mathbf{X}), Dis(\mathbf{X})_x, \widehat{L_x}) \longrightarrow \mathcal{Q}(Dis(\mathbf{X}/\alpha), H, \widehat{L_{[x]}}), \quad hDis(\mathbf{X})_x \mapsto \pi_\alpha^*(h)H$$

is a well defined isomorphism of quandles.

(2) $\Rightarrow$ (1) Let $\mathbf{Y}_H = (Dis(\mathbf{X}/\alpha), H, \widehat{L_{[x]}})$ for some $H \leq Dis(\mathbf{X}/\alpha)_{[x]}$. First note that $\mathbf{Y}_H$ is a connected covering of $\mathbf{X}/\alpha$ by Remark 3.22 and Proposition 5.25.

By Proposition 3.21 $Dis(\mathbf{Y}_H) \simeq Dis(\mathbf{X}/\alpha)$. □

7. Simple Abelian Quandles

7.1. **Doubly transitive Action.** This Section is about finite quandles which automorphism group is *doubly transitive*. We do not show a characterization of this class of quandles but we just point out that any quandle with this property is either projection or Latin. We show some property of quandle of this class which will be used in the following Sections.

A group action is k-transitive if it is transitive on k-tuples with distinct entries. If $k = 2$, the group is called *doubly transitive* The automorphism group of non projection quandles can be at most doubly transitive, at least if the quandle is not very small.

Proposition 7.1. [25, Proposition 5] *Every quandle with at least four elements and a 3-transitive automorphism group is projection.*

Remark 7.2. *The automorphism group of finite projection quandles is the whole permutation group of the underlying set, which is n-transitive, where n is the size of the set. Then is is in particular doubly transitive.*

Doubly transitive actions can be characterized in the following well known way.

Proposition 7.3. *Let G be a group, then the following are equivalent:*

(1) *A group G is doubly transitive on a set X;*
(2) *G_x is transitive on $X \setminus \{x\}$ for every $x \in X$.*

Quandles which automorphism group is doubly transitive are contained within two classes: Latin quandles and projection quandles.

Lemma 7.4. *Let $\mathbf{X}$ be a non-projection finite quandle. If $Aut(\mathbf{X})$ acts doubly transitively on X, then $\mathbf{X}$ is Latin.*

Proof. Since $\mathbf{X}$ is not a projection quandle, then for every $x \in X$ there exists $y \in X$ such that $yx \neq x$, since it is homogeneous. Let $z \in X$, then there exists $f \in Aut(\mathbf{X})_x$ such that $z = f(yx)$, since $Aut(\mathbf{X})$ is doubly transitive. Then

$$z = f(yx) = f(y)x = R_x(f(y))$$

and then R_x is surjective. Since $\mathbf{X}$ is finite, R_x is a bijection for every $x \in X$. □

The two-transitivity of $Aut(\mathbf{X})$ allows to verify identities between binary term operations just on an arbitrary pair of elements of $\mathbf{X}$.

Proposition 7.5. *Let $\mathbf{X}$ be quandle such that $Aut(\mathbf{X})$ acts doubly transitively on $\mathbf{X}$ and t and s be binary quandle term operations. Then the following are equivalent:*

(1) *there exists $x, y \in X$, $x \neq y$ such that $t(x,y) = s(x,y)$;*
(2) *$t \approx s$.*

Proof. Note that $t(x,x) = x = s(x,x)$ for every $x \in X$, since $\mathbf{X}$ is idempotent.

Assume that $t(x,y) = s(x,y)$ holds for some $x \neq y \in X$. Let $h \in Aut(\mathbf{X})$, then

$$t(h(x), h(y)) = h(t(x,y)) = h(s(x,y)) = s(h(x), h(y))$$

Since $Aut(\mathbf{X})$ is doubly transitive, it holds for every pair $(z,t) \in X \times X$. Hence, $t \approx s$. □

This Proposition actually holds for any idempotent algebra $\mathbf{X}$ for which $Aut(\mathbf{X})$ is doubly transitive.

Corollary 7.6. *Let $\mathbf{X}$ be a finite quandle. If $Aut(\mathbf{X})$ acts doubly transitively on X then $\langle L_x \rangle$ acts semiregularly on $X \setminus \{x\}$, for every $x \in X$.*

Proof. Let $x \neq y \in X$ and $k \in \mathbb{Z}$ such that $L_x^k(y) = y$. By Proposition 7.5, it holds for every $x, y \in X$ since it is an identity between binary terms, i.e., $L_x^k = 1$. Therefore, the group $\langle L_x \rangle$ is semiregular on $\mathbf{X} \smallsetminus \{x\}$. □

A quandle is said to be *semiregular* whenever $\langle L_x \rangle$ is semiregular on $\mathbf{X} \smallsetminus \{x\}$ for every $x \in X$.

Remark 7.7. *For finite quandles this property is equivalent to have*

$$|O_{\langle L_x \rangle}(y)| = o(L_x)$$

for every $x, y \in X$, i.e. the cycle decomposition of L_x is given by disjoint cycles of the same length, namely $o(L_x)$. If $\boldsymbol{X}$ is strongly faithful then $o(L_x)$ divides $|X| - 1$.

The class of quandles with doubly transitive left multiplication group has the following characterization.

Theorem 7.8. [33, Corollary 4] *Let $\boldsymbol{X}$ be a quandle. Then the following are equivalent:*

(1) *$LMlt(\boldsymbol{X})$ is doubly transitive;*
(2) *$\boldsymbol{X} \simeq \mathcal{Q}\left(\mathbb{Z}_p^n, \alpha\right)$ and $o(\alpha) = |X| - 1$.*

A characterization of the class of finite Latin quandles with doubly transitive automorphism group is still unknown.

Problem 4. Find a characterization of the class of finite Latin quandles with doubly transitive automorphism group.

7.2. **Minimal Quandles.** In this Section we investigate the class of finite *minimal quandles*, i.e., finite quandles with no proper subquandles and we prove that this class is given by the finite *simple Abelian* quandles.

In universal algebra is known that simple Abelian algebra has no proper subalgebras (Theorem 3.4 of [32]), so we prove that also the converse is true in the variety of quandles.

Simple quandles has been characterized by Joyce in [23] and the first paper about minimal left-distributive quasigroup is the paper of Galkin ([16]).

It turns out that minimal quandles are characterized by several different properties among the simple ones, and we collect them in Theorem 7.18.

Moreover, this characterization allows us to show that there is no finite quandle which satifies *meet semidistributivity* in Theorem 7.19.

Definition 7.9. A quandle $\mathbf{X}$ is called

(a) *simple* if the lattice of the congruences has just two elements $1_{\mathbf{X}}$ and $0_{\mathbf{X}}$;
(b) *minimal* if every proper subquandle of $\mathbf{X}$ is trivial.

Proposition 7.10. *Let $\boldsymbol{X}$ be a minimal quandle. Then $\boldsymbol{X}$ is simple.*

Proof. Let $\mathbf{X}$ be minimal and α a congruence. Since every block of α is a subquandle, then either $\alpha = 1_{\mathbf{X}}$ or $\alpha = 0_{\mathbf{X}}$. □

The following Propositions show some properties of simple quandles.

Proposition 7.11. [22, Lemma 1] *Let $\boldsymbol{X}$ be a simple quandle and $|X| \neq 2$. Then it is connected and faithful.*

Proposition 7.12. *Let $\boldsymbol{X} \simeq \mathcal{Q}(Dis(\boldsymbol{X}), Dis(\boldsymbol{X})_x, \widehat{L_x})$ be a simple quandle. Then $Dis(\boldsymbol{X})$ has no proper normal subgroups invariant under $\widehat{L_x}$. In particular it has no proper characteristic subgroups.*

Proof. By Lemma 4.2 of [4], any proper normal subgroup $N \leq Dis(\mathbf{X})$ invariant under $\widehat{L_x}$ is normal in $LMlt(\mathbf{X})$. By Lemma 6.5, it provides a congruence. Therefore, either $N = \{1\}$ or $N = Dis(\mathbf{X})$. □

Minimal quandles are precisely quandles generated by any pair of elements. Note that this property characterizes minimal quandles among all quandles without any finiteness assumption.

Proposition 7.13. *Let $\boldsymbol{X}$ be a quandle. Then it is minimal if and only if it is generated by any pair of elements $x, y \in X$. Moreover, every group of automorphisms of $\boldsymbol{X}$ is Frobenius.*

Proof. If $\mathbf{X}$ is minimal then the subquandle generated by x, y has size at least 2, therefore is the whole $\mathbf{X}$.

Assume that $\mathbf{X}$ is generated by any pair of elements. Let Q be a subquandle and $x, y \in Q$. Then $\mathbf{X} = Sg(\{x, y\}) \leq Q$. Therefore $Q = \mathbf{X}$.

Let G be a group of automorphisms and $g \in G$ such that $g(x) = x$ and $g(y) = y$ for some $x, y \in X$. Let $z \in X$, then $z = t^{\mathbf{X}}(x_1, \dots, x_n)$, for some term operation $t^{\mathbf{X}}$ and $x_i \in \{x, y\}$ for every $1 \leq i \leq n$, since $\mathbf{X} = Sg(\{x, y\})$. Therefore,

$$g(z) = g(t^{\mathbf{X}}(x_1, \dots, x_n)) = t^{\mathbf{X}}(g(x_1), \dots, g(x_n)) = t^{\mathbf{X}}(x_1, \dots, x_n) = z$$

for every $z \in X$. □

Proposition 7.13 holds for every finite idempotent algebra with no proper subalgebras.

Any finite minimal quandles has an affine representations over an elementary Abelian group.

Lemma 7.14. *Let G be a finite solvable group with no proper charateristic group. Then it is elementary Abelian.*

Proof. The commutator subgroup $G^{(1)}$ is proper, since G is solvable, therefore G is Abelian. Every p-Sylow is unique, since it is normal, and therefore it is characteristic. Hence, G is a p-group. Finally, the Frattini subgroup of G is trivial, then it is elementary Abelian. □

Proposition 7.15. *Let $\boldsymbol{X}$ be a finite quandle and $|X| \neq 2$. Then the following are equivalent:*

(1) *$\boldsymbol{X}$ is minimal;*
(2) *$\boldsymbol{X} \simeq \mathcal{Q}(\mathbb{Z}_p^n, \alpha)$ and α has no proper invariant subgroups.*

Proof. (1) ⇒ (2) Assume that $\mathbf{X}$ is minimal, then it is simple and connected and $Dis(\mathbf{X})$ is a Frobenius group (Proposition 7.13). By Theorem 1 of [30], it has a regular nilpotent subgroup N. Since $\mathbf{X}$ is connected, $Dis(\mathbf{X}) = N$ (see Remark 4.3) and therefore it is nilpotent.

By Lemma 7.14, $Dis(\mathbf{X})$ is elementary Abelian, and it has no α-invariant subgroups by Proposition 7.12.

(2) $\Rightarrow$ (1) Assume that $\mathbf{X} \simeq \mathcal{Q}(\mathbb{Z}_p^n, \alpha)$ is simple and α has no proper invariant subgroups. Therefore, it is affine and connected, hence Latin. By Corollary 4.7, $\mathbf{X}$ is minimal. □

The automorphism group of minimal quandles is doubly transitive.

Proposition 7.16. *Let $\boldsymbol{X}$ be a finite minimal quandle. Then $Aut(\boldsymbol{X})$ is doubly transitive.*

Proof. By Proposition 7.15, $\mathbf{X} \simeq \mathcal{Q}(\mathbb{Z}_p^n, \alpha)$. Let $x \in X$ and let $\mathbf{a} = (a_0, a_1, \dots, a_{n-1}) \in \mathbb{Z}_p^n$ be a non zero vector, such that

$$\sum_{i=0}^{n-1} a_i \alpha^i(x) = 0$$

Then the subgroup generated by the set $B_x = \{\alpha^i(x),\ 0 \leq i \leq n-1\}$ is invariant under α. Therefore, the set B_x is a base for $\mathbb{Z}_p^n$, since α has no invariant subgroups.

The map

$$f_{\mathbf{a}} : X \longrightarrow X, \qquad x \mapsto \sum_{i=0}^{n-1} a_i \alpha^i(x)$$

is an automorphism for every non-zero vector $\mathbf{a} \in \mathbb{Z}_p^n$, since B_x is a base for every $x \in X$. The subgroup $\mathcal{F} = \langle f_{\mathbf{a}},\ \mathbf{a} \in \mathbb{Z}_p^n \rangle$ is a subgroup of $Aut(\mathbf{X})_0$, since $f_{\mathbf{a}} \in C_{Aut(\mathbf{X})}(\alpha)$.

Let $x \in X$ and $\mathbf{a}$, then

$$\sum_{i=0}^{n-1} a_i \alpha^i(x) = x \iff (\alpha_0 - 1)x + \sum_{i=1}^{n-1} a_i \alpha^i(x) = 0$$

Therefore, $\mathbf{a} = (1, 0, \dots, 0)$ and then $\mathcal{F}$ is semiregular on $X \setminus \{0\}$. The size of $\mathcal{F}$ is $p^n - 1$, then it is transitive on $X \setminus \{0\}$. By Proposition 7.3, $Aut(\mathbf{X})$ is doubly transitive. □

Remark 7.17. *Let $\boldsymbol{X} = \mathcal{Q}(\mathbb{Z}_p^n, \alpha)$ be a minimal quandle. Since every orbit under α generates an invariant subgroup then it has to contain a base. Then $n \leq o(\alpha)$.*

Moreover, by Corollary 7.6, $\boldsymbol{X}$ is semiregular, since $Aut(\boldsymbol{X})$ is doubly transitive.

Note that if $\boldsymbol{X}$ is involutory then $n = 1$. Indeed,

$$\alpha^2 = 1 \implies \alpha = -1$$

and then every subgroups would be invariant under α.

The following proposition summarizes all the contents of this Section, in order to show several different characterization of minimal quandles among the simple ones.

Theorem 7.18. *Let $\boldsymbol{X}$ be a finite simple quandle and $|X| > 2$. Then the following are equivalent:*

(1) *$\boldsymbol{X}$ is Abelian;*
(2) *$\boldsymbol{X}$ is minimal;*
(3) *$\boldsymbol{X} \simeq \mathcal{Q}(\mathbb{Z}_p^n, \alpha)$ and α has no proper invariant subgroups;*
(4) *$Aut(\boldsymbol{X})$ is doubly transitive;*
(5) *$\boldsymbol{X}$ is Latin.*

Proof. (1) ⇒ (2) By Theorem 3.4 of [32], every simple Abelian algebras has no proper subalgebras.

(2) ⇔ (3) It follows by Proposition 7.15.

(3) ⇒ (4) It follows by Proposition 7.16.

(4) ⇒ (5) It follows by Lemma 7.4.

(5) ⇒ (1) By Theorem 1.4 of [29], $Dis(\mathbf{X})$ is solvable, so it is elementary Abelian by Proposition 7.12 and Lemma 7.14. Therefore, by Proposition 6.17, $\mathbf{X}$ is Abelian. □

The proof of Theorem 1.4 of [29] uses the classification of finite simple groups.

Any finite quandle has a simple Abelian subquandle, since any minimal non trivial element of the lattice of the subquandles is simple Abelian, since it has no proper subquandles. This allows us to state the following theorem.

Theorem 7.19. *There are no finite quandles $\boldsymbol{X}$ satisfying meet semidistributivity.*

Proof. Consider the lattice of subquandles of a finite quandle. Then minimal non trivial elements of the lattice are subquandles with no proper subquandles. Therefore they are simple Abelian quandles by Proposition 7.18.

Hence, $\mathcal{S}(\mathbf{X}) \subset \mathcal{HS}(\mathbf{X})$ contains simple Abelian quandles. By Proposition 1.30, $\mathcal{V}(\mathbf{X})$ does not satisfies $SD(\wedge)$. □

8. Cohomology of Latin quandle

8.1. **Non-Faithful quandles.** In this Section we present some further details about the congruence lattices of non-faithful quandles. We reformulate Proposition 3.1 of [1] in the language of universal algebra (Proposition 8.1) and we show that there exists a minimal congruence among those with faihful factor (Proposition 8.2).

Non-faithful quandles have a particular chain of congruences, as shown in the following Proposition.

Proposition 8.1. *Let $\boldsymbol{X}$ be a finite quandle. There exists a chain of congruences*

$$0_{\boldsymbol{X}} = \alpha_0 \leq ker(L_{\boldsymbol{X}}) = \alpha_1 \leq \alpha_2 \leq \ldots \leq \alpha_n$$

such that α_{k+1}/α_k is strongly Abelian for every $1 \leq k \leq n-1$ and $\boldsymbol{X}/\alpha_n$ is faithful.

Proof. If $\mathbf{X}$ is faithful, then $ker(L_{\mathbf{X}}) = 0_{\mathbf{X}}$ and therefore the length of the chain is 1.

Assume that $\mathbf{X}$ is not faithful, then the chain of morphism

$$\mathbf{X} \longrightarrow L(\mathbf{X}) \simeq \mathbf{X}/ker(L_{\mathbf{X}}) \longrightarrow LL(\mathbf{X}) \simeq \mathbf{X}/\alpha_1 \longrightarrow \ldots \longrightarrow L^k(\mathbf{X}) \simeq \mathbf{X}/\alpha_k \longrightarrow \ldots$$

correspond to a chain of congruences

$$ker(L_{\mathbf{X}}) \leq \alpha_2 \leq \ldots \leq \alpha_k \leq \ldots$$

Since $\mathbf{X}$ is finite, the chain stops when $\mathbf{X}/\alpha_n$ is faithful. Moreover

$$L^k(\mathbf{X}) = L(\mathbf{X}/\alpha_{k-1}) \simeq \mathbf{X}/\alpha_k \simeq (\mathbf{X}/\alpha_{k-1})/(\alpha_k/\alpha_{k-1})$$

Therefore, $\alpha_k/\alpha_{k-1} = ker(L_{\mathbf{X}/\alpha_{k-1}})$ and it is strongly Abelian. □

Corollary 8.2. *Let $\boldsymbol{X}$ be a finite connected non-faithful quandle. Then there exists a proper minimal congruence with faithful factor.*

Proof. By Proposition 8.1, there exists a chain of congruences

$$0_{\mathbf{X}} = \alpha_0 \leq ker(L_{\mathbf{X}}) = \alpha_1 \leq \alpha_2 \leq \ldots \leq \alpha_n$$

such that α_{i+1}/α_i is strongly Abelian for every $1 \leq k \leq n-1$. Assume that $\mathbf{X}/\alpha_n$ is trivial. Since $L(\mathbf{X}/\alpha_{n-1}) \in \mathcal{H}(\mathbf{X}/\alpha_n)$, $\mathbf{X}/\alpha_{n-1}$ is projection and connected, hence trivial. Therefore, $\mathbf{X}$ is trivial and then faithful, contradiction. Hence α_n is proper and $\mathbf{X}/\alpha_n$ is faithful.

Let and $\beta \in Con(\mathbf{X})$ such that $\mathbf{X}/\beta$ is faithful. Then by Lemma 3.23, there exists a morphism between $L^n(\mathbf{X}) \simeq \mathbf{X}/\alpha_n$ and $\mathbf{X}/\beta$, i.e. $\alpha_n \leq \beta$. □

Corollary 8.3. *Let $\boldsymbol{X}$ be a faithful quandle and $(\boldsymbol{Y}, \phi)$ be a covering of $\boldsymbol{X}$. Then $\boldsymbol{X} \simeq L(\boldsymbol{Y})$.*

Proof. Let $\alpha \leq ker(L_{\mathbf{Y}})$ such that $\mathbf{X} \simeq \mathbf{Y}/\alpha$ is faithful. By Proposition 8.1,

$$ker(L_{\mathbf{Y}}) \leq \alpha \leq ker(L_{\mathbf{Y}}).$$

Therefore, $\alpha = ker(L_{\mathbf{Y}})$. □

8.2. **Normalized Cocycles.** The following Sections are about cocycles describing non-faithful quandles for which the length of the chain of congruences defined in Proposition 8.1 is one (i.e. $\alpha = ker(L_{\mathbf{X}})$ as shown by Lemma 8.3) and moreover the factor is Latin.

Hence, we are interested in the computation of the cohomology of Latin quandles. For Latin quandles it is possible to define special representatives of the elements of $H^2_c(\mathbf{X}, \mathrm{Sym}(S))$ with some nice properties, called *normalized cocycles*. The definition of such a cocycles has been inspired by Lemma 5.1 of [17].

In the sequel we show some properties of normalized cocycles which will be used to show that quandles belonging to some families of Latin quandles have trivial cohomology by using a combinatorial approach.

All the following computations work for cocycles with coefficients in any group Γ.

Definition 8.4. Let $\mathbf{X}$ be a Latin quandle, $u \in X$ and $\beta \in Z^2_c(\mathbf{X}, \Gamma)$. If

$$\beta(x, u) = 1 \tag{N}$$

for every $x \in X$, then β is said to be *u-normalized*. This condition will be called the normalization condition.

Every class in $H^2(\mathbf{X}, \Gamma)$ has a normalized representative.

Proposition 8.5. *Let $\boldsymbol{X}$ be a Latin quandle, $u \in X$ and $\beta \in Z^2_c(\boldsymbol{X}, \Gamma)$. Then there exists a u-normalized cocycle β_u, such that $\beta_u \sim \beta$.*

Proof. We want to find a suitable γ to get a u-normalized cocycle. Hence

$$\beta_u(x, u) = \gamma(xu)\,\beta(x, u)\,\gamma(u)^{-1} = 1 \Longleftrightarrow \gamma(xu) = \gamma(u)\,\beta(x, u)^{-1}$$

for every $x \in X$. Then, necessarily $\gamma(x) = \gamma(u)\,\beta(x/u, u)^{-1}$ for every $x \in X$. The map γ is well defined since

$$\gamma(u) = \gamma(u)\,\beta(u/u, u)^{-1} = \gamma(u)\,\beta(u, u)^{-1} = \gamma(u)$$

So γ is unique up to the choice of $\gamma(u)$, so we can choose $\gamma(u) = 1$. □

Remark 8.6. *Note that the choice of $u \in X$ in Proposition 8.5 is arbitrary.*

Proposition 8.7. *Let $\boldsymbol{X}$ be a Latin quandle, $u \in X$, $\beta, \beta' \in Z^2_c(\boldsymbol{X}, \Gamma)$ and β_u, β'_u the u-normalized cocycle cohomologous to β and β'.*
Then $\beta \sim \beta'$ if and only if

$$\beta'_u(x,y) = a\beta_u(x,y)a^{-1}$$

for some $a \in S$. Then $\beta \sim \boldsymbol{1}$ if and only if $\beta_u = \mathbf{1}$, for every $u \in X$.

Proof. Clearly $\beta \sim \beta'$ if and only if $\beta_u \sim \beta'_u$. Then there exists $\gamma : X \longrightarrow \mathrm{Sym}(S)$ such that

$$\beta'_u(x,y) = \gamma(xy)\,\beta_u(x,y)\gamma(y)^{-1}$$

for every $x, y \in X$. Since $\beta_u(x,u) = \beta'_u(x,u) = 1$ for every $x \in X$, we have

$$\gamma(xu) = \gamma(u)$$

for every $x \in X$. Since R_u is a permutation we get that γ is a constant map.
The second claim follows since $\mathbf{1}$ is a u-normalized cocycle. □

Remark 8.8. *Proving that $H^2_c(\boldsymbol{X}, \Gamma) = \{\boldsymbol{1}\}$ is therefore equivalent to show that $\beta_u = \boldsymbol{1}$ for every $\beta \in Z^2_c(\boldsymbol{X}, \Gamma)$.*

Normalized cocycles are invariant under an action of a permutation group on the set $X \times X$.

This invariance is granted by the identities following by the normalization condition (together with the cocycle condition).

Proposition 8.9. *Let $\boldsymbol{X}$ be a Latin quandle, $u \in X$ and $\beta \in Z^2_c(\boldsymbol{X}, \Gamma)$ a u-normalized cocycle, then the following equivalent identities hold*

(1) *$\beta(u,x) = 1$ for every $x \in X$;*
(2) *$\beta(ux,uy) = \beta(x,y)$ for every $x, y \in X$.*

Therefore, β is invariant under the diagonal action of L_u.

Proof. First we proove that (1) and (2) are equivalent and then we proove just (1).
Moreover it is easy to see that (2) is equivalent to invariance of β under the diagonal action of L_u.

(1) ⇒ (2) It follows from (CC), since

$$\beta(ux,uy) \overset{(1)}{=} \beta(ux,uy)\,\beta(u,y) \overset{CC}{=} \beta(u,xy)\,\beta(x,y) \overset{(1)}{=} \beta(x,y)$$

(2) ⇒ (1) Let $x = u/y$, then

$$\begin{aligned} \beta(u,y) &\overset{CC}{=} \beta(u(u/y), uy)^{-1}\,\beta(u,(u/y)y)\,\beta(u/y,y) = \\ &= \beta(u(u/y), uy)^{-1}\,\beta(u,u)\,\beta(u/y,y) \overset{CQ}{=} \\ &= \beta(u(u/y), uy)^{-1}\,\beta(u/y,y) \overset{(2)}{=} 1 \end{aligned}$$

for every $y \in X$.

The claim (1) follows since

$$\beta_u(u,yu) \overset{N}{=} \beta_u(u,yu)\,\beta_u(y,u) \overset{CC}{=} \beta_u(uy,u)\,\beta_u(u,u) \overset{CQ}{=} \beta_u(uy,u) = 1$$

for every $y \in X$ and since R_u is a bijection. □

Proposition 8.10. *Let $\boldsymbol{X}$ be a Latin quandle and $u \in X$. Then the map*

$$f : X \times X \longrightarrow X \times X, \quad (x, y) \mapsto (x \cdot y/u, xu)$$

is a bijection and any u-normalized cocyle is invariant under the action of f, i.e.

$$\beta(f(x,y)) = \beta(x \cdot y/u, xu) = \beta(x,y) \tag{22}$$

for every $x, y \in X$.

Proof. The map f has an inverse, given by

$$f^{-1}(x,y) = (y/u, (y/u)\backslash x \cdot u)$$

for evey $x, y \in X$. Moreover, since $\beta(x,u) = \beta(y,u)$ for every $x, y \in X$, (WCC) implies that

$$\beta(xy, xu) \overset{WCC}{=} \beta(x, yu)$$

for every $x, y \in X$. Setting $yu = z$ we get formula (22). □

Proposition 8.11. *Let $\boldsymbol{X}$ be a finite Latin quandle and $u \in X$. Then the map*

$$\omega : X \times X \longrightarrow X \times X, \quad (x, y) \mapsto (M_y M_u^{-1}(x) \cdot x, y) = (y/(x\backslash u) \cdot x, y)$$

is a bijection and any u-normalized cocycle is invariant under the action of ω, i.e.

$$\beta(\omega(x,y)) = \beta(y/(x\backslash u) \cdot x, y) = \beta(x,y) \tag{23}$$

for every $x, y \in X$.

Proof. Let us denote $x\backslash u = a$, $z\backslash u = b$, $u_x = M_y M_u^{-1}(x)$ and $u_z = M_y M_u^{-1}(z)$. The map $x \mapsto u_x$ is bijective by Proposition 2.3 of [12]. Let $x, z \in X$ such that $u_x x = u_z z$, then

$$\begin{aligned} u_x(xa) &= u_x u \\ u_x(xa) &= u_x x \cdot u_x a = u_x x \cdot y = \\ &= u_z z \cdot y = u_z z \cdot u_z b = \\ &= u_z \cdot zb = u_z u \end{aligned}$$

Therefore $u_x = u_z$, hence $x = z$. The map ω is injective and then bijective.

Let $x, y \in X$, then

$$\begin{aligned} \beta(u/y, y) &\overset{N}{=} \beta(u/y \cdot x, u/y \cdot y)\beta(u/y, y) \overset{CC}{=} \beta(u/y, xy)\beta(x,y) \\ \beta(u/y, y) &\overset{N}{=} \beta(x, u/y \cdot y)\beta(u/y, y) \overset{CC}{=} \beta(x \cdot u/y, xy)\beta(x,y) \end{aligned}$$

Therefore, $\beta(u/y, xy) = \beta(x \cdot u/y, xy)$ for every $x, y \in X$. Setting $u/y = z$ and $xy = v$, we have $x = v/y = v/\left(z\backslash u\right)$. So that

$$\beta\left(z, v\right) = \beta\left(v/\left(z\backslash u\right) \cdot z, v\right)$$

for every $z, v \in X$. □

Notation 8.12. *We will use the following notation*

$$\begin{aligned} \Delta(x,y) &= \{(L_u^n(x), L_u^n(y),\ n \in \mathbb{Z}\} \\ \Delta &= \{\Delta(x,y),\ x, y \in X\} \\ F(x,y) &= \{f^n(x,y),\ n \in \mathbb{Z}\} \end{aligned}$$

$$l(x) = |\{L_0^n(x),\ n \in \mathbb{Z}\}|$$

The element of Δ *will be called diagonals.*

Remark 8.13. *Let* $\boldsymbol{X}$ *be a finite quandle. Then* $\Delta(x,y) \subseteq O_{\langle L_u \rangle}(x) \times O_{\langle L_u \rangle}(y)$ *and* $|\Delta(x,y)| = L.C.M.\{l(x), l(y)\}$ *for every* $(x,y) \in X \times X$.

Moreover if $\boldsymbol{X}$ *is semiregular then* $|\Delta| = \frac{|X|^2-1}{l} + 1$. *where* l *is the order of the left multiplication* L_u.

Several different identities can be derived from the normalization condition together with condition (CC) and (CQ). In the present work we will use just the following one.

Lemma 8.14. *Let* $\boldsymbol{X}$ *be a Latin quandle, and let* β *be a u-normalized cocycled, then*

$$\beta(u/(u/x), x) = \beta(u/x, x)$$

for every $x \in X$. *Moreover* $u/(u/x) \cdot x = u$ *if and only if* $x = u$.

Proof. Setting $x = u/y$ and $y = u/z$ in (CC), we get $\beta(u/(u/z), z) = \beta(u/z, z)$ for every $z \in X$. Moreover

$$u/(u/x) \cdot x = u \ \Leftrightarrow\ u/(u/x) = u/x \ \Leftrightarrow\ u/x = u \ \Leftrightarrow\ x = u$$

□

8.3. **Orbits of the action preserving normalized cocycles.** In the previous Section we have seen that normalized cocycle are invariant under the action of the group $\langle L_u \times L_u, f, \omega \rangle$, where $L_u \times L_u$ denotes the diagonal action of L_u.

In this Section we show that f and ω acts on Δ and we show some features of this action using the properties of the action of f and ω on $X \times X$.

First of all you can see that the point (u,u) is the only fixed point by this action.

Lemma 8.15. *Let* $\boldsymbol{X}$ *be a Latin quandle and let* $x, y \in X$. *Then*

$$f^k(x,y) = (x_k, x_{k-1}u)$$

where

$$x_k = \begin{cases} x_{-1} = y/u \\ (L_x L_{y/u})^{\frac{k}{2}}(x), & \textit{if } k \textit{ is even} \\ (L_x L_{y/u})^{\frac{k+1}{2}}(y/u), & \textit{if } k \textit{ is odd} \end{cases}$$

for every $k \in \mathbb{Z}$.

Proof. Set $x_{-1} = y/u = z$ and $f^k(x,y) = (x_k, y_k)$. By definition,

$$f^{k+1}(x,y) = f(x_k, y_k) = (x_k \cdot y_k/u, x_k u) = (x_{k+1}, y_{k+1})$$

and then $y_{k+1} = x_k u$ and $x_{k+1} = x_k x_{k-1}$ for every $k > 0$. Moreover

$$x_0 = x = (L_x L_z)^0(x)$$
$$x_1 = xz = (L_x L_z)^1(z)$$

Assume by induction that

$$x_k = \begin{cases} (L_x L_{y/u})^{\frac{k}{2}}(x), & \text{if k is even} \\ (L_x L_{y/u})^{\frac{k+1}{2}}(y/u), & \text{if k is odd} \end{cases}$$

for every $k \leq n$. Without loss of generality $n = 2k$ is even. Hence,

$$\begin{aligned} x_{2k+1} &= x_{2k}x_{2k-1} = (L_x L_z)^k(x) \cdot (L_x L_z)^k (z) = \\ &= (L_x L_z)^k(xz) = (L_x L_z)^k L_x L_z (z) = \\ &= (L_x L_z)^{k+1} (z) \end{aligned}$$

In the very same way you can proove that $x_{2k+2} = (L_x L_z)^{k+1}(x)$. □

Let us denote the product map $(x, y) \mapsto xy$ by p. The map f preserves the product.

Lemma 8.16. *Let* $\boldsymbol{X}$ *be a Latin quandle, then*

$$p(x, y) = p(f(x, y))$$

for every $x, y \in X$.

Proof. We have that

$$p(f(x, y)) = p(x \cdot y/u, xu) = x(y/u) \cdot xu = x \cdot (y/u)u = xy = p(x, y)$$

for every $x, y \in X$. □

Remark 8.17. *Note that if* $\boldsymbol{X}$ *is finite, then* $|F(x, y)| \leq |X|$. *Indeed, the product is constant along the orbits of* f *and there at* $|X|$ *pair of elements with a given product.*

By this property follows that the length of the orbits under f are determined just by one of the two components.

Proposition 8.18. *Let* $\boldsymbol{X}$ *be a Latin quandle and* $x, y \in X$. *Then the following are equivalent:*

(1) $f^k(x, y) = (x, y)$;
(2) $x_k = x$;
(3) $x_{k-1} = y/u$.

Therefore, $(x, y) \in Fix(f)$ *if and only if* $y = xu$.

Proof. Clearly (1) implies (2) and (3) and (2) and (3) together imply (1). Hence it is enought to show that (2) and (3) are equivalent.
By Proposition 8.16, we have that

$$xy = x_k \cdot x_{k-1}u$$

for every $k \in \mathbb{N}$. Since $\mathbf{X}$ is a Latin quandle, then $x_k = x$ if and only if $x_{k-1}u = y$. Therefore, (2) and (3) are equivalent. □

The length of the orbit under f of (x, y) depends on the length of the cycle of the map $L_x L_{y/u}$.

Proposition 8.19. *Let* X *be a finite Latin quandle,* $x, y \in X$ *and* $g = L_x L_{y/u}$. *Then*

$$|F(x, y)| = \begin{cases} 2|O_g(x)|, & \textit{if } |F(x, y)| \textit{ is even} \\ |O_g(x)|, & \textit{if } |F(x, y)| \textit{ is odd} \end{cases}$$

Proof. Let assume that $|F(x,y)| = 2r$ for some natural r. Then by Proposition 8.18,

$$x_{2r} = g^r(x) = x$$

and r is the minimum integer which satysfies this equation. Therefore $2r = 2|O_g(x)|$.

Let assume that $|F(x,y)| = 2r+1$ for some natural r. Then

$$\begin{cases} x_{2r+1} = g^{r+1}(y/u) = x \\ x_{2r} = g^r(x) = y/u \end{cases}$$

Therefore $O_g(x) = O_g(y/u)$ and both r and $r+1$ are the minimum naturals satisfying these equations. Therefore, $2r+1 = |F(x,y)| = |O_g(x)|$. □

Corollary 8.20. *Let $\boldsymbol{X}$ be a finite Latin quandle, then $|O_g(x)| = |O_g(y/u)|$.*

Proof. If $|F(x,y)|$ is odd, by Proposition 8.19, $O_g(x) = O_g(y/u)$ and therefore they have the same size.

If $|F(x,y)| = 2r$ for some natural r, then

$$\begin{cases} x_{2r} = g^r(x) = x \\ x_{2r-1} = g^r(y/u) = y/u \end{cases}$$

and r is the minimum natural satisfying these equations, therefore $r = |O_g(x)| = |O_g(y/u)|$. □

Let us show some properties of the map ω.

Lemma 8.21. *Let $\boldsymbol{X}$ be a finite Latin quandle and $x, y \in X$. Then the following are equivalent*

(1) $\omega(x,y) = (x,y)$;
(2) $p(\omega(x,y)) = (x,y)$;
(3) $y = u$.

Proof. Note that $\omega(x,u) = (x,u)$ for every $x \in X$. Therefore, (3) implies (1) and clearly (1) implies (2).

(2) ⇔ (3) Since $\mathbf{X}$ is a Latin quandle, then

$$p(\omega(x,y)) = (y/(x\backslash u))x \cdot y = xy \;\Leftrightarrow\; y/(x\backslash u) = x \;\Leftrightarrow\; y = u$$

□

Actually, the action of the group $G = \langle f, g\rangle$ on $X \times X$ induces an action on the set Δ. We will use the following notation

$$\begin{aligned} \Delta^f &= \{\Delta(x, xu),\ u \neq x \in X\} \\ \Delta_u &= \{\Delta(u/x, x),\ u \neq x \in X\} \end{aligned}$$

Proposition 8.22. *Let $\boldsymbol{X}$ be a Latin quandle and $G = \langle f, \omega\rangle$. Then*

$$g(\Delta(x,y)) = \Delta(g(x,y)) \tag{24}$$

defines a group action of G on Δ.

Proof. It is enough to show that f and ω commutes with $L_u \times L_u$. Let $x, y \in X$, then

$$\begin{aligned} f((L_u \times L_u)(x,y)) &= f(ux, uy) = (ux \cdot (uy)/u, uxu) = \\ &= (ux \cdot u(y/u), uxu) = (u \cdot x(y/u), uxu) = \\ &= (L_u \times L_u)(x(y/u), xu) = (L_u \times L_u)(f(x,y)) \end{aligned}$$

Moreover

$$\begin{aligned} \omega((L_u \times L_u)(x,y)) &= \omega(ux, uy) = \\ &= (L_{R^{-1}_{L^{-1}_{ux}(u)}(uy)}(ux), uy) = (L_{L_u R^{-1}_{L^{-1}_x(u)} L^{-1}_u(uy)}(ux), uy) \\ &= (L_u L_{R^{-1}_{L^{-1}_x(u)}(y)} L_u^{-1}(ux), uy) = (L_u L_{R^{-1}_{L^{-1}_x(u)}(y)}(x), uy) = \\ &= (u\omega_y(x), uy) = (L_u \times L_u)(\omega(x,y)) \end{aligned}$$

Then the action in formula (24) is well defined. ☐

On the other hand, the maps f and ω do not commute.

Proposition 8.23. *Let X be a Latin quandle, then*

$$(f\omega)(x,y) = (\omega f)(x,y)$$

if and only if $x = y = u$.

Proof. Let us denote $\omega(x,y) = (\omega_y(x), y)$ for every $x, y \in X$. Assume that $f\omega(x,y) = \omega f(x,y)$, i.e.

$$\begin{aligned} f\omega(x,y) &= (\omega_y(x) \cdot y/u, \omega_y(x)u) \\ \omega f(x,y) &= (\omega_{xu}(x \cdot y/u) \cdot x(y/u), xu). \end{aligned}$$

By Proposition 8.21, $\omega_y(x) = x$ implies $y = u$. So it follows that $\omega_{xu}(xu) = xu$. Then, by Proposition 8.21, we have $xu = u$ and therefore $x = u$. ☐

Corollary 8.24. *Let X be a Latin quandle then*

1. $\omega(\Delta(u/x, x)) \notin \Delta_u$;
2. $\omega(\Delta(x, xu)) \notin \Delta^f$;
3. $f(\Delta(x, xu)) = \Delta(x, xu)$;
4. $f(\Delta_u) = \Delta_u$;

for every $u \neq x \in X$.

Proof. (1) It follows by Lemma 8.21.
(2) It follows by Proposition 8.23.
(3) If follows since f and the diagonal action of L_u commutes.
(4) If follows by Lemma 8.16 (f preserves the product). ☐

The length of the orbits of the action on f and ω on Δ might be different from the size of the orbits of their action on $X \times X$. This actually coincides under some further assumption on the quandle **X**.

Lemma 8.25. *Let **X** be a Latin semiregular quandle. Then the length of the orbit of (x,y) and $\Delta(x,y)$ under the action of f and ω are the same.*

Proof. Under this assumption, $|\Delta(x,y)| = o(L_u)$. Clearly the size of the orbit of $\Delta(x,y)$ under f (ω) divides the size of the orbits of (x,y) under f (ω).

Assume that $f^k(\Delta(x,y)) = \Delta(x,y)$, then

$$f^k(x,y) = ({L_u}^r(x), {L_u}^r(y))$$

for some $r \in \mathbb{N}$. Therefore, $p(x,y) = xy = {L_u}^r(xy) = p(({L_u}^r(x), {L_u}^r(y))$. Hence, r divides $o(L_u) = |\Delta(x,y)|$, therefore $f^k(x,y) = (x,y)$.

Assume that $\omega^k(\Delta(x,y)) = \Delta(x,y)$, then

$$\omega^k(x,y) = (z,y) = ({L_u}^r(x), {L_u}^r(y))$$

for some $r \in \mathbb{N}$ and some $z \in X$, i.e., $L_u^r(y) = y$. Therefore, $\omega^k(x,y) = (x,y)$. □

Remark 8.26. *Let $O(\Delta(x,y))$ denotes the orbit of $\Delta(x,y)$ under the action of $\langle f, \omega\rangle$. Then if $\Delta = \bigcup_{x\in X} O(\Delta(x,x))$ then $\boldsymbol{X}$ has trivial cohomology. It follows since*

$$\begin{aligned} f(u,y) &= f(u,xu) = (ux,uu) = (ux,u) \\ f^2(u,y) &= (ux\cdot u, ux\cdot u) = (uxu,uxu) \end{aligned}$$

and since $\beta(x,x) = 1$ for every $x \in X$.

9. Some particular cases

9.1. **Cohomology of principal Latin Quandles.** A principal representation allows us to exploit the underlying group structure to understand better the behaviour of the orbits under the action of f and ω.

In the whole Section we make the choice $u = 1 \in G$, the group operation is denoted by juxtaposition.

Proposition 9.1. *Let $\boldsymbol{X} = \mathcal{Q}(G,\alpha)$ be a finite principal Latin quandle, $x,y \in X$. Then*

$$|F(x,y)| = min\{n \in \mathbb{N},\ \textstyle\prod_{k=0}^{n-1} \alpha^k\left(x_{k-1}^{-1}x_k\right) = 1\}$$

where

$$x_k = \begin{cases} x, & \text{if } k \text{ is even} \\ y/1, & \text{otherwise} \end{cases}$$

Let $n = |F(x,y)|$. Then $\alpha^n\left(x_n^{-1}x_{n-1}\right) = x^{-1}z$

Proof. By Proposition 8.18, it is enough to consider just one of the coordinates of f. By Proposition 3.9, we have that

$$x_n = x\textstyle\prod_{k=1}^{n} \alpha^k\left(x_{k-1}^{-1}x_k\right)$$

for every $n \in \mathbb{N}$, where $x_k = x$ if k is even and $x_k = y/1$ if k is odd. Hence $x_n = x$ if and only if

$$\textstyle\prod_{k=1}^{n} \alpha^k\left(x_{k-1}^{-1}x_k\right) = 1 \iff \prod_{k=0}^{n-1} \alpha^k\left(x_{k-1}^{-1}x_k\right) = 1$$

Let $n = |F(x,y)|$. The second claim follows by Proposition 8.18, putting together the equivalent equations

$$\begin{aligned} x_n &= x\textstyle\prod_{k=1}^{n} \alpha^k\left(x_{k-1}^{-1}x_k\right) = x \\ x_{n-1} &= x\textstyle\prod_{k=1}^{n-1} \alpha^k\left(x_{k-1}^{-1}x_k\right) = z. \end{aligned}$$

□

Corollary 9.2. *Let $\boldsymbol{X} = \mathcal{Q}(G,\alpha)$ be a finite principal faithful quandle, $x, y \in X$ and $n = |F(x,y)|$. If n is even, then $l(x^{-1}(y/1))$ divides n. If n is odd then $l(x^{-1}(y/1))$ divides $2n$.*

Proof. Let $z = y/1$. By Proposition 9.1, if $n = |F(x,y)|$ is even, $\alpha^n(x^{-1}z) = x^{-1}z$ and then $l(x^{-1}z)$ divides n. Otherwise, $\alpha^n(z^{-1}x) = x^{-1}z$. Hence, $\alpha^{2n}(x^{-1}z) = \alpha^n(x^{-1}z)^{-1} = x^{-1}z$. Therefore, $l(x^{-1}z)$ divides $2n$. □

For principal quandles ω has a nice form.

Lemma 9.3. *Let $\boldsymbol{X} = \mathcal{Q}(G,\alpha)$ be a finite principal Latin quandle and β a quandle constant cocyle. Then*

$$\omega(x,y) = (yx, y) \tag{25}$$

for every $x, y \in G$.

Proof. Assume that $u = 1$, then

$$\begin{aligned} y/(x\backslash 1)\cdot x &= R_x R^{-1}_{L_x^{-1}(1)}(y) = \lambda_x t \lambda_x^{-1} L_x^{-1} t^{-1} L_x(y) = \\ &= \lambda_x t\alpha^{-1}\lambda_x^{-1} t^{-1}\lambda_x \alpha \lambda_x^{-1}(y) = xt\alpha^{-1}(x^{-1}t^{-1}(x\alpha(x^{-1}(y)))) = \\ &= xt\alpha^{-1}(x^{-1}x)x^{-1}yx = yx \end{aligned}$$

Then ω is a permutation also if $\mathbf{X}$ is infinite. □

Remark 9.4. *Formula (25) states that the orbit of (x,y) under the action of ω is given by*

$$O_{\langle\omega\rangle}(x,y) = \{(y^n x, y),\ n \in \mathbb{Z}\}$$

i.e. the first component is nothing but the geometric progression of ratio y with scale factor x. The length of the orbit under ω of (x,y) is given by the order of y. Moreover,

$$\beta(y^n x, y) = \beta(x,y) \tag{26}$$

for every $x.y \in G$ and $n \in \mathbb{N}$.

Corollary 9.5. *Let $\boldsymbol{X} = \mathcal{Q}(G,\alpha)$ a principal finite Latin quandle and β a constant cocyle. Then*

$$\beta_u(x^n, x) = 1 \tag{27}$$

for every $n \in \mathbb{Z}$, $x \in G$.

Proof. It is enough to set $x = y$ in formula (26). □

Remark 9.6. *Let $\boldsymbol{X} = \mathcal{Q}(G,\alpha)$ be a finite Latin quandle. Assume that the map*

$$g : X \times X \longrightarrow X \times X, \quad x \mapsto x \cdot xu = x\alpha^2(x)^{-1}$$

is bijective. Then f-fixed points belong to different subsets of the partition given by the product map, i.e.

$$X \times X = \bigcup_{c\in X}\{(x,y),\ xy = c\} = \bigcup_{c\in X} P_c$$

This condition is equivalent to have no cycle of length two for α.

Under this assumption $|F(x,y)| \leq |X| - 1$. *If the equality is realized by any pair* $x, y \in X$, *then any subset* P_c *is given by one orbit under* f *of size* $|X| - 1$ *and one trivial orbit. It* $c \neq u$, *then there is an element of the form* $(x,u) \in P_c$.

Therefore $\beta|_{\Delta(x,y)} = 1$ *for every* $\Delta(x,y) \notin \Delta_u \cup \Delta^f$. *By virtue of Proposition 8.24, if either* $\beta|_{\Delta(x,y)} = 1$ *for some* $\Delta(x,y) \in \Delta_u \cup \Delta^f$ *or if* ω *does not decompose* $\Delta_u \cup \Delta^f$, *then* $\beta = \mathbf{1}$.

We will show that this condition is sufficient for having trivial cohomology for any finite principal Latin quandle with size different from 4 *(see Corollary 9.34).*

Definition 9.7. Let $\mathbf{X}$ be a Latin quandle $\mathbf{X}$. If

$$\text{(F)} \qquad |F(x,y)| = |X| - 1, \text{ for every } x, y \in X$$

then we say that $\mathbf{X}$ satisfies condition (F).

Proposition 9.8. *Let* G *be a finite non-Abelian group and let* $\boldsymbol{X} = \mathcal{Q}(G,\alpha)$ *be a Latin quandle. If* $\boldsymbol{X}$ *satisfies condition (F) then* $\boldsymbol{X}$ *has trivial cohomology.*

Proof. Note that

$$\omega(\Delta(x, x \cdot 1)) = \Delta(x\alpha(x^{-1})x, x\alpha(x^{-1})) \in \Delta_u \iff o(x\alpha(x^{-1})) = o(t(x)) = 2$$

Since G is not Abelian and t is surjective, then there exists an element $t(x)$ with order different from 2. Then ω does not decompose $\Delta_u \cup \Delta^f$ and by Remark 9.6, $\mathbf{X}$ has trivial cohomology. □

9.2. **Cohomology of Connected Affine Quandles.** This Section is about non-abelian cohomology of finite affine quandles. By virtue of Proposition 4.15, we can apply all the results about cocycles showed in the previous Sections.

For affine quandles we can compute the length of the orbits of f and this allows us to extend Lemma 5.1 of [17] to all connected affine quandles over *cyclic groups* and to quandles with *doubly transitive left multiplication group.*

Fact 9.9. *Let* A *be an Abelian group,* $\alpha, 1 - \alpha \in Aut(A)$ *and* $x \in A$. *Then*

$$\alpha^n(x) = x \iff \sum_{k=0}^{n-1} \alpha^k(x) = 0$$

Remark 9.10. *Let* $\boldsymbol{X} = \mathcal{Q}(A,\alpha)$ *be a finite connected affine quandle and* $x, y \in X$. *By virtue of Proposition 9.1 we have that*

$$|F(x,y)| = min\{n \in \mathbb{N}, \ \sum_{j=0}^{n-1} (-1)^j \alpha^j (x - y/0) = 0\} \tag{28}$$

$$(-1)^n \alpha^{|F(x,y)|}(x - y/0) = x - y/0. \tag{29}$$

If $|F(x,y)|$ *is even, then* $l(x - y/0)$ *divides* $|F(x,y)|$, *otherwise* $l(x - y/0)$ *divides* $2|F(x,y)|$ *(see Corollary 9.2). Furthermore, by Lemma 9.3,*

$$\omega(x,y) = (y + x, y) \tag{30}$$

$$\beta(ny + x, y) = \beta(x,y) \tag{31}$$

$$\beta(nx, x) = 1 \tag{32}$$

for every $x, y \in A$ *and every* 0*-normalized cocycle.*

In the finite affine case it is possible to compute the length of the orbits of f from the length of the cycle of α and the order of the elements of the underlying group.

Corollary 9.11. *Let $\boldsymbol{X} = \mathcal{Q}(A,\alpha)$ be a finite connected affine quandle and $x, y \in X$. If $o(x-y/0) = 2$ then $|F(x,y)| = l(x-y/0)$.*

Proof. It follows by formula (28, in view of Fact 9.9). □

Lemma 9.12. *Let $\boldsymbol{X} = \mathcal{Q}(A,\alpha)$ be a finite connected affine quandle and $x, y \in A$ such that $l(x-y/0)$ is odd. Then*

$$|F(x,y)| = \begin{cases} l(x-z), & \text{if } o(x-y/0) = 2 \\ 2l(x-y/0), & \text{otherwise} \end{cases}$$

Proof. Let $l = l(x-y/0)$ and $n = |F(x,y)|$.

If n is even, then by Corollary 9.2, $n = rl$ for some even r. Therefore, by formula (28), r is the minimum even natural for which

$$\sum_{j=0}^{rl-1} (-1)^{-1} \alpha^j (x-1/0) = 0 \tag{33}$$

holds. Since l is odd then $r = 2$ satisfies formula (33). Hence $r = 2$ and so $n = 2l$.

If n is odd, then by Corollary 9.2, l divides $2n$ and since l is odd then l divides n. Then, by formula (29), $o(x-y/0) = 2$ and by Corollary 9.11, $n = l$. □

Lemma 9.13. *Let $\boldsymbol{X} = \mathcal{Q}(A,\alpha)$ be a finite connected affine quandle and let $x, y \in X$. Assume that $l = l(x-y/0)$ is even, then*

$$|F(x,y)| = \begin{cases} kl, & \text{if } |F(x,y)| \text{ is even} \\ k'\frac{l}{2}, & \text{otherwise} \end{cases}$$

where $k = o\left(\sum_{k=1}^{l} (-1)^k \alpha^k (x-y/0)\right)$, $k' = o\left(\sum_{k=1}^{\frac{l}{2}} (-1)^k \alpha^k (x-y/0)\right)$.

Proof. Let $l = l(x-y/0)$ and $n = |F(x,y)|$.

If n is even the by formula (28), $n = rl$ for some r. Since l is even, we have that

$$\sum_{k=1}^{rl} (-1)^k \alpha^k (x-y/0) = r \sum_{k=1}^{l} (-1)^k \alpha^k (x-y/0) = 0 \tag{34}$$

and r is the minimum for which equation (34) holds. Then by definition r is the order of $\sum_{k=1}^{l} (-1)^k \alpha^k (x-y/0)$.

Let n be odd, then by formula (28), $n = (2s+1)\frac{l}{2}$ for some s, and $\alpha^{\frac{l}{2}}(x-y/0) = -(x-y/0)$. Hence we get that

$$\sum_{k=1}^{(2s+1)\frac{l}{2}} (-1)^k \alpha^k (x-y/0) = (2s+1) \sum_{k=1}^{\frac{l}{2}} (-1)^k \alpha^k (x-y/0) = 0 \tag{35}$$

and s is the minimum for which equation (35) holds. By definition $2s+1$ is the order of $\sum_{k=1}^{\frac{l}{2}} (-1)^k \alpha^k (x-z)$. □

Remark 9.14. *Note that if $l = l(x-y/0)$ is even and $|F(x,y)|$ is odd, then the order of $\sum_{k=1}^{\frac{l}{2}} (-1)^k \alpha^k (x-z)$ and $\frac{l}{2}$ need to be odd.*

The following Lemma is needed to extend Proposition 9.8 to the affine case.

Lemma 9.15. *Let $X = \mathcal{Q}(A,\alpha)$ be a connected affine quandle.*

1. *$\omega(\Delta(0/x, x)) \in \Delta^f$ if and only if $o(x) = 2$.*
2. *$\Delta(0/(0/x), x) \in \Delta^f$ if and only if $(\alpha^2 + \alpha - 1)(x) = 0$.*

Proof. (1) We have that

$$(0/x+x)\cdot 0=(1-\alpha)(2x-(1-\alpha)^{-1}(x))=x$$

if and only if $2x=0$.

(2) We have that

$$(0/(0/x))\cdot 0=(1-\alpha)\left(x-2(1-\alpha)^{-1}(x)+(1-\alpha)^{-2}(x)\right)=x$$

if and only if $(\alpha^2+\alpha-1)(x)=0$. □

Proposition 9.16. *Let $\boldsymbol{X}=\mathcal{Q}(A,\alpha)$ be a finite connected affine quandle. If $exp(A)\neq 2$ and $\boldsymbol{X}$ satisfies condition (F), then $\boldsymbol{X}$ has trivial cohomology.*

Proof. By Lemma 9.15 (1), it follows that there exists $x\in A$ such that $\omega(\Delta(x,x\backslash u))\notin \Delta_u\cup\Delta^f$. Therefore $\beta|_{\Delta_u}=\mathbf{1}$. □

Proposition 9.17. *Let $\boldsymbol{X}=\mathcal{Q}(\mathbb{Z}_2^n,\alpha)$ be a connected affine quandle. If $o(\alpha)\neq 3$ and $\boldsymbol{X}$ satisfies condition (F), then $\boldsymbol{X}$ has trivial cohomology.*

Proof. By Lemma 9.15 (2), if $o(\alpha)\neq 3$ we have that there exists $x\in X$ such that

$$(\alpha^2+\alpha-1)(x)\overset{exp(A)=2}{=}(\alpha^2+\alpha+1)(x)\neq 0$$

By Proposition 8.14, $(u/(u/x),x)\notin\Delta^f\cup\Delta_u$ and $\beta(u/x,x)=\beta(u/(u/x),x)=1$. Thus, $\beta|_{\Delta_u}=\mathbf{1}$. □

The next Proposition shows which are the finite affine quandles satisfying the condition (F).

Proposition 9.18. *Let $\boldsymbol{X}=\mathcal{Q}(A,\alpha)$ be a finite connected affine quandle.*

(i) *If $|X|$ is even then,*

$$\boldsymbol{X}\text{ satisfies (F)}\iff \boldsymbol{X}=\mathcal{Q}(\mathbb{Z}_2^n,\alpha)\text{ and }o(\alpha)=|X|-1.$$

(ii) *If $|X|$ is odd and $o(\alpha)$ is odd, then*

$$\boldsymbol{X}\text{ satisfies (F)}\iff \boldsymbol{X}=\mathcal{Q}(\mathbb{Z}_p^n,\alpha)\text{ where }p\geq 3\text{ and }o(\alpha)=\frac{|X|-1}{2}\text{ is odd;}$$

(iii) *If $|X|$ is odd and $o(\alpha)$ is even, then*

$$\boldsymbol{X}\text{ satisfies (F)}\implies \boldsymbol{X}=\mathcal{Q}(\mathbb{Z}_p^n,\alpha)\text{ where }p\geq 3\text{and }o(\alpha)=|X|-1.$$

Proof. (i) Assume that condition (F) holds and $o(\alpha)$ be odd. Since there exists $x\in A$, such that $o(x)=2$, then by Proposition 9.10

$$|F(x,0)|=l(x)=|X|-1$$

By Theorem 7.8, $\mathbf{X}\simeq\mathcal{Q}(\mathbb{Z}_2^n,\alpha)$.

If $\mathbf{X}=\mathcal{Q}(\mathbb{Z}_2^n,\alpha)$ and $o(\alpha)=|X|-1$, Lemma 9.12 applies and condition (F) holds.

(ii) Let assume that condition (F) holds and that $o(\alpha)$ is odd. By Lemma 9.12,

$$|F(x,y)|=2l(x-y/0)=|X|-1$$

for every $x,y\in X$. Hence, $l(x)=\frac{|X|-1}{2}=o(\alpha)$ for every $x\in X$ and it need to be odd. Let assume that there are $x,y\in A$ of prime orders p and q. Therefore $o(x+y)=pq$. Since α has just two non-trivial orbits then $p=q$ and $A\simeq\mathbb{Z}_p^n\times\mathbb{Z}_{p^2}^m$ for some prime integer $p \geq 3$ and some naturals n, m. Let $x = x_1 + \ldots + x_n + x_{n+1} + \ldots + x_{n+m} \in A$. Then $o(x) = p$ if and only if $x_{n+i} \in \{0, p\}$ for every $1 \leq i \leq m$. Therefore

$$|\{x \in A,\ o(x) = p\}| = p^n 2^m - 1 = \frac{|X| - 1}{2} = \frac{p^{n+2m} - 1}{2}$$

which implies $p = 1$. Hence if $|X| \geq 1$, then $A \simeq \mathbb{Z}_p^n$.

If $\mathbf{X} = \mathcal{Q}\left(\mathbb{Z}_p^n, \alpha\right)$ for some $p \geq 3$ and $o(\alpha) = \frac{|X|-1}{2}$ is odd, $\mathbf{X}$ satisfies condition (F) by Lemma 9.12.

(iii) Assume that condition (F) holds. By Lemma 9.13,

$$|F(x, y)| = l(x - y/0) o\left(\sum_{j=0}^{l(x-y/0)-1} (-1)^k \alpha (x - y/0)\right) = |X| - 1$$

Then $k = o(\sum_{j=0}^{l(x-y/0)-1} (-1)^k \alpha^k (x - y/0))$ divides $|X|$ and divides $|X| - 1$. Therefore $k = 1$ and $l(x) = |X| - 1$ for every $x \in X$. By Theorem 7.8, $\mathbf{X} = \mathcal{Q}\left(\mathbb{Z}_p^n, \alpha\right)$ for some $p \geq 3$ and $o(\alpha) = |X| - 1$. □

Corollary 9.19. *Let $p > 3$ be a prime integer, $\boldsymbol{X} = \mathcal{Q}(\mathbb{Z}_p^n, \alpha)$ such that $o(\alpha) = \frac{|X|-1}{2}$ is odd. Then $\boldsymbol{X}$ has trivial cohomology.*

Now we are ready to extend Lemma 5.1 of [17] to all the connected affine quandles over cyclic groups. The Lemma is the following.

Proposition 9.20. [17, Lemma 5.1] *$H_c^2(\mathcal{Q}(\mathbb{Z}_p, \alpha), \Gamma) = \{\mathbf{1}\}$ for every Γ.*

This result has a very useful Corollary, which was stated in Proposition 2.10 of [17] just for the case $p = q$. It follows by using the classification of connected quandles of prime size given in [14].

Proposition 9.21. [14, Lemma 3] *Let p be a prime integer and $\boldsymbol{X}$ be a connected quandle of size p. Then $\boldsymbol{X} \simeq \mathcal{Q}(\mathbb{Z}_p, \alpha)$.*

Corollary 9.22. [17, Proposition 2.10] *Let p, q be prime integers. Every connected quandle of order pq is faithful.*

Proof. Let $\mathbf{X}$ be a connected quandle of order pq. Assume that $(\mathbf{X}, L_{\mathbf{X}})$ is a proper covering of $L(\mathbf{X})$, hence $L(\mathbf{X})$ has size p or q. In view of Proposition 9.20, $\mathbf{X}$ would be a trivial covering of $L_{\mathbf{X}}$, which is connected if and only if the blocks are trivial (by Proposition 5.12), contradiction. □

Remark 9.23. *It is a very well known fact that the automorphisms of a cyclic group are given by $Aut(\mathbb{Z}_m) = \{\lambda_n,\ G.C.D.\{n, m\} = 1\}$ where λ_n is the give by the map $k \mapsto nk$. Therefore, $\boldsymbol{X} = \mathcal{Q}(\mathbb{Z}_m, \lambda_n)$ is connected if and only if $G.C.D.\{m, n\} = G.C.D.\{m, 1 - n\} = 1$. Then m has necessarily to be odd.*

In the following $\mathcal{U}(\mathbb{Z}_m)$ will denoted the invertible elements of $\mathbb{Z}_m$ with respect to the ring structure.

Proposition 9.24. *Let $\boldsymbol{X} = \mathcal{Q}(\mathbb{Z}_m, \lambda_n)$ be a connected quandle and β be a 0-normalized cocycle. Then β is a u-normalized for every $u \in \mathcal{U}(\mathbb{Z}_m)$ and therefore*

(1) *$\beta(k, u) = 1$, for every $u \in \mathcal{U}(\mathbb{Z}_m)$ and $k \in \mathbb{Z}_m$.*
(2) *$\beta(u, k) = 1$, for every $u \in \mathcal{U}(\mathbb{Z}_m)$ and $k \in \mathbb{Z}_m$.*

(3) *β is invariant under the diagonal action of L_u for every $u \in \mathcal{U}$.*

Proof. In view of Proposition 8.9, it is enough to prove (1). Since every invertible elements u generates the whole group, by formula (32), we have

$$\beta(k, u) = \beta(nu, u) = 1.$$

for every $u \in \mathcal{U}(\mathbb{Z}_m)$ and every $k \in \mathbb{Z}_m$. Thus β is u-normalized for every $u \in \mathcal{U}(\mathbb{Z}_m)$. □

Lemma 9.25. *Let m be a odd natural number. Then every element $x \in \mathbb{Z}_m$ can be written as $x = u \cdot v$ for some $u, v \in U(\mathbb{Z}_m)$.*

Proof. Since $u+v = u/0{\cdot}0\backslash v = (1-\alpha)^{-1}(u){\cdot}\alpha^{-1}(v)$ and α and $1-\alpha$ are automorphisms, it is enought to prove that $x = u + v$ for some $u, v \in \mathcal{U}(\mathbb{Z}_m)$.

Let $m = \prod_{i=1}^{k} p_i^{a_i}$ and $x = x_1 + \ldots + x_k$ be the canonical decomposition of $x \in \mathbb{Z}_m$. with $x_i \in \mathbb{Z}_{p_i^{a_i}}$.

Any non invertible element of $\mathbb{Z}_{p_i{}^{a_i}}$ can be written as sum of two invertible, since it is nilpotent. Since m is odd, then any invertible elements $u \in \mathbb{Z}_{p_i{}^{a_i}}$ can be written as $u = 2u - u$, which is a sum of invertible elements. In any case, we can write $x_i = u_i + v_i$ with $u_i, v_i \in \mathcal{U}(\mathbb{Z}_{p_i^{a_i}})$. By the Chinese remainder theorem, $u = u_1 + \ldots + u_k$ and $v = v_1 + \ldots + v_k$ belong to $\mathcal{U}(\mathbb{Z}_m)$. Finally, we have that $x = u + v$. □

Theorem 9.26. *Let $\boldsymbol{X} = \mathcal{Q}(\mathbb{Z}_m, \lambda_n)$ be a connected quandle. Then $\boldsymbol{X}$ has trivial cohomology.*

Proof. Let $x \notin \mathcal{U}(\mathbb{Z}_m)$ and β a 0-normalized cocycle. By Proposition 9.25, we have that $x = u \cdot v$ for some invertible elements u, v. By Proposition 9.24, it follows that

$$\beta(x, y) = \beta(u \cdot v, u \cdot y') = \beta(v, y') = 1$$

for every $x, y \in X$. □

Now we show that all doubly transitive quandles but the one of size 4 have trivial cohomology. First we show some results about cohomology of minimal quandles.

Remark 9.27. *Let $\boldsymbol{X} = \mathcal{Q}(A, \alpha)$ be a finite connected affine quandle, then the following are equivalent:*

(1) *$1 + \alpha \in Aut(A)$;*
(2) *$|O_u(x)| \neq 2$ for every $x \in X$;*
(3) *the map $x \mapsto x \cdot (x \cdot 0)$ is bijective.*

Note that if one of the previous condition holds, then $|F(x,y)| \leq |X| - 1$ for every $x, y \in A$. In view of Remark 7.17, minimal quandles satisfies these conditions.

Proposition 9.28. *Let $\boldsymbol{X} = \mathcal{Q}(\mathbb{Z}_p^n, \alpha)$ be a minimal quandle and $n > 1$. Then all non trivial f-orbit have the same length and it divides $|X| - 1$. All the non trivial ω-orbits have size p.*

Proof. By Proposition 8.15, the length of the orbits under the action of f is determined by identities involving binary terms. By Proposition 7.5, non trivial orbits have all the same length. By Remark 9.27, then F divides $|X| - 1$.

The second claims follows since every element has order p. □

Notation 9.29. *The length of the non trivial f-orbits will be denoted by L_f.*

By virtue of the previous results we can compute L_f.

Lemma 9.30. *Let $\boldsymbol{X} = \mathcal{Q}(\mathbb{Z}_p^n, \alpha)$ be minimal quandle for some $n > 1$. Then:*

(i) *If $p = 2$ then $L_f = o(\alpha)$;*

(ii) *if $p \geq 3$ then* $L_f = \begin{cases} o(\alpha), & \text{if it is even} \\ \frac{o(\alpha)}{2}, & \text{otherwise} \end{cases}$

In particular if $\boldsymbol{X}$ is doubly transitive, then:

(i) *if $p = 2$ then $L_f = |X| - 1$, i.e. it satifies (F);*

(ii) *if $p > 2$, then $L_f = |X| - 1$, i.e. it satifies (F), or $L_f = \frac{|X|-1}{2}$.*

Proof. (i) The first statement follows by Lemma 9.12, since $l(x) = o(\alpha)$ for every $x \in X$.

(ii) If $p \geq 3$, then $o(\alpha)$ is even, since it divides $|X| - 1$. By Lemma 9.13, since L_f divides $|X| - 1$, necessarily $L_f = o(\alpha)$ when it is even and $L_f = \frac{o(\alpha)}{2}$ otherwise. □

By Lemma 8.25, we have that for doubly transitive quandles L_f coincides with le length of the orbits of the action of f on Δ. Moreover Δ_0 and Δ^f are one element sets.

Theorem 9.31. *Let $\boldsymbol{X} = \mathcal{Q}\left(\mathbb{Z}_p^n, \alpha\right)$ be a doubly transitive quandle with $p \geq 3$ and $n > 1$. Then $\boldsymbol{X}$ has trivial cohomology.*

Proof. If **X** satisfies condition (F), then **X** has trivial cohomology by Proposition 9.16.

Let us assume $L_f = \frac{|X|-1}{2}$, then the map f decomposes $\Delta \setminus (\Delta_u \cup \Delta^f)$ in two orbits Δ_0 and Δ_1 of size $\frac{|X|-1}{2}$, such that $\Delta(0, x) \in \Delta_0$ for $x \neq 0$.

By Proposition 8.24, it is enought to show that $\omega(\Delta(0, x)) \notin \Delta_0$. Let $x \neq 0$ and assume that it does not hold, i.e. there exists $k < \frac{|X|-1}{2}$ and $r < |X| - 1$ such that

$$\omega(0, x) = (x, x) = f^k(\alpha^r(0), \alpha^r(x)) = f^k(0, \alpha^r(x)). \tag{36}$$

Therefore,

$$p(x, x) = x = p(f^k(0, \alpha^r(x)) = p(0, \alpha^r(x)) = \alpha^{r+1}(x), \tag{37}$$

i.e., $x = \alpha^{r+1}(x)$. So $|X| - 1$ divides $r + 1$ and since $r + 1 < |X|$, then necessarily $r + 1 = |X| - 1$. Hence by equation (36), we get

$$\begin{cases} x = \alpha^{-1}\left(x + \sum_{j=1}^{k} (-1)^{j+1} \alpha^j (1-\alpha)^{-1}(x)\right) \\ x = (1-\alpha)\alpha^{-1}\left(x + \sum_{j=1}^{k-1} (-1)^{j+1} \alpha^j (1-\alpha)^{-1}(x)\right) \end{cases} \tag{38}$$

Taking the difference between the two equations of (38), we have

$$x = (-1)^k \alpha^{k-2}(x). \tag{39}$$

If k is even, then $|X| - 1 \leq k - 2 < \frac{|X|-1}{2}$, contradiction. If k is odd, then $\frac{|X|-1}{2} \leq k - 2 < \frac{|X|-1}{2}$, contradiction. □

Theorem 9.32. *Let $\boldsymbol{X} = \mathcal{Q}(\mathbb{Z}_2^n, \alpha)$ be a doubly transitive quandle with $n \neq 2$. Then $\boldsymbol{X}$ has trivial cohomology.*

Proof. It follows from Proposition 9.17, since $o(\alpha) = 3$ if and only if $n = 2$. □

Proposition 9.33. *Let* $\boldsymbol{X}$ *be a connected quandle of size* 4. *Then* $H^2_c(\boldsymbol{X}, S) = \{[\beta_\sigma], \quad \sigma^2 = 1\}$ *where*

$$\beta_\sigma = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & \sigma & \sigma \\ 1 & \sigma & 1 & \sigma \\ 1 & \sigma & \sigma & 1 \end{bmatrix} \tag{40}$$

and $\beta_\sigma \sim \beta_\tau$ *if and only if* σ *and* τ *are conjugated.*

Proof. It is a very well known fact that there is only one isomorphism class of connected quandles of order 4. One of its representative is given by $\mathbf{X} = \mathcal{Q}(\mathbb{Z}_2^2, \alpha)$ where $o(\alpha) = 3$. Every non trivial cocycle $\beta \in Z^2_c(\mathbf{X}, S)$ is equivalent to a 0-normalized cocycle of the form (40) where $\sigma^2 = 1$. By Proposition 8.7, β_σ and β_τ are equivalent if and only σ and τ are conjugated. □

The following Corollary puts together Proposition 9.8 and Theorems 9.32, 9.31 and Corollary 9.19.

Corollary 9.34. *Let* $\boldsymbol{X}$ *be a finite principal Latin quandle and* $|X| \neq 4$. *If* $\boldsymbol{X}$ *satisfies condition (F) then it has trivial cohomology.*

10. A categorical approach to Coverings

10.1. **Coverings and the Adjoint group of a quandle.** In this Section we want to show an alternative approach to quandle coverings. It basically summarizes the contents of the paper of Eisermann [13], whose approach is categorical and relies on the properties of the *Adjoint group* of a quandle (which was also introduced in Section 2.2 of [18]). We just point out that for finite quandles it is enough to consider an appropriate finite quotient of the Adjoint group (already defined in [18]).

There is a straightforward way to define a functor from the category of groups to the category of quandles. It was actually implicitely introduced in Example 3.2 (ii).

Proposition 10.1. [13, Example 2.2] *Conj* : **Grps** ⟶ **Qnd** *is a functor.*

This functor has a right adjoint, given by the following definition.

Definition 10.2. [13, Definition 2.18] The *Adjoint group* of a quandle $\mathbf{X}$ is a pair $(Adj(\mathbf{X}), adj)$ where $Adj(\mathbf{X})$ is a group and $adj : \mathbf{X} \longrightarrow Adj(\mathbf{X})$ is a mapping, such that for every quandle morphism

$$\phi : \mathbf{X} \longrightarrow Conj\,(G)$$

there exists a unique group morphism $\widehat{\phi}$ making the following diagram to commute

$$\begin{array}{ccc} \mathbf{X} & \xrightarrow{\;adj\;} & Adj(\mathbf{X}) \\ & \searrow^{\phi} & \downarrow{\scriptstyle \widehat{\phi}} \\ & & Conj(G) \end{array} \tag{41}$$

Clearly the adjoint group of a quandle is unique up to isomorphism. The following Proposition proves the existence.

Proposition 10.3. [13, Definition 2.18], [13, Remark 2.21] *Let $\boldsymbol{X}$ be a quandle and*

$$R = \left\{x \cdot y = xyx^{-1},\ x, y \in X\right\}$$

Then $(\langle X \mid R\rangle, \pi_R \circ i)$ is the Adjoint group of the quandle $\boldsymbol{X}$.

Moreover, $Adj : \mathbf{Qnd} \longrightarrow \mathbf{Grps}$ is a functor and $(Adj, Conj)$ is an adjunction.

The structure of $Adj(\mathbf{X})$ can be computed and it is given by the following Proposition.

Proposition 10.4. [13, Remark 2.35] *Let $\boldsymbol{X}$ be a quandle and $x \in X$.*

(i) *There exists a unique group morphism*

$$\epsilon : Adj(\boldsymbol{X}) \longrightarrow \mathbb{Z}$$

such that $\epsilon(adj(y)) = 1$ for every $y \in X$.

(ii) *$Adj(\boldsymbol{X}) = Adj(\boldsymbol{X})^0 \rtimes \langle adj(x)\rangle$, where $Adj(\boldsymbol{X})^0 = ker(\epsilon)$.*

(iii) *If $\boldsymbol{X}$ is connected then $Adj(\boldsymbol{X})^0 = Adj(\boldsymbol{X})^{(1)}$.*

Remark 10.5. *By the universal property of $Adj(\boldsymbol{X})$, there exists a unique group morphism*

$$\widehat{L_{\boldsymbol{X}}} : Adj(\boldsymbol{X}) \longrightarrow LMlt(\boldsymbol{X})$$

such that $\widehat{L_{\boldsymbol{X}}}(adj(x)) = L_x$. So the adjoint group acts on $\boldsymbol{X}$ by automorphisms.

The properties of $Dis(\boldsymbol{X})$ reflect the properties of $Adj(\boldsymbol{X})^0$ (see 3.15), since $Dis(\boldsymbol{X}) = \widehat{L_{\boldsymbol{X}}}(Adj(\boldsymbol{X})^0)$.

Coverings and central extensions of groups are related. Actually, the core of this relationship is given by the following Lemma.

Lemma 10.6. [13, Corollary 2.41] *Let $\boldsymbol{X}$ be a quandle. Then*

$$1 \longrightarrow ker(\widehat{L_{\boldsymbol{X}}}) \longrightarrow Adj(\boldsymbol{X}) \xrightarrow{\widehat{L_{\boldsymbol{X}}}} LMlt(\boldsymbol{X}) \longrightarrow 1$$

is a central extension of groups.

In his paper Eisermann characterized all the (pointed) connected coverings of a (pointed) connected quandle introducing the category of pointed coverings of a quandles and by using the properties of the adjoint group. The statement of the main theorem is the following.

Theorem 10.7. [13, Theorem 5.22] *Let $\boldsymbol{X}$ be a connected quandle and $x \in X$. Then there exists a natural equivalence between the category of pointed connected coverings of $\boldsymbol{X}$ and the category of subgroups of $Adj(\boldsymbol{X})^0_x$.*

Therefore, there is a corrispondence between connected coverings and subgroup of $Adj(\mathbf{X})^0_x$.

The adjoint group is infinite in general, but for connected finite quandles the same informations about coverings are given by a finite group.

Definition 10.8. [18] Let $\mathbf{X}$ be a quandle, then the group $Adj_F(\mathbf{X}) = \langle X \mid R' \rangle$, where $R' = \{xyx^{-1} = x \cdot y,\ x^{o(L_x)} = 1,\ x, y \in X\}$ is called the *finite adjoint group* of $\mathbf{X}$.

Proposition 10.9. [18, Lemma 2.19] *Let $\boldsymbol{X}$ be a finite connected quandle and $n = o(L_x)$. Then*

$$Adj_F(\boldsymbol{X}) \simeq Adj(\boldsymbol{X})/\langle adj(x)^n \rangle = Adj(\boldsymbol{X})^0 \rtimes \mathbb{Z}_n$$

and $Adj_F(\boldsymbol{X})$ is finite.

Remark 10.10. *By Proposition 10.9, both $Adj(\boldsymbol{X})^0$ and $Adj(\boldsymbol{X})^0_x$ are finite groups. Since $adj(x)^{o(L_x)} \in ker(\widehat{L_{\boldsymbol{X}}})$ for every $x \in X$, then there exists ϕ such that the following diagram is commutative*

$$\begin{array}{ccc} Adj(\boldsymbol{X}) & \xrightarrow{\widehat{L_{\boldsymbol{X}}}} & LMlt(\boldsymbol{X}) \\ \big\downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle \phi} & \\ Adj_F(\boldsymbol{X}) & & \end{array}$$

Therefore, the actions of $Adj(\boldsymbol{X})$ and $Adj_F(\boldsymbol{X})$ on $\boldsymbol{X}$ are the same. Since $Adj(\boldsymbol{X})^0 \cap \langle adj(x) \rangle = \{1\}$, it is enough to deal with the finite Adjoint group in order to study connected coverings.

The finiteness of $Adj_F(\mathbf{X})$ and the existence of the universal covering ([13, Definition 5.1]) lead to the following Proposition.

Proposition 10.11. *All connected coverings of a finite connected quandle are finite and there are finitely many of them.*

Proof. By theorem 10.7, $Adj(\mathbf{X})^0$ is a finite group and therefore $Adj(\mathbf{X})^0_x$ has a finite number of subgroups. The size of every connected covering is finite since by Theorem 5.3 of [13], the cardinality of the universal covering is finite and any connected coverings is a quotient of it. □

10.2. **Simply connected quandles.** A natural problem about quandle coverings is to characterize connected quandles with just trivial coverings i.e. coverings given by the trivial cocycle. Eisermann gives a characterization of them and we use his result to identify this class of quandles as a subclass of principal connected quandles in the finite case. This original result is given by Theorem 10.17.

Definition 10.12. [13, Definition 5.14] A connected quandle $\mathbf{X}$ is called *simply connected* if $Adj(\mathbf{X})^0_x = \{1\}$ for every $x \in X$.

Simply connected quandles have been characterized by Eisermann as follows. The following Proposition gives a statement equivalent to Proposition 5.15 of [13].

Proposition 10.13. *Let $\boldsymbol{X}$ be a connected quandle. Then the following are equivalent*

(1) *$\boldsymbol{X}$ is simply connected;*
(2) *$H^2_c(\boldsymbol{X}, \mathrm{Sym}(S)) = \{\mathbf{1}\}$ for every S.*

This criterion can be stated in terms of properties of $\mathbf{X}$ and $Dis(\mathbf{X})$. First note that a simply connected quandle has to be principal.

Proposition 10.14. *Let $\boldsymbol{X}$ be a simply connected quandle. Then $\boldsymbol{X}$ is principal.*

Proof. By Proposition 5.25, $\mathbf{Y} = \mathcal{Q}(Dis(\mathbf{X}), \widehat{L_x}) \simeq \mathbf{X} \times_{\mathbf{1}} Dis(\mathbf{X})_x$ and it is connected by Remark 3.22. Therefore, since $O_{LMlt(\mathbf{Y})}(x,s) = \mathbf{X} \times \{s\}$, then $Dis(\mathbf{X})_x = \{1\}$. Hence, $\mathbf{X}$ is principal. □

Remark 10.15. *The converse is not true. Let $\boldsymbol{X}$ be a connected non faithful quandle $\boldsymbol{X}$ of order p^3 for some prime p. Then $L(\boldsymbol{X})$ has cardinality p or p^2, which are affine in both cases. Then $(\boldsymbol{X}, L_{\boldsymbol{X}})$ is a covering of an affine quandle.*

Lemma 10.16. *A connected quandle $\boldsymbol{X}$ is principal if and only if*

$$1 \longrightarrow Adj(\boldsymbol{X})^0_x \longrightarrow Adj(\boldsymbol{X})^0 \xrightarrow{\widehat{L_{\boldsymbol{X}}}} Dis(\boldsymbol{X}) \longrightarrow 1 \tag{42}$$

is a central extension of groups for every $x \in X$.

Proof. By Corollary 10.6, it is enough to prove that $Adj(\mathbf{X})^0_x = ker(\widehat{L_{\mathbf{X}}}) \cap Adj(\mathbf{X})^0$ if and only if $\mathbf{X}$ is principal. Moreover, $ker(\widehat{L_{\mathbf{X}}}) \cap Adj(\mathbf{X})^0 \leq Adj(\mathbf{X})^0_x$ holds for any quandle.

A connected quandle is principal if and only if $Dis(\mathbf{X})_x$ is trivial (Proposition 4.2). Since $\widehat{L}(Adj(\mathbf{X})^0_x) = Dis(\mathbf{X})_x$, then necessarily $Adj(\mathbf{X})^0_x \leq ker(\widehat{L_{\mathbf{X}}}) \cap Adj(\mathbf{X})^0$, i.e. $ker(\widehat{L_{\mathbf{X}}}) \cap Adj(\mathbf{X})^0 = Adj(\mathbf{X})^0_x$.

Therefore $\mathbf{X}$ is principal if and only if the extension given by (42) is a central group extension. □

By virtue of Lemma 10.16, finite simply connected quandles can be characterized in the following way.

Theorem 10.17. *Let $\boldsymbol{X}$ be a finite connected quandle $\boldsymbol{X}$. Then the following are equivalent*

(1) *$\boldsymbol{X}$ is simply connected;*
(2) *$\boldsymbol{X}$ is principal and $Dis(\boldsymbol{X}) \simeq Adj(\boldsymbol{X})^0$.*

Proof. (1) ⇒ (2) By Proposition 10.14 any simply connected quandle is principal. By Lemma 10.16, if a principal quandle $\mathbf{X}$ is simply connected then $Dis(\mathbf{X}) \simeq Adj(\mathbf{X})^0$.

(2) ⇒ (1) Let $\mathbf{X}$ be a finite principal connected quandle and $Dis(\mathbf{X}) \simeq Adj(\mathbf{X})^0$. Then $Adj(\mathbf{X})^0 = \{1\}$, by Lemma 10.16. □

Remark 10.18. *The previous Corollary is equivalent to claim that finite simply connected quandles are the principal quandles such that $LMlt(\boldsymbol{X}) \simeq Adj_F(\boldsymbol{X})$.*

For affine quandles there exists an explicit computation for the Adjoint group, given by Clawens in [11].

Theorem 10.19. [11, Theorem 1] *Let $\boldsymbol{X} = \mathcal{Q}(A, \alpha)$ be a connected affine quandle and let*

$$\tau : A \otimes A \longrightarrow A \otimes A, \quad x \otimes y \mapsto \alpha(y) \otimes x$$

Then $Adj(\boldsymbol{X}) \simeq (\mathbb{Z} \times A \times Coker(1 - \tau), \cdot)$, where

$$(n, x, y) \cdot (m, x'y') = (n + m, x + \alpha^n(x'), y + y' + x \otimes \alpha^n(x'))$$

for every $a, a' \in \mathbb{Z}$, $x, x' \in A$ *and* $y, y' \in A \otimes A$.

Since $Adj(\mathbf{X})^0_x \simeq Coker(1-\tau)$, Theorem 10.19 allows us to restate Proposition 10.13 in the following way.

Corollary 10.20. *Let* $\boldsymbol{X} = \mathcal{Q}(A,\alpha)$ *be a connected affine quandle. Then the following are equivalent*

(1) $\boldsymbol{X}$ *is simply connected;*
(2) $A \otimes A = \langle x \otimes y - \alpha(y) \otimes y, x, y \in A\rangle$.

10.3. **Coverings and central extensions of groups.** Coverings and *central extensions of groups* are closely related. Their relationship has been studied in [13]. In this Section we just collect some of the results in order to complete the picture of the approach of Eisermann to coverings.

Corollary 10.24 is the unique new contribution. Proposition 10.25 is new and it is due to Prof. Stanovsky (unpublished) and we present an alternative proof of it which is due to Dr. Giuliano Bianco.

Next Proposition shows the connection between coverings and central extensions of groups.

Proposition 10.21. [13, Proposition 2.49] *Let* $(\boldsymbol{X}, \pi_\alpha)$ *be a covering of* $\boldsymbol{X}/\alpha$, *then*

$$1 \longrightarrow ker(\pi_\alpha^*) \longrightarrow LMlt(\boldsymbol{X}) \longrightarrow LMlt(\boldsymbol{X}/\alpha) \longrightarrow 1 \tag{43}$$

$$1 \longrightarrow Dis^\alpha(\boldsymbol{X}) \longrightarrow Dis(\boldsymbol{X}) \longrightarrow Dis(\boldsymbol{X}/\alpha) \longrightarrow 1$$

are central extension of groups.

Remark 10.22. *The converse is not true. For any quotient* $\boldsymbol{X}/\alpha$ *of a connected affine quandle* $\boldsymbol{X}$ *the extension written in (43) is central, but the quotient map is not a covering, since both* $\boldsymbol{X}$ *and* $\boldsymbol{X}/\alpha$ *are Latin.*

Some examples of coverings come from the class of conjugation quandles.

Proposition 10.23. [13, Example 1.5] *Let* G *and* H *be groups,* $f : G \longrightarrow H$ *a surjective morphism of groups and* $X \subseteq G$ *be a union of conjugacy classes. Then the following are equivalent:*

(1) $(Conj(X), f|_X)$ *is a covering of* $Conj(f(X))$;
(2) *the short exact sequence*

$$1 \longrightarrow ker(f|_{\langle X\rangle}) \longrightarrow \langle X\rangle \longrightarrow f(\langle X\rangle) \longrightarrow 1 \tag{44}$$

is a central extension.

The functor L preserves coverings.

Corollary 10.24. *Let* $(\boldsymbol{X}, \pi_\alpha)$ *be a covering of* $\boldsymbol{X}/\alpha$. *Then* $(L(\boldsymbol{X}), L(\pi_\alpha))$ *is a covering of* $L(\boldsymbol{X}/\alpha)$.

Proof. The set $L(\mathbf{X})$ is union of conjugacy classes generating $LMlt(\mathbf{X})$ and

$$1 \longrightarrow ker(\pi_\alpha^*) \longrightarrow LMlt(\mathbf{X}) \longrightarrow LMlt(\mathbf{X}/\alpha) \longrightarrow 1$$

is a central extension of groups by Proposition 10.21. Note that $\pi_\alpha^*|_{L(\mathbf{X})} = L(\pi_\alpha)$. By Proposition 10.23, $(L(\mathbf{X}), L(\pi_\alpha^*))$ is a covering of $L(\mathbf{X}/\alpha)$. □

The order of the left multiplications is preserved by coverings.

Proposition 10.25. *Let* $(\boldsymbol{X}, \pi_\alpha)$ *be a covering of a connected quandle* $\boldsymbol{X}/\alpha$ *and* $n = o(L_{[x]})$ *for every* $[x] \in \boldsymbol{X}/\alpha$. *Then* $o(L_x) = n$ *for every* $x \in \boldsymbol{X}$.

Proof. Since π_α^* is surjective then n divides $o(L_x)$ for every $x \in \mathbf{X}$. Moreover $L_x^n \in ker(\pi_\alpha^*)$ and then it is central.

Let $y, z \in \mathbf{X}$. Since $\mathbf{X}/\alpha$ is connected, by Proposition 2.11 there exists $h \in LMlt(\mathbf{X})$ such that $[h(y)] = \pi_\alpha^*(h)([y]) = [z]$.

Then h maps isomorphically the block $[y]$ to $[h(y)]$ for every $y \in \mathbf{X}$. Let $w \in \mathbf{X}$ such that $[w] = [y]$ and $h(w) = z$. Since $L_w = L_y$, then

$$L_y^n(z) = L_y^n h(w) = hL_y^n(w) = hL_w^n(w) = h(w) = z.$$

Therefore, $o(L_y)$ divides n. □

Remark 10.26. *The property of preserving the order of left multiplications does not characterize coverings. It is enough to consider faithful connected non simple quandles such that* $o(L_x)$ *is prime (for instance connected involutory affine quandles) to get an extension which preserves the order of the left multiplications but which is not a covering.*

This order-preserving property can be stated in terms of identities satisfied by cocycles.

Corollary 10.27. *Let* $\boldsymbol{X}$ *be a connected quandle,* $\beta \in Z_c^2(\boldsymbol{X}, \mathrm{Sym}(S))$ *and* $n = o(L_x)$ *for every* $x \in \boldsymbol{X}$. *Then*

$$\prod_{k=0}^{n-1} \beta\left(x, L_x^k(y)\right) = 1$$

for every $x, y \in \boldsymbol{X}$.

11. Future directions

11.1. **Questions and open problems.** In this final Section we give a list of open problems and questions which arose from the the results of the thesis. Some of them were already written in the previous Sections.

The condition $\mathbf{P}\text{-}\mathbf{LQ}_2 \notin \mathcal{S}(\mathbf{X})$ has a nice interpretation in the variety of quandles (Proposition 3.33). We wonder it this is true in the framework of universal algebra.

Question. *Does the condition* $\boldsymbol{P}_2 \notin \mathcal{S}(\boldsymbol{X})$ *have some characterization in universal algebra?*

Since we prove that Taylor quandles have a nice characterization and that they behave nicely with respect to solvability and nilpotency one possible future direction of research is to attemp a classification of finite Taylor quandles (up to some size).

Problem. *Classify all the finite Taylor quandles (up to some size).*

We can not prove that Maltsev quandles are a proper class of Taylor quandles, then we formulate it as an open problem.

Problem. *Find a characterization of the class of Maltsev quandles.*
Does it coincide with the class of Taylor quandles?

We prove that the class of principal Latin quandles is a variety (Theorem 4.8), therefore it is an equational class.

Problem. *Find an equational axiomatization for the variety of principal Latin quandles.*

In the variety of latin quandles the class of quandles with doubly transitive automorphism group has not been characterized.

Problem. *Find a characterization of the class of finite Latin quandles with doubly transitive automorphism group.*

In order to exploit the Galois correspondence between the congruence lattice of a quandle and the lattice of normal subgroups of left multiplication group, it will be useful to solve the following problem.

Problem. *Let $\boldsymbol{X}$ a quandle and α be its congruence. Find some suitable condition under which $Dis_\alpha(\boldsymbol{X}) = Dis^\alpha(\boldsymbol{X})$.*

The combinatorial approach to the computation of cohomology for Latin quandles can be used to further extend Corollary 9.34.

Problem. *Use the combinatorial approach to cohomology to find some other families of Latin quandles with trivial cohomology.*

Give a characterization of Latin quandles with trivial cohomology. Note that this class is a subclass of the variety of principal Latin quandles by virtue of Theorem 10.17.

Question. *Is there any combinatorial characterization of this class in terms of the properties of the action of f and ω?*

Are there any sufficient conditions for a principal Latin quandle for having trivial cohomology other than condition (F)?

11.2. **Connected Quandles of size pq.** The characterization of connected quandles of size pq where p and q are distinct primes is an open problem. The characterization of connected quandle of size p and p^2 is given respectively is given in [14] and [17] through a characterization of their transvection groups. We claim that a similar result can be obtained through the theory developed in Section 6 for non-simple ones (note that for simple quandles this theory does not help) in the pq case.

Problem. *Find a characterization of the transvection group of a non-simple connected quandle of size pq.*

The starting point is the description of the congruence lattices of such quandles.

Proposition 11.1. *Let p, q be prime integers and $\boldsymbol{X}$ be a connected quandle of size pq. Then $Con(\boldsymbol{X})$ is one of them showed in figure 1.*

Proof. Note that, since the blocks of a congruence have all the same size, every factor of $\mathbf{X}$ has prime size and then it is simple. Hence, $\alpha \wedge \beta = 0_{\mathbf{X}}$ and $\alpha \vee \beta = 1_{\mathbf{X}}$ for any pair of proper congruences. Otherwise, the factor $\mathbf{X}/\alpha$ and $\mathbf{X}/(\alpha \vee \beta)$ would not be simple.

(A) Clearly if $\mathbf{X}$ is simple, then $Con(\mathbf{X})$ is the two element lattice.

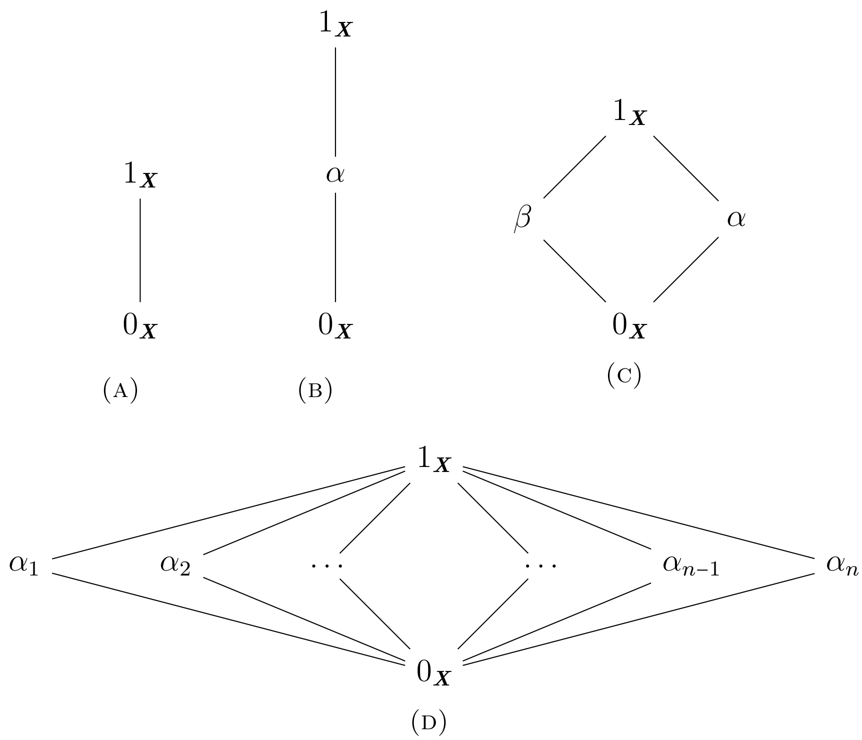


FIGURE 1. (A) Simple - (B) Subdirectly Irreducible - (C) Subdirectly reducible, $p < q$ - (D) Subdirectly reducible $p = q$

(B) Let $\mathbf{X}$ be a subdirectly irredubicle quandle and let μ be its monolith. Let $\mu \neq \beta \in Con(\mathbf{X})$. Hence, $\mu \vee \beta = \beta = 1_{\mathbf{X}}$. Therefore $Con(\mathbf{X})$ is as in (B) of figure 1.

(C) Let $\mathbf{X}$ be not subdirectly irreducible and let α and β be congruences and assume that $\mathbf{X}/\alpha$ and $\mathbf{X}/\beta$ have both size p. Then $\mathbf{X}/\alpha \simeq \mathcal{Q}(\mathbb{Z}_p, \phi)$ and $\mathbf{X}/\beta \simeq \mathcal{Q}(\mathbb{Z}_p, \psi)$. Since $\alpha \wedge \beta = 0_{\mathbf{X}}$, then we have the following subdirect embedding:

$$\mathbf{X} \longrightarrow \mathbf{X}/\alpha \times \mathbf{X}/\beta \simeq \mathcal{Q}(\mathbb{Z}_p \times \mathbb{Z}_p, \phi \times \psi)$$

By Corollary 4.7, the size of $\mathbf{X}$ divides p^2, contradiction. Therefore, $Con(\mathbf{X})$ is as in (C) of figure 1, and the size of $\mathbf{X}/\alpha$ is p and the size of $\mathbf{X}/\beta$ is q.

(D) If $p = q$, $Con(\mathbf{X})$ is as in (D) of figure 1, since $\alpha \wedge \beta = 0_{\mathbf{X}}$ and $\alpha \vee \beta = 1_{\mathbf{X}}$ for any pair of proper congruences. □

Remark 11.2. *It is easy to see that a connected quandle of size pq with $p \neq q$ is affine if and only if it is subdirectly reducible. Therefore the problem reduces to the subdirectly irreducible case.*

11.3. **Galkin quandles.** *Galkin* quandles are a family of Latin quandles of size $3p$ where p is a prime integer. They were defined by Galkin in [16] and his construction was generalized and studied in [7] and [8] in relation to pointed Abelian groups.

Definition 11.3. Let p be a prime integer, $c \in \mathbb{Z}_p$ and $\mu, \tau : \mathbb{Z}_3 \longrightarrow \mathbb{Z}$, defined by

$$\mu(x) = \begin{cases} 2, & \text{if } x = 0 \\ -1, & \text{if } x \neq 0 \end{cases} \qquad \tau(x) = \begin{cases} 1, & \text{if } x = 2 \\ 0, & \text{if } x \neq 2 \end{cases}$$

Then $\mathbf{X} = (\mathbb{Z}_3 \times \mathbb{Z}_p, \cdot)$ where

$$(x,a)\cdot(y,b) = (-x-y, -b+\mu(x-y)a+\tau(x-y)c)$$

is called *Galkin quandle.*

It is easy to see that any Galkin quandle is Latin and that it is an abelian extension of the unique connected quandle of order 3. In Proposition 5.7 of [7] it has been proven that a Galkin quandle is affine if and only if $p = 3$. Therefore we can formulate the following questions by virtue of Remark 11.2.

Question. *Let $p > 3$ be a prime integer.*

(i) *Is any Latin SI connected quandle of order $3p$ a Galkin quandle?*
(ii) *Is any connected SI quandle of order $3p$ Latin?*

On the RIG database the answer to this question is positive and moreover we can formulate the following conjecture about the transvection group of such quandles.

Conjecture 11.4. *Let $\boldsymbol{X}$ be a connected SI quandle of order $3p$. Then*

$$Dis(\boldsymbol{X}) \simeq \mathbb{Z}_p^2 \rtimes \mathbb{Z}_3$$

Moreover we can extend the same Conjecture to the general case of quandle of size pq.

Conjecture 11.5. *Let $\boldsymbol{X}$ be a connected SI quandle of order pq with $p < q$. Then*

$$Dis(\boldsymbol{X}) \simeq \mathbb{Z}_q^2 \rtimes \mathbb{Z}_p$$

References

[1] Andruskiewitsch N., Graña M., *From racks to pointed Hopf algebras*, Advances in Mathematics 178 (2), 177–243 (2003).

[2] Barto L., Kozik M., Stanovskỳ D., *Maltsev Conditions, lack of absorption, and solvability*, Algebra Universalis 74/1-2 (2015), 185–206.

[3] Bergman C., *Universal algebra: foundamentals and selected topics*, CRC Press (2011)

[4] Bianco G., *On the Transvection Group of a Rack*, PhD thesis (2015).

[5] Burris S., Sankappanavar H.P., *A course in universal algebra*, Springer-Verlag (1981).

[6] Carter J. S., Elhamdadi M., Graña M., Saito M., *Cocycle knot invariants from quandle modules and generalized quandle homology*, Osaka J. Math. 42 (2005), no. 3, 499–541.

[7] Clark W.E., Elhamdadi M., Hou X., Saito M., Yeatman T. *Galkin quandles associated with pointed Abelian groups*, Pacific Journal of Mathematics Vol. 264, No. 1, (2013).

[8] Clark W.E., Hou X., *Galkin quandles, pointed abelian groups, and sequence A000712*, Electronic Journal of Combinatorics, 20 (1), No. P45 (2013).

[9] Clark W.E., Saito M., *Algebraic properties of quandle extensions and values of cocycle knot invariants*, J. Knot Theory Ramifications 25, 1650080 (2016).

[10] Clark W.E., Saito M., Vendramin L., *Quandle coloring and cocycle invariants of composite knots and Abelian extensions*, J. Knot Theory Ramifications 25 (2016), no. 5, 1650024, 34 pp.

[11] Clawens F.J.-B.J., *The Adjoint Group of an Alexander Quandle*, arXiv:1011.1587v1 [math.GR].

[12] Deriyenko I., *On middle translations of nite quasigroups*, Quasigroups and Related Systems 16 (2008), 17–24.

[13] Eisermann M., *Quandle coverings and their Galois correspondence*, Fundamenta Mathematicae 225 (2014), no. 1, 103–168.

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

[15] Freese R., McKenzie R., *Commutator Theory for Congruence Modular Varieties*, London Mathematical Society Lecture Notes, vol. 125, Cambridge University Press, Cambridge, New York and Mel- bourne, 1987, 227 pp.

[16] Galkin, V. M., *Left distributive finite order quasigroups*, (Russian) Quasigroups and loops. Mat. Issled. No. 51 (1979), 43–54, 163.

[17] Graña M., *Indecomposable racks of order p^2*, Beitrõge zur Algebra und Geometrie. Contributions to Algebra and Geometry 45 (2004), no. 2, 665–676.

[18] Heckenberger I., Lochmann A.,Vendramin L., *Nichols algebras of group type with many quadratic relations*, Adv. Math. 227 (2011), no. 5, 1956–1989.

[19] Hobby D., McKenzie R., *The structure of finite algebras*, Contemporary Mathematics Vol. 76. American Mathematical Society, Providence (1988)

[20] Hulpke A., Stanovskỳ D., Vojtěchovský P., *Connected quandles and transitive groups*, Journal of Pure and Applied Algebra 220 (2016), no. 2, 735–758.

[21] Jedlicka, P., Pilitowska A., Stanovsky D., Zamojska-Dzienio A., *Structure of Medial Quandles*, Journal of Algebra 443 (2015), 300–334.

[22] Joyce D., *A Classifying invatiant of knots, the knot quandle*, Journal of Pure and Applied Algebra 23 (1982) 37–65, North-Holland Publishing Company.

[23] Joyce, D., *Simple quandles*, J. Algebra 79 (1982), no. 2, 307–318.

[24] Maltsev A.I., *On the general theory of algebraic systems*, Mat. Sb. (N.S.), 35(77):1 (1954), 3–20.

[25] McCarron J., *Small homogeneous quandles*, Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation, ISSAC 12, pages 257–264, New York, NY, USA, (2012).

[26] Taylor W., *Variety Obeying Homotopic Laws*, Canad. J. Math. 29 (1977), 498-527.

[27] Stanovskỳ D., *A guide to self-distributive quasigroups or Latin quandles*, Quasigroups and Related Systems 23, 91–128 (2015).

[28] Stanovskỳ D., Vojtěchovský P., *Commutator theory for loops*, J. Algebra 399C (2014), 290–322.

[29] Stein A., *A Conjugacy Class as a Transversal in a Finite Group*, Journal of Algebra 239, 365–390 (2001).

[30] Thompson, John G., *Finite Groups with Fixed-Point-Free Automorphisms of Prime Order*, Proceedings of the National Academy of Sciences of the United States of America, Vol. 45, No. 4 (Apr. 15, 1959), 578–581.

[31] Valeriote, M. A. *A subalgebra intersection property for congruence distributive varieties*, the Canadian Journal of Mathematics, 61 (2009), no. 2, 451–464

[32] Valeriote, M.A. *Finite Simple Abelian Algebras are Strictly Simple*, Proceedings of the American Mathematical Society 108(1), 49-49, January 1990.

[33] Vendramin L., *Doubly Transitive Group and Quandles* , accepted for publication in J. Math. Soc. Japan