©2021 The Mathematical Society of Japan
J. Math. Soc. Japan
Vol. 73, No. 1 (2021) pp. 41–75
doi: 10.2969/jmsj/83168316

Commutator theory for racks and quandles

By Marco Bonatto and David Stanovský

(Received Aug. 19, 2019)

Abstract. We adapt the commutator theory of universal algebra to the particular setting of racks and quandles, exploiting a Galois connection between congruences and certain normal subgroups of the displacement group. Congruence properties, such as abelianness and centrality, are reflected by the corresponding relative displacement groups, and the global properties, solvability and nilpotence, are reflected by the properties of the whole displacement group. To show the new tool in action, we present three applications: non-existence theorems for quandles (no connected involutory quandles of order 2^k, no latin quandles of order $\equiv 2 \pmod 4$), a non-colorability theorem (knots with trivial Alexander polynomial are not colorable by solvable quandles; in particular, by finite latin quandles), and a strengthening of Glauberman's results on Bruck loops of odd order.

1. Introduction.

1.1. Motivation.

The primary motivation for the development of the theory of racks and quandles comes from constructions of knot invariants [**16**], [**21**], [**35**], describing set-theoretic solutions to the quantum Yang–Baxter equation [**22**], [**23**], constructions of Hopf algebras [**2**], or the abstract theory of quasigroups and loops [**44**]. In the present paper, we develop the concepts of *abelianness* and *centrality*, and the derived concepts of *solvability* and *nilpotence*, for racks and quandles, by adaptation of the general commutator theory of universal algebra [**26**] to the particular setting of racks. We aim at new tools to be used in a deeper study of rack theory and its applications.

The *commutator theory*, as developed in universal algebra, originated in the 1970's works of Smith [**42**], and culminated in the Freese–McKenzie monograph [**26**], expanding the scope from Mal'tsev varieties to congruence modular varieties and beyond. The initial ideas developed into a rather deep theory that proved immensely useful in solving various problems of universal algebra and combinatorics of functions, see [**38**] for references. We also refer to [**45**], [**46**] for a successful adaptation of the commutator theory to quasigroups and loops ("non-associative groups"), which was an inspiration for the present work.

Quandles do not form a congruence modular variety, hence one cannot expect the best behavior of the congruence commutator. Nevertheless, the derived notions of abelianness and centrality, and subsequently solvability and nilpotence, are important structural concepts in any algebraic structure [**30**]. The main idea behind our paper is

2010 *Mathematics Subject Classification.* Primary 57M27; Secondary 08A30, 20N02, 20N05.

Key Words and Phrases. quandles and racks, solvability, nilpotence, commutator theory, left distributive quasigroups.

This research was partly supported by the GAČR grant 18-20123S.

that, in racks, they are well reflected inside the *displacement group* of rack, thus allowing to use group-theoretical arguments to prove theorems about racks. The main results are stated in Section 1.2, and their proof occupies a major part of the paper. Several simple applications of the new tool are presented in Section 8, and more involved results will be the subject of subsequent papers [**8**], [**9**], [**10**], [**40**].

The strong interplay between congruences of a rack and normal subgroups of its displacement group has been noticed already at the very dawn of quandle theory by Nagao [**39**], and later rediscovered and developed in various forms, for example, [**13**], [**36**]. They all inspired our approach which is based on the Galois connection given by the operators Dis_α and con_N, developed in Section 3.

Our results are also relevant in the context of the general theory of quasigroups and loops. Latin quandles are also known as *left distributive quasigroups* and have been studied extensively even before the quandle theory was born, see [**44**] for a survey. The concept of solvability was introduced on several independent occasions. Formal definitions were somewhat different, but all shared the property that solvable latin quandles had solvable left multiplication groups. Here we show that the latter property is equivalent to solvability in the sense of universal algebra, and using Stein's theorem [**47**] we conclude that all finite latin quandles are solvable. Principal isotopy translates the results into the setting of loops. Using the Belousov–Onoi correspondence [**4**], we obtain that Bruck loops of odd order are solvable in the sense of universal algebra, thus strengthening Glauberman's theorem [**29**] whose English statement was identical, however, using a weaker definition of solvability (see [**45**] for a discussion). This is one of the rare examples when a result about loops is derived from the properties of their quasigroup isotopes, turning the usual flow of ideas.

Our results are also relevant in the context of the theory of *supernilpotence* [**1**]. This is a stronger property than nilpotence, based on Bulatov's commutators of higher arity. A theorem by Kearnes [**37**, Theorem 3.14] says that a finite algebraic structure with a Mal'tsev term (a quasigroup, or a latin quandle, in particular) is supernilpotent if and only if it is a direct product of nilpotent algebras of prime power size. In this context, our Theorem 1.4 and Corollary 8.5 state that, for finite latin quandles and for Bruck loops of odd order, nilpotence is equivalent to supernilpotence.

Some of the properties of the connection between congruences and normal subgroups hold more generally, in any binary algebraic structure with bijective left translations, so called *left quasigroup*. Our motivation for general formulation comes from the quantum Yang–Baxter equation: the non-degenerate set-theoretic solutions can be interpreted as a pair of left quasigroups, and in some cases, as a single left quasigroup. One example is the class of racks, and another one is the class of involutive solutions in Rump's notation [**41**]. Some of our concepts are immediately useful in this context.

1.2. Main results.

Let Q be a rack. We define the *displacement group* of Q by $\mathrm{Dis}(Q) = \langle L_a L_b^{-1} : a, b \in Q\rangle$ where $L_u(x) = u * x$ is the left translation by u. For a congruence α of Q, we define *the displacement group relative to* α by $\mathrm{Dis}_\alpha = \langle L_a L_b^{-1} : a \,\alpha\, b\rangle$. See Sections 2 and 3 for details.

Let α be an equivalence on a set X and let a group G act on X. We call the action *α-semiregular* if for every $g \in G$, if $g(a) = a$ then $g(b) = b$ for every $b \,\alpha\, a$.

The first main theorem, proved in Section 5.1, characterizes abelian and central congruences by group-theoretic properties of the corresponding relative displacement groups. The proof actually works for a larger class, properly containing all racks, so called *ltt left quasigroups*. The ltt property is a syntactic condition that requires all terms to take a particular equivalent form, explained in Section 4.1.

Theorem 1.1. *Let Q be an ltt left quasigroup and α its congruence. Then*

(1) *α is abelian if and only if the subgroup* Dis_α *is abelian and it acts α-semiregularly on Q;*

(2) *α is central if and only if the subgroup* Dis_α *is central in* $\mathrm{Dis}(Q)$ *and* $\mathrm{Dis}(Q)$ *acts α-semiregularly on Q.*

As a special case, we obtain that an ltt left quasigroup Q is abelian if and only if $\mathrm{Dis}(Q)$ is abelian and acts semiregularly on Q. This partly extends the main result of [**33**].

The second main theorem, proved in Section 6.1, characterizes solvability and nilpotence of a rack by the corresponding group-theoretic property of the displacement group.

Theorem 1.2. *Let Q be rack. Then*

(1) *Q is solvable if and only if* $\mathrm{Dis}(Q)$ *is solvable;*

(2) *Q is nilpotent if and only if* $\mathrm{Dis}(Q)$ *is nilpotent.*

Corollary 1.3. *Finite latin quandles are solvable.*

Proof. Finite latin quandles have solvable displacement groups by [**47**, Theorem 1.4], hence Theorem 1.2 applies. □

In Section 6.2, we prove the prime decomposition theorem for finite nilpotent quandles satisfying certain homogeneity assumptions. In particular, it applies to latin quandles.

Theorem 1.4. *Let Q be a finite connected faithful quandle. Then Q is nilpotent if and only if Q is a direct product of connected quandles of prime power size.*

In Section 7, we present the construction of abelian and central extensions, inspired by [**2**, Section 2.3] and [**26**, Section 7], and ask which surjective homomorphisms can be represented by these extensions. We show a positive result for central extensions (Proposition 7.8) and a negative result for abelian extensions (Example 7.11 which stands in contrast to our positive results on abelian extensions of loops [**46**, Theorem 4.1]).

In the last section, we present three applications. The proofs are simple, yet, with previous methods, the results were either very complicated to prove, or inaccessible. First, we show two non-existence results: there are no connected involutory quandles of order 2^k (Theorem 8.1), and there are no latin quandles of order $\equiv 2 \pmod 4$ (Theorem 8.2). The latter is known as Stein's theorem [**48**] and originally required a rather involved topological argument. Next, we prove that knots and links with trivial Alexander polynomial are not colorable by any solvable quandle (Theorem 8.4), extending an analogical result for affine quandles [**3**]. Finally, we explain the Belousov–Onoi correspondence that translates our results for latin quandles into their loop isotopes.

1.3. The structure of the paper.

In Section 2, we summarize the basic facts and observations about quandles, racks and left quasigroups, necessary to understand the rest of the paper. Section 3 explains the Galois correspondence between congruences and subgroups of the displacement group. In the end, we also discuss when the two operators Dis_α and con_N give mutually inverse lattice isomorphisms. In Section 4, we give a brief introduction to the commutator theory and present several basic facts about terms in left quasigroups, including the ltt property. In Section 5, we adapt the commutator theory to ltt quasigroups and prove Theorem 1.1. Then we show that for faithful quandles, one can drop the semiregularity conditions, and, in turn, the commutator has better properties. We also calculate the center of a rack, and prove that medial racks are nilpotent. In Section 6, we investigate nilpotence and solvability, and prove Theorems 1.2 and 1.4. Section 7 is about abelian and central extensions, and Section 8 contains the applications.

2. Rack and quandle theoretic concepts.

2.1. Division in binary algebraic structures.

By an *algebraic structure* we mean a non-empty set equipped with a collection of operations (of arbitrary finite arity). We will mostly consider algebraic structures with two binary operations.

Let $*$ be a binary operation on Q. For $a \in Q$, let

$$L_a : Q \to Q, \quad b \mapsto a * b; \qquad R_a : Q \to Q, \quad a \mapsto b * a$$

be the *left translation* by a and the *right translation* by a, respectively. If all left translations are bijective, we can define the left division operation by

$$a \backslash b = L_a^{-1}(b).$$

The resulting algebraic structure $Q = (Q, *, \backslash)$ will be called a *left quasigroup*. Left quasigroups can be axiomatized by the identities $x \backslash (x * y) = y = x * (x \backslash y)$. A left quasigroup is called *involutory* if $L_a^2 = 1$ for every a, i.e., if the identity $x * (x * y) = y$ holds for every $x, y \in Q$, or equivalently, if $* = \backslash$.

If all left and right translations are bijective, we use the term *quasigroup*, or we use the adjective *latin*. The right division operation is defined analogically.

Many universal algebraic concepts, such as subalgebras, congruences and their properties (in particular, the centralizing relation $C(\alpha, \beta; \delta)$ that defines the commutator), are sensitive to the choice of operations. In our paper, left quasigroups, including racks and quandles, will always be considered as structures $(Q, *, \backslash)$, including left division (and excluding right division in the latin case). In particular, substructures and quotients of left quasigroups are always left quasigroups.

For latin quandles, there is a collision with the standard setting of quasigroup theory, where both division operations are considered. We avoid this collision by stating all results only for finite quasigroups where the choice of operations is irrelevant, since both divisions can be defined by a multiplicative term: indeed, if n is the least common multiple of orders of all left translations, then $a\backslash b = L_a^{n-1}(b) = a * (a * (\cdots * (a * b)))$, and similarly for right division.

For a left quasigroup Q, we define two important subgroups of the symmetric group over the set Q: the *left multiplication group* and the *displacement group*

$$\mathrm{LMlt}(Q) = \langle L_a :\ a \in Q\rangle, \qquad \mathrm{Dis}(Q) = \langle L_a L_b^{-1} :\ a, b \in Q\rangle.$$

The group $\mathrm{LMlt}(Q)$ acts naturally on the set Q. Whenever we say that (a subgroup of) $\mathrm{LMlt}(Q)$ acts in some way, we implicitly mean the natural action on Q.

A left quasigroup Q is called *connected* if $\mathrm{LMlt}(Q)$ acts transitively on Q. Quasigroups are always connected, since $L_{b/a}(a) = b$ for every a, b.

2.2. Racks and quandles.

A *rack* is a left quasigroup in which all left translations are automorphisms. This can be expressed as an identity,

$$x * (y * z) = (x * y) * (x * z), \tag{2.1}$$

called *left self-distributivity.* An idempotent rack (i.e., where $x * x = x$ holds) is called a *quandle.* We refer to [**35**, Sections 1–8] or [**31**, Section 2] for a collection of basic properties of racks and quandles to be used in the present paper. In particular, we will use without further reference that, in quandles, the actions of $\mathrm{LMlt}(Q)$ and $\mathrm{Dis}(Q)$ have the same orbits.

A binary algebraic structure satisfying the identity $(x * y) * (u * v) = (x * u) * (y * v)$ is called *medial.* A rack is medial if and only if its displacement group is abelian [**31**, Proposition 2.4]. A comprehensive study of medial quandles can be found in [**34**].

Let $(Q, *)$ be a binary algebraic structure. For every $f \in \mathrm{Aut}(Q)$ and $a \in Q$, we have

$$L_{f(a)} = f L_a f^{-1}. \tag{2.2}$$

In particular, if Q is a rack, then $L_{a*b} = L_a L_b L_a^{-1}$ for every $a, b \in Q$.

We will need the following constructions of quandles.

Example 2.1. Let G be a group and $C \subseteq G$ closed under conjugation. For $a, b \in C$, let $a * b = aba^{-1}$ and $a\backslash b = a^{-1}ba$. Then $(C, *, \backslash)$ is a quandle, called the *conjugation quandle* on C.

Example 2.2. Let G be a group, $f \in \mathrm{Aut}(G)$ and $H \leq \mathrm{Fix}(f) = \{a \in G : f(a) = a\}$. Let G/H be the set of left cosets, $G/H = \{aH\ :\ a \in G\}$, and define

$$aH * bH = af(a^{-1}b)H.$$

It is easy to calculate that there is a left division operation $\backslash$ such that $\mathcal{Q}_{\mathrm{Hom}}(G, H, f) = (G/H, *, \backslash)$ is a quandle, called the *coset quandle.* A coset quandle of the form $\mathcal{Q}_{\mathrm{Hom}}(G, 1, f)$ is called *principal.* If, in addition, G is an abelian group, then

$\mathcal{Q}_{\mathrm{Hom}}(G,1,f)$ is called *affine*, and it is also denoted by $\mathrm{Aff}(G,f)$.

A general quandle is called *principal* (resp. *affine*), if it is isomorphic to a principal (resp. affine) coset quandle.

Example 2.3. A *permutation rack* is a rack whose $*$ operation does not depend on the left argument, i.e., $a*b=\sigma(b)$ where σ is a permutation of the underlying set. In particular, by a *projection quandle* we mean a permutation quandle with the operation $a*b=b$. (The adjective *trivial* is reserved for one-element structures.)

All connected quandles with ≤ 47 elements were enumerated [**31**], [**49**] and stored in the RIG library, a part of the RIG package for GAP. We often pick examples from the library, and our claims are easy to verify in GAP. To put the subject of our study into the RIG context: there are 791 connected quandles of order ≤ 47, of which 492 are abelian, 49 nilpotent non-abelian, and 185 solvable non-nilpotent. Among the 65 non-solvable quandles, 23 are simple non-abelian, and the remaining 42 have an abelian congruence with a simple non-abelian factor.

2.3. Congruences and homomorphisms.

Let α be an equivalence on a set A. We will use the notation $a\,\alpha\,b$ instead of $(a,b)\in\alpha$. The blocks will be denoted by $[a]_\alpha=\{b\in A\,:\,a\,\alpha\,b\}$, and we let $A/\alpha=\{[a]_\alpha\,:\,a\in A\}$. We drop the index α if it is clear to which equivalence we are referring.

To study quotients (or factors) of left quasigroups, we borrow the concept of a *congruence* from universal algebra [**6**, Chapter 1]. A congruence of an algebraic structure A is an equivalence α on A compatible with all operations of A. For left quasigroups, this means that, for every a,b,c,d,

$$a\,\alpha\,b \ \text{ and } \ c\,\alpha\,d \ \Rightarrow \ (a*c)\,\alpha\,(b*d) \ \text{ and } \ (a\backslash c)\,\alpha\,(b\backslash d).$$

Note that an equivalence α is compatible with a binary operation $\circ$ if and only if, for every a,b,c,

$$a\,\alpha\,b \ \Rightarrow \ (a\circ c)\,\alpha\,(b\circ c) \ \text{ and } \ (c\circ a)\,\alpha\,(c\circ b).$$

Congruences of an algebraic structure A form a complete lattice, denoted by $\mathrm{Con}(A)$, with the largest element $1_A=A\times A$ and the smallest element $0_A=\{(a,a)\,:\,a\in A\}$. The lattice operations will be denoted by $\wedge$ and $\vee$. Namely, $\alpha\wedge\beta$ is the intersection of α and β, and $\alpha\vee\beta$ is the smallest congruence containing the union of α and β.

If α is a congruence of A, the quotient A/α is well defined. It is easy to see that

$$\mathrm{Con}(A/\alpha)=\{\beta/\alpha:\ \alpha\leq\beta\in\mathrm{Con}(A)\}$$

where $[a]_\alpha\,\beta/\alpha\,[b]_\alpha$ if and only if $a\,\beta\,b$.

Let Q be a left quasigroup and α its congruence. We will frequently use the following two observations. For every $f\in\mathrm{LMlt}(Q)$, if $a\,\alpha\,b$ then $f(a)\,\alpha\,f(b)$. If a is an idempotent element, then the block $[a]_\alpha$ is a subalgebra of Q (indeed, if $b,c\in[a]$, then $(b*c)\,\alpha\,(a*a)=a$ and $(b\backslash c)\,\alpha\,(a\backslash a)=a$).

Let Q and R be left quasigroups. A mapping $f : Q \to R$ is called a *homomorphism*, if $f(a * b) = f(a) * f(b)$ for every $a, b \in Q$. Then also $f(a\backslash b) = f(a)\backslash f(b)$ for every $a, b \in Q$: we have $f(b) = f(a * (a\backslash b)) = f(a) * f(a\backslash b)$, and divide by $f(a)$ from the left. Every homomorphism $f : Q \to R$ carries a congruence of Q, called the *kernel*:

$$\ker(f) = \{(a, b) \,:\, f(a) = f(b)\}.$$

By the first isomorphism theorem, $Q/\ker(f) \simeq \operatorname{Im}(f)$, hence quotients and homomorphic images are essentially the same thing.

Let Q be a left quasigroup and α its congruence. It is straightforward to check that the mapping

$$\pi_\alpha : \mathrm{LMlt}(Q) \longrightarrow \mathrm{LMlt}(Q/\alpha), \quad L_{a_1}^{k_1} \cdots L_{a_n}^{k_n} \mapsto L_{[a_1]}^{k_1} \cdots L_{[a_n]}^{k_n} \tag{2.3}$$

is a well defined surjective homomorphism of groups [**2**]. The restriction of π_α to $\mathrm{Dis}(Q)$ gives a surjective homomorphism $\mathrm{Dis}(Q) \to \mathrm{Dis}(Q/\alpha)$, and its kernel will be denoted by Dis^α. It has the following characterization.

Lemma 2.4. *Let Q be a left quasigroup and α its congruence. Then*

$$\mathrm{Dis}^\alpha = \{h \in \mathrm{Dis}(Q) \,:\, h(a)\,\alpha\,a \textit{ for every } a \in Q\}.$$

Proof. Since $[h(a)] = \pi_\alpha(h)([a]) = [a]$, then $\pi_\alpha(h) = 1$ if and only if $[h(a)] = [a]$ for every $a \in Q$. □

Observe that if Q is a connected left quasigroup, then every factor is also connected (apply the mapping π_α). The converse is false, e.g., for any direct product of a connected and disconnected rack.

A congruence in which all blocks have the same size is called *uniform*.

Proposition 2.5. *Let Q be a left quasigroup and α its congruence such that Q/α is connected. Then α is uniform. Moreover, if Q is a quandle, the blocks of α are pairwise isomorphic subquandles of Q.*

Proof. Since Q/α is connected, for every $[a], [b] \in Q/\alpha$ there is $h \in \mathrm{LMlt}(Q)$ such that $[b] = \pi_\alpha(h)([a])$. Then $h|_{[a]}$ is a bijection $[a] \to [b]$: it maps $[a]$ into $[b]$, because $c\,\alpha\,a$ implies $h(c)\,\alpha\,h(a) = b$, and $h^{-1}|_{[b]}$ is its inverse mapping.

If Q is a quandle then every congruence block is a subquandle, and thus $h|_{[a]}$ is an isomorphism, since $h \in \mathrm{LMlt}(Q) \leq \mathrm{Aut}(Q)$. □

2.4. Orbit decomposition and Cayley kernel.

In the variety of racks, two particular congruences play a very important role: the *orbit decomposition*, and the *Cayley kernel*.

Let Q be a left quasigroup, and N a normal subgroup of $\mathrm{LMlt}(Q)$. We denote by $\mathcal{O}_N$ the transitivity relation of the action of N on Q. In particular, for $N = \mathrm{LMlt}(Q)$, we obtain the *orbit decomposition* of Q, denoted shortly $\mathcal{O}_Q$.

Lemma 2.6 ([**13**, Theorem 6.1]). *Let Q be a rack and $N \trianglelefteq \mathrm{LMlt}(Q)$. Then $\mathcal{O}_N$ is a congruence of Q.*

Proof. Clearly $\mathcal{O}_N$ is an equivalence relation on Q. Let $b\,\mathcal{O}_N\,c$, i.e., $c = f(b)$ for some $f \in N$. Since N is normal in $\mathrm{LMlt}(Q)$,

$$\begin{aligned} a * c = L_a(c) = L_a f(b) = L_a f L_a^{-1}(a * b),\\ a\backslash c = L_a^{-1}(c) = L_a^{-1} f(b) = L_a^{-1} f L_a(a\backslash b), \end{aligned}$$

and thus $(a * c)\,\mathcal{O}_N\,(a * b)$ and $(a\backslash c)\,\mathcal{O}_N\,(a\backslash b)$. On the other side,

$$\begin{aligned} c * a = L_c(a) = L_{f(b)} L_b^{-1}(b * a) = f L_b f^{-1} L_b^{-1}(b * a),\\ c\backslash a = L_c^{-1}(a) = L_{f(b)}^{-1} L_b(b\backslash a) = f L_b^{-1} f^{-1} L_b(b\backslash a), \end{aligned}$$

and thus $(c * a)\,\mathcal{O}_N\,(b * a)$ and $(c\backslash a)\,\mathcal{O}_N\,(b\backslash a)$. □

Various properties of the $\mathcal{O}_N$ congruences were proved by Even and Gran in [**24**]: for example, that they permute with any other congruence.

Let Q be a left quasigroup. The *Cayley representation* is the mapping $L_Q : Q \to \mathrm{Sym}(Q)$, $a \mapsto L_a$. For racks, L_Q is a quandle homomorphism (with respect to the conjugation operation on $\mathrm{Sym}(Q)$), but, unlike for groups, L_Q is not necessarily one-to-one. The kernel of L_Q,

$$\lambda_Q = \{(a, b) : L_a = L_b\},$$

will be called the *Cayley kernel* Q. A rack with trivial Cayley kernel is called *faithful.* Note that every faithful rack is a quandle (in racks, $L_{a*a} = L_a$ for every a), isomorphic to a conjugation quandle (the image of the Cayley representation).

3. Congruences and subgroups of the displacement group.

3.1. Displacement groups relative to congruences.

Let Q be a left quasigroup and α its congruence. We define the *displacement group relative to* α, denoted by Dis_α, as the smallest normal subgroup of $\mathrm{LMlt}(Q)$ containing all $L_a L_b^{-1}$ such that $a\,\alpha\,b$. That is,

$$\mathrm{Dis}_\alpha = \langle f L_a L_b^{-1} f^{-1} : a\,\alpha\,b,\ f \in \mathrm{LMlt}(Q)\rangle \leq \mathrm{LMlt}(Q).$$

The generating set is closed with respect to conjugation by any automorphism of Q. In particular, if Q is a rack, then

$$\mathrm{Dis}_\alpha = \langle L_a L_b^{-1} : a\,\alpha\,b\rangle.$$

The elements of the relative displacement group can be described as follows.

Lemma 3.1. *Let Q be a left quasigroup and α its congruence. Then*

$$\mathrm{Dis}_\alpha = \big\{L_{a_n}^{k_n} \cdots L_{a_1}^{k_1} L_{b_1}^{-k_1} \cdots L_{b_n}^{-k_n} : k_i \in \mathbb{Z},\ a_i\,\alpha\,b_i \textit{ for all } i = 1, \dots, n\big\}.$$

Proof. Let N denote the set on the right hand side of the expression. Temporarily, we will say that two mappings $u,v\in\mathrm{LMlt}(Q)$ are *α-symmetric*, if $u=L_{a_n}^{k_n}\cdots L_{a_1}^{k_1}$ and $v=L_{b_1}^{-k_1}\cdots L_{b_n}^{-k_n}$ for some $k_i\in\mathbb{Z}$ and $a_i\,\alpha\,b_i$. So, N consists of all mappings of the form uv where u,v are α-symmetric.

First, we prove that N is a normal subgroup of $\mathrm{LMlt}(Q)$. Let $f=f_1f_2$ and $g=g_1g_2$ be elements of N where both f_1,f_2 and g_1,g_2 are α-symmetric. Then the inverse $f^{-1}=f_2^{-1}f_1^{-1}$ belongs to N, since f_1^{-1},f_2^{-1} are also α-symmetric; the composition $fg=g_1g_1^{-1}f_1f_2g_1g_2$ belongs to N, since all three pairs g_1,g_2 and g_1^{-1},g_1 and f_1,f_2 are α-symmetric; and the conjugate $L_a^{\pm1}fL_a^{\mp1}$ belongs to N for an obvious reason. Since N contains the generators of Dis_α, we have that $\mathrm{Dis}_\alpha\subseteq N$.

For the converse inclusion, we proceed by induction on the length of the expression, i.e., on $n=\sum_{i=1}^n|k_i|$ where $f=L_{a_n}^{k_n}\cdots L_{a_1}^{k_1}L_{b_1}^{-k_1}\cdots L_{b_n}^{-k_n}\in N$, $k_i\neq0$. For $n=0$, we have $f=1$ and the statement is trivial. In the induction step, let

$$g=L_{a_n}^{k_n-e}L_{a_{n-1}}^{k_{n-1}}\cdots L_{a_1}^{k_1}L_{b_1}^{-k_1}\cdots L_{b_{n-1}}^{-k_{n-1}}L_{b_n}^{-k_n+e}\in N,$$

where $e=1$ if $k_n>0$, and $e=-1$ otherwise. It has a shorter length, and therefore belongs to Dis_α. Now, since Dis_α is a normal subgroup,

$$f=L_{a_n}^{e}gL_{b_n}^{-e}=\underbrace{L_{a_n}^{e}gL_{a_n}^{-e}}_{\in\mathrm{Dis}_\alpha}\underbrace{L_{a_n}^{e}L_{b_n}^{-e}}_{\in\mathrm{Dis}_\alpha}\in\mathrm{Dis}_\alpha,$$

and the proof is finished. □

Observe that $\mathrm{Dis}_\alpha\leq\mathrm{Dis}^\alpha$: if $a\,\alpha\,b$, then $L_{[a]}L_{[b]}^{-1}$ is the identity mapping on Q/α, and using the definition from (2.3),

$$\pi_\alpha(fL_aL_b^{-1}f^{-1})=\pi_\alpha(f)L_{[a]}L_{[b]}^{-1}\pi_\alpha(f)^{-1}=1_{Q/\alpha}.$$

It is often the case that $\mathrm{Dis}_\alpha\neq\mathrm{Dis}^\alpha$. Obviously, $\mathrm{Dis}_\alpha\neq\mathrm{Dis}^\alpha$ happens whenever $\alpha\leq\lambda_Q$ (hence $\mathrm{Dis}_\alpha=1$) and $\mathrm{Dis}(Q)\not\simeq\mathrm{Dis}(Q/\alpha)$. There are also examples which cannot be explained by the Cayley kernel, e.g., in non-principal latin quandles of size 27, as can be checked directly in the RIG library. On the positive side, $\mathrm{Dis}_\alpha=\mathrm{Dis}^\alpha$ in any finite principal latin quandle, see Example 3.11.

Proposition 3.2. *Let Q be a left quasigroup and α,β its congruences. Then*

(1) *if $\alpha\leq\beta$, then $\pi_\alpha(\mathrm{Dis}_\beta)=\mathrm{Dis}_{\beta/\alpha}$ and $\pi_\alpha(\mathrm{Dis}^\beta)=\mathrm{Dis}^{\beta/\alpha}$,*

(2) *$\mathrm{Dis}^{\alpha\wedge\beta}=\mathrm{Dis}^\alpha\cap\mathrm{Dis}^\beta$ and $\mathrm{Dis}_{\alpha\vee\beta}=\mathrm{Dis}_\alpha\mathrm{Dis}_\beta$,*

(3) *if λ_Q is a congruence, then $\mathrm{Dis}_\alpha=\mathrm{Dis}_{\alpha\vee\lambda_Q}$.*

Proof. (1) Using Lemma 2.4, we have

$$\mathrm{Dis}_{\beta/\alpha}=\langle fL_{[a]_\alpha}L_{[b]_\alpha}^{-1}f^{-1}\,:\,a\,\beta\,b,\ f\in\mathrm{LMlt}(Q/\alpha)\rangle=\pi_\alpha(\mathrm{Dis}_\beta),$$
$$\mathrm{Dis}^{\beta/\alpha}=\{\pi_\alpha(h)\in\mathrm{Dis}(Q/\alpha)\,:\,h(a)\,\beta\,a\}=\pi_\alpha(\mathrm{Dis}^\beta).$$

(2) For intersection, using Lemma 2.4,

$$\begin{aligned}\mathrm{Dis}^{\alpha\wedge\beta} &= \{h \in \mathrm{Dis}(Q) \,:\, h(a)\,(\alpha\wedge\beta)\,a\,,\forall a\in Q\}\\ &= \{h \in \mathrm{Dis}(Q) \,:\, h(a)\,\alpha\,a \ \text{ and } \ h(a)\,\beta\,a, \forall a\in Q\} = \mathrm{Dis}^{\alpha}\cap\mathrm{Dis}^{\beta}.\end{aligned}$$

For join, it is easy to see that both $\mathrm{Dis}_\alpha, \mathrm{Dis}_\beta \le \mathrm{Dis}_{\alpha\vee\beta}$, and thus $\mathrm{Dis}_\alpha\mathrm{Dis}_\beta \le \mathrm{Dis}_{\alpha\vee\beta}$. For the other inclusion, let $a\,(\alpha\vee\beta)\,b$, and take the witnesses $a=a_1,\dots,a_n$ and $b_1,\dots,b_n=b$ such that $a_i\,\alpha\,b_i$ and $b_i\,\beta\,a_{i+1}$, for every i. Then

$$L_aL_b^{-1} = \underbrace{L_{a_1}L_{b_1}^{-1}}_{\in\mathrm{Dis}_\alpha}\underbrace{L_{b_1}L_{a_2}^{-1}}_{\in\mathrm{Dis}_\beta}\underbrace{L_{a_2}L_{b_2}^{-1}}_{\in\mathrm{Dis}_\alpha}\cdots\underbrace{L_{a_n}L_{b_n}^{-1}}_{\in\mathrm{Dis}_\beta} \in \mathrm{Dis}_\alpha\mathrm{Dis}_\beta,$$

and thus every generator $fL_aL_b^{-1}f^{-1}$ of $\mathrm{Dis}_{\alpha\vee\beta}$ belongs to $\mathrm{Dis}_\alpha\mathrm{Dis}_\beta$.

(3) This is an immediate consequence of (2) with $\beta=\lambda_Q$, since $\mathrm{Dis}_{\lambda_Q}=1$. □

Proposition 3.3. *Let Q be a rack and α its congruence. Then*

(1) $[\mathrm{Dis}^\alpha, \mathrm{LMlt}(Q)] \le \mathrm{Dis}_\alpha$,

(2) $\mathrm{Dis}^\alpha = \mathrm{Dis}^{\mathcal{O}_{\mathrm{Dis}^\alpha}}$ *and* $\mathcal{O}_N = \mathcal{O}_{\mathrm{Dis}^{\mathcal{O}_N}}$,

(3) $\mathcal{O}_{\mathrm{Dis}^\alpha} \le \alpha$,

(4) *if Q is a quandle and* $\mathrm{Dis}_\alpha = \mathrm{Dis}(Q)$, *then* $\mathcal{O}_Q \le \alpha$.

Proof. (1) Consider $f \in \mathrm{Dis}^\alpha \le \mathrm{Aut}(Q)$ and $a \in Q$. Then $f(a)\,\alpha\,a$, and thus, using (2.2), $[f, L_a] = L_aL_{f(a)}^{-1} \in \mathrm{Dis}_\alpha$.

(2) Let $\beta = \mathcal{O}_{\mathrm{Dis}^\alpha}$. Then $\beta \le \alpha$, and so $\mathrm{Dis}^\beta \le \mathrm{Dis}^\alpha$. In the other direction, for $h \in \mathrm{Dis}^\alpha$ we have $h(a)\,\beta\,a$ for every $a \in Q$, and thus $h \in \mathrm{Dis}^\beta$.
According to Lemma 2.4, $N \le \mathrm{Dis}^{\mathcal{O}_N}$ and the orbits of $\mathrm{Dis}^{\mathcal{O}_N}$ are contained in the orbit of N. Therefore N and $\mathrm{Dis}^{\mathcal{O}_N}$ have the same orbits, i.e., $\mathcal{O}_N = \mathcal{O}_{\mathrm{Dis}^{\mathcal{O}_N}}$.

(3) If $b = h(a)$ for some $h \in \mathrm{Dis}^\alpha$, then $b = h(a)\,\alpha\,a$ by Lemma 2.4.

(4) If $\mathrm{Dis}_\alpha = \mathrm{Dis}(Q)$, then also $\mathrm{Dis}^\alpha = \mathrm{Dis}(Q)$ and thus $\mathrm{Dis}(Q/\alpha) = 1$. So Q/α is a projection quandle and thus $\mathcal{O}_Q \le \alpha$. □

The converse of (4) fails, for example, for any 2-reductive medial quandle Q which is not a projection quandle: there we have $\mathcal{O}_Q \le \lambda_Q$ and thus $\mathrm{Dis}_{\mathcal{O}_Q} = 1$ (see [**34**] for details). In the condition (4), the assumption of idempotence is necessary: for example, permutation racks have trivial displacement groups, but $\mathcal{O}_Q$ can be non-trivial.

3.2. Congruences determined by subgroups.

Let Q be a left quasigroup. We will denote $\mathrm{Norm}(Q)$ the lattice of all subgroups of $\mathrm{Dis}(Q)$ that are normal in $\mathrm{LMlt}(Q)$ (this is a sublattice of the normal subgroups of $\mathrm{Dis}(Q)$). For $N \in \mathrm{Norm}(Q)$, we define a relation

$$\mathrm{con}_N = \{(a,b) : L_aL_b^{-1} \in N\},$$

called the *equivalence determined by N*.

Lemma 3.4. *Let Q be a rack and $N \in \mathrm{Norm}(Q)$. Then con_N is a congruence of Q.*

Proof. Assume $a \,\mathrm{con}_N\, b$, i.e., $L_a L_b^{-1} \in N$, and let $c \in Q$. Since N is normal in $\mathrm{LMlt}(Q)$,

$$L_{c*a} L_{c*b}^{-1} = L_c L_a L_c^{-1} L_c L_b^{-1} L_c^{-1} = L_c L_a L_b^{-1} L_c^{-1} \in N,$$

hence $(c*a) \,\mathrm{con}_N\, (c*b)$, and similarly, $(c\backslash a) \,\mathrm{con}_N\, (c\backslash b)$. On the other hand,

$$L_{a*c} L_{b*c}^{-1} = (L_a L_c L_a^{-1})(L_b L_c^{-1} L_b^{-1}) = \underbrace{(L_a L_b^{-1})}_{\in N} \underbrace{(L_b L_c (L_a^{-1} L_b) L_c^{-1} L_b^{-1})}_{\in N} \in N,$$

hence $(a*c) \,\mathrm{con}_N\, (b*c)$, and similarly, $(a\backslash c) \,\mathrm{con}_N\, (b\backslash c)$. □

Proposition 3.5. *Let Q be a rack and $N \in \mathrm{Norm}(Q)$. Then*

(1) $\mathrm{Dis}_{\mathrm{con}_N} \leq N \leq \mathrm{Dis}^{\mathrm{con}_N}$,

(2) $\mathrm{con}_N = 1_Q$ *if and only if* $N = \mathrm{Dis}(Q)$,

(3) *if* $N = \bigcap_{i\in I} N_i$, $N_i \in \mathrm{Norm}(Q)$, *then* $\mathrm{con}_N = \bigwedge_{i\in I} \mathrm{con}_{N_i}$,

(4) $\mathcal{O}_N \leq \mathrm{con}_N$.

Proof. (1) For the first inequality, note that $\mathrm{Dis}_{\mathrm{con}_N}$ is generated by all pairs $L_a L_b^{-1}$ which belong to N. For the second inequality, let $h \in N$. For every $a \in Q$, we have

$$L_{h(a)} L_a^{-1} = h L_a h^{-1} L_a^{-1} \in N,$$

because N is normal in $\mathrm{LMlt}(Q)$, and thus $h(a) \,\mathrm{con}_N\, a$. Using Lemma 2.4, $h \in \mathrm{Dis}^{\mathrm{con}_N}$.

(2) Clearly $\mathrm{con}_{\mathrm{Dis}(Q)} = 1_Q$. If $\mathrm{con}_N = 1_Q$, then $\mathrm{Dis}(Q) = \mathrm{Dis}_{1_Q} = \mathrm{Dis}_{\mathrm{con}_N} \leq N$ by (1).

(3) Clearly $L_a L_b^{-1} \in N$ if and only if $L_a L_b^{-1} \in N_i$ for every $i \in I$.

(4) It follows from the item (1) using Lemma 2.4. □

As we shall see soon, the Dis and con operators form a monotone Galois connection between $\mathrm{Con}(Q)$, the congruence lattice of a rack Q, and the lattice $\mathrm{Norm}(Q)$. Note that $\lambda_Q \leq \mathrm{con}_N$ for every N, and if $\alpha \leq \lambda_Q$ then $\mathrm{Dis}_\alpha = 1$. Therefore, the smaller the Cayley kernel is, the finer properties of the connection one can expect.

3.3. A Galois connection.

Recall that a *monotone Galois connection* is a pair of monotone functions between two ordered sets, $F : X \to Y$, $G : Y \to X$, such that $F(x) \leq y$ if and only if $x \leq G(y)$. Then, GF is a closure operator on X, FG is a kernel operator on Y, and $FGF = F$ and $GFG = G$. (See [**6**, Section 2.5] for details.)

Proposition 3.6. *Let Q be a rack. Then $\alpha \mapsto \mathrm{Dis}_\alpha$ and $N \mapsto \mathrm{con}_N$ is a monotone Galois connection between* $\mathrm{Con}(Q)$ *and* $\mathrm{Norm}(Q)$.

PROOF. Both mappings are indeed monotone. We prove that $\mathrm{Dis}_\alpha \leq N$ if and only if $\alpha \leq \mathrm{con}_N$.

($\Rightarrow$) If $a\,\alpha\,b$, then $L_aL_b^{-1} \in \mathrm{Dis}_\alpha \subseteq N$, and thus $a\,\mathrm{con}_N\,b$.

($\Leftarrow$) We need to show that $L_aL_b^{-1} \in N$ whenever $a\,\alpha\,b$. But $a\,\alpha\,b$ implies $a\,\mathrm{con}_N\,b$, and thus $L_aL_b^{-1} \in N$ by definition. □

In particular, the closure property says that $\alpha \leq \mathrm{con}_{\mathrm{Dis}_\alpha}$, and the kernel property says that $\mathrm{Dis}_{\mathrm{con}_N} \leq N$.

For a given rack Q, the connection of Proposition 3.6 is rarely bijective. The Cayley kernel is one obvious reason: the con operator cannot reach congruences below λ_Q, and the Dis operator maps all congruences below λ_Q to the trivial subgroup. Other reasons must exist, too, since, for example, neither operator is 1-1 or onto in the non-principal latin quandles of order 27 mentioned earlier.

The connection of Proposition 3.6 can recognize certain properties of factors. For example, we discuss faithfulness as follows.

PROPOSITION 3.7. *Let Q be a rack and α its congruence. Then Q/α is faithful if and only if $\alpha = \mathrm{con}_{\mathrm{Dis}^\alpha}$.*

PROOF. We prove that $\mathrm{con}_{\mathrm{Dis}^\alpha}/\alpha = \lambda_{Q/\alpha}$. Indeed, for $[a],[b] \in Q/\alpha$,

$$[a]\,(\mathrm{con}_{\mathrm{Dis}^\alpha}/\alpha)\,[b] \;\Leftrightarrow\; a\,\mathrm{con}_{\mathrm{Dis}^\alpha}\,b \;\Leftrightarrow\; L_aL_b^{-1} \in \mathrm{Dis}^\alpha \;\Leftrightarrow\; L_{[a]} = L_{[b]}.$$

Therefore, Q/α is faithful if and only if $\mathrm{con}_{\mathrm{Dis}^\alpha}/\alpha = 0_{Q/\alpha}$, that is, if and only if $\alpha = \mathrm{con}_{\mathrm{Dis}^\alpha}$. □

Proposition 3.7 implies that if Q/α is faithful and $\mathrm{Dis}_\alpha \neq \mathrm{Dis}^\alpha$, then $\alpha = \mathrm{con}_{\mathrm{Dis}_\alpha} = \mathrm{con}_{\mathrm{Dis}^\alpha}$, so the con operator cannot be injective.

PROPOSITION 3.8. *Let Q be a quandle such that every factor of Q is faithful. Then the* Dis *operator is injective and the* con *operator is surjective.*

PROOF. By Proposition 3.7, we have $\alpha \leq \mathrm{con}_{\mathrm{Dis}_\alpha} \leq \mathrm{con}_{\mathrm{Dis}^\alpha} = \alpha$, and thus $\mathrm{con}_{\mathrm{Dis}_\alpha} = \alpha$. This means that the con operator is left inverse to the Dis operator. Hence Dis must be injective and con must be surjective. □

REMARK 3.9. Let Q be a rack. Then $\alpha \mapsto \mathrm{Dis}^\alpha$ and $N \mapsto \mathcal{O}_N$ is also a monotone Galois connection between $\mathrm{Con}(Q)$ and $\mathrm{Norm}(Q)$. Indeed, from the characterization of Dis^α in Lemma 2.4 it is easy to check that $N \leq \mathrm{Dis}^\alpha$ if and only if $\mathcal{O}_N \leq \alpha$. At the moment, we have no use for this connection, and therefore focus on the one from Proposition 3.6.

3.4. Quandles with congruences determined by subgroups.

A rack is said to have *congruences determined by subgroups* (shortly, *CDSg*), if the connection in Proposition 3.6 is a lattice isomorphism $\mathrm{Con}(Q) \simeq \mathrm{Norm}(Q)$.

EXAMPLE 3.10. All simple quandles of size > 2 have CDSg, since both lattices have just two elements, as proved in [**36**, Lemma 2].

Example 3.11. The *polynomial functions* of an algebraic structure are obtained by term functions substituting some of the variables by constants. Two algebraic structures over a given set are *polynomially equivalent* if they have the same polynomial functions (see [**44**, Section 2.3] for an explanation of polynomial equivalence in the context of quasigroups).

Finite affine latin quandles have CDSg. They are polynomially equivalent to modules, and therefore, congruences correspond to submodules, which are exactly the elements of $\mathrm{Norm}(Q)$. A similar argument works more generally, for finite principal latin quandles, which are polynomially equivalent to algebraic structures of the form $(\mathrm{Dis}(Q), \cdot, ^{-1}, 1, \widehat{L_e})$ where $\widehat{L_e}$ denotes the inner automorphism given by L_e.

In the rest of the section, we characterize racks with CDSg and show that they are actually connected quandles.

Lemma 3.12. *Let Q be a rack and α its congruence. If Q has CDSg, then Q/α has CDSg.*

Proof. We know that $\mathrm{Con}(Q/\alpha) \simeq [\alpha, 1_Q]$ and $\mathrm{Norm}(Q/\alpha) \simeq [\mathrm{Dis}^\alpha, \mathrm{Dis}(Q)]$. The mapping Dis restricted to this interval is an isomorphism as well (and restricted con is its inverse), and the following diagram is commutative:

$$\begin{tikzcd}
{[\alpha, 1_Q]} \arrow[r, "\mathrm{Dis}"] \arrow[d] & {[\mathrm{Dis}^\alpha, \mathrm{Dis}(Q)]} \arrow[d] \\
\mathrm{Con}(Q/\alpha) \arrow[r, "\mathrm{Dis}"] & \mathrm{Norm}(Q/\alpha)
\end{tikzcd}$$

(the vertical arrows are the canonical isomorphisms). □

Proposition 3.13. *Let Q be a rack. Then Q has CDSg if and only if the following two conditions hold*:

(1) $\mathrm{Dis}_\alpha = \mathrm{Dis}^\alpha$ *for every* $\alpha \in \mathrm{Con}(Q)$,

(2) *every factor of Q is faithful.*

Proof. ($\Rightarrow$) Since $\mathrm{Dis}_{0_Q} = \mathrm{Dis}_{\lambda_Q} = 1$, necessarily $\lambda_Q = 0_Q$, and Q is faithful. Hence every factor of Q is faithful, and since $\alpha = \mathrm{con}_{\mathrm{Dis}^\alpha} = \mathrm{con}_{\mathrm{Dis}_\alpha}$, we have $\mathrm{Dis}_\alpha = \mathrm{Dis}^\alpha$ for every congruence α.

($\Leftarrow$) Let $N \in \mathrm{Norm}(Q)$. Then $\mathrm{Dis}_{\mathrm{con}_N} \leq N \leq \mathrm{Dis}^{\mathrm{con}_N}$, and condition (1) implies that $N = \mathrm{Dis}_{\mathrm{con}_N}$. By Proposition 3.7, $\mathrm{con}_{\mathrm{Dis}_\alpha} = \alpha$ for every $\alpha \in \mathrm{Con}(Q)$. □

Proposition 3.14. *Let Q be a rack with CDSg. Then $\alpha = \mathcal{O}_{\mathrm{Dis}_\alpha}$ for every $\alpha \in \mathrm{Con}(Q)$. In particular, Q is a connected quandle.*

Proof. In racks, $L_a = L_{a*a}$ for every a, hence non-idempotent racks are never faithful, contradicting Proposition 3.13(2). Let $\beta = \mathcal{O}_{\mathrm{Dis}_\alpha}$. By Proposition 3.13(1), $\mathrm{Dis}_\alpha = \mathrm{Dis}^\alpha$ and $\mathrm{Dis}_\beta = \mathrm{Dis}^\beta$, hence Proposition 3.3(2) says that $\mathrm{Dis}_\alpha = \mathrm{Dis}_\beta$, and thus $\mathrm{Dis}_{\alpha/\beta} = 1$ and $\alpha/\beta \leq \lambda_{Q/\beta}$. But Q/β is faithful, hence $\alpha = \beta$. In particular, for $\alpha = 1_Q$ we obtain that Q is connected. □

4. Universal algebraic concepts.

4.1. Left translation terms.

A term is a well-defined expression using variables and operation symbols in a given language; we will write $t(x_1,\dots,x_n)$ for a term using a subset of variables $x_1,\dots,x_n$. Given a term $t(x_1,\dots,x_n)$ and an algebraic structure $A=(A,\dots)$, the associated *term function* $t^A : A^n \to A$ evaluates the term t in A (see [**6**, Section 4.3] for formal definitions).

From now on, we will use the language $\{*,\backslash\}$ of left quasigroups. Terms will be considered as labeled rooted binary trees, with inner nodes labeled by operations and leaves by variables.

Left translation terms (shortly, *lt-terms*) are the terms in the language of left quasigroups of the form

$$t(x_1,\dots,x_n) = s_1(x_{i_1}) \circ_1 \big(s_2(x_{i_2}) \circ_2 (\dots (s_{m-1}(x_{i_{m-1}}) \circ_{m-1} s_m(x_{i_m})))\big), \qquad (4.1)$$

where $\circ_j \in \{*,\backslash\}$, s_j are unary terms, and $i_j \in \{1,\dots,n\}$. Somewhat less formally, we can write

$$t(x_1,\dots,x_n) = L^{\varepsilon_1}_{s_1(x_{i_1})} \cdots L^{\varepsilon_{m-1}}_{s_{m-1}(x_{i_{m-1}})}(s_m(x_{i_m}))$$

where $\varepsilon_j = 1$ if $\circ_j = *$ and $\varepsilon_j = -1$ if $\circ_j = \backslash$ (the expression makes a formal sense in the free left quasigroup over the alphabet $x_1,\dots,x_n$).

A left quasigroup, in which every term function results from some lt-term, will be called *ltt* left quasigroup. The following fact is well known and crucial for our adaptation of the general commutator theory to racks.

Proposition 4.1. *Every rack is an ltt left quasigroup.*

Proof. Using equation (2.2), it is easy to see that the following identities hold in every rack:

$$(x*y)*z = x*(y*(x\backslash z)), \quad (x\backslash y)*z = x\backslash(y*(x*z)),$$
$$(x*y)\backslash z = x*(y\backslash(x\backslash z)), \quad (x\backslash y)\backslash z = x\backslash(y\backslash(x\backslash z)).$$

Using these identities, every term can be transformed to an lt-term, by repeatedly expanding the uppermost left subterm which is not a leaf (see Figure 4.1 for an example). □

The proof suggests that there are many more examples of ltt left quasigroups: any quadruple of identities will work, as long as it "flattens" the term. For instance, a different class of ltt left quasigroups can be defined by modifying self-distributivity as follows.

Example 4.2. Let $\mathcal{C}$ be the class of left quasigroups satisfying the identities

$$(x*y)*z = x\backslash(y\backslash(x*z)) \quad \text{and} \quad (x\backslash y)*z = x*(y\backslash(x\backslash z)),$$

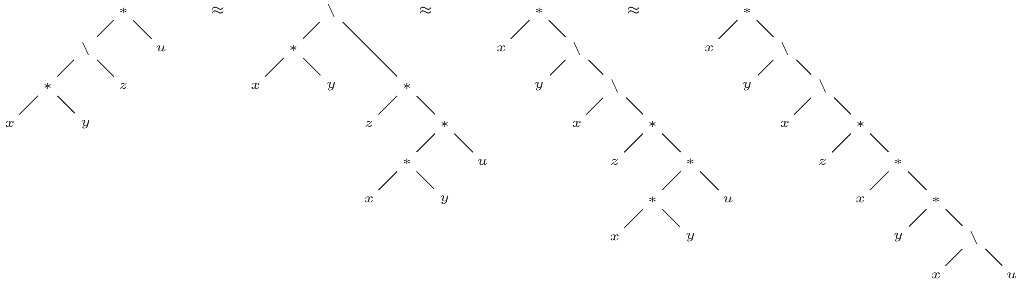

Figure 4.1. Transforming the term $((x*y)\backslash z)*u$ into a left translation form.

resulting from the corresponding rack identities by switching $*$ and $\backslash$ on the right-hand side. The ltt property can be proved similarly as for racks.

For involutory left quasigroups, the identities for $\mathcal{C}$ are equivalent to self-distributivity. However, in $\mathcal{C}$, $L_{a*a} = L_a^{-1}$, while in racks, $L_{a*a} = L_a$. Hence, the racks in $\mathcal{C}$ are precisely the involutory racks. An exhaustive computer search reveals that the smallest member of $\mathcal{C}$ which is not a rack has 4 elements and it is unique up to isomorphism. Furthermore the numbers of members of $\mathcal{C}$ which are not a rack are 1 of order 5, 8 of order 6, 20 of order 7 and 125 of order 8. The multiplication tables of the two smallest examples are below.

2	4	1	3
3	1	4	2
3	1	4	2
2	4	1	3

3	4	1	5	2
3	2	1	4	5
3	5	1	2	4
3	2	1	4	5
3	2	1	4	5

4.2. The commutator theory.

Let A be an algebraic structure. The commutator is a binary operation on the lattice $\mathrm{Con}(A)$, defined using the concept of centralization, explained below. For further study, we refer to [**26**], [**38**].

Let α, β, δ be congruences of A. We say that α *centralizes* β *over* δ, and write $C(\alpha,\beta;\delta)$, if for every $(n+1)$-ary term operation t, every pair $a\,\alpha\,b$ and every $u_1\,\beta\,v_1$, $\dots$, $u_n\,\beta\,v_n$ we have

$$t^A(a,u_1,\dots,u_n)\,\delta\,t^A(a,v_1,\dots,v_n) \quad \text{implies} \quad t^A(b,u_1,\dots,u_n)\,\delta\,t^A(b,v_1,\dots,v_n). \tag{TC}$$

The implication (TC) is referred to as the *term condition* for t, or shortly $\mathrm{TC}(t,\alpha,\beta,\delta)$. It is easy to show that $C(\alpha,\beta;\delta)$ holds if and only if $TC(t,\alpha,\beta,\delta)$ is satisfied for every term t in which the first variable occurs only once: indeed, we can use (TC) several times to replace every occurrence one-by-one (see [**45**, Lemma 4.1] for a formal proof). We will also need the following observations:

(C1) if $C(\alpha,\beta;\delta_i)$ for every $i\in I$, then $C(\alpha,\beta;\bigwedge\delta_i)$,

(C2) $C(\alpha,\beta;\alpha\wedge\beta)$, (C3) if $\theta \le \alpha \wedge \beta \wedge \delta$, then $C(\alpha, \beta; \delta)$ in A if and only if $C(\alpha/\theta, \beta/\theta; \delta/\theta)$ in A/θ.

Now, the *commutator* of α, β, denoted by $[\alpha, \beta]$, is the smallest congruence δ such that $C(\alpha, \beta; \delta)$ (the definition makes sense thanks to (C1)). From (C2) follows that $[\alpha, \beta] \le \alpha \wedge \beta$. Finally, a congruence α is called

- *abelian* if $C(\alpha, \alpha; 0_A)$, i.e., if $[\alpha, \alpha] = 0_A$,
- *central* if $C(\alpha, 1_A; 0_A)$, i.e., if $[\alpha, 1_A] = 0_A$.

Subsequently, the *center* of A, denoted by ζ_A, is the largest congruence of A such that $C(\zeta_A, 1_A; 0_A)$. Hence, $[\alpha, 1_A]$ is the smallest congruence δ such that $\alpha/\delta \le \zeta_{A/\delta}$. Similarly, $[\alpha, \alpha]$ is the smallest congruence δ such that α/δ is an abelian congruence of A/δ.

The following lemma resembles the second isomorphism theorem for groups, and will be used later in induction arguments.

Lemma 4.3. *Let A be an algebraic structure, and $\theta \le \alpha \le \beta$ its congruences. Then β/α is central* (*resp. abelian*) *in A/α if and only if $(\beta/\theta)/(\alpha/\theta)$ is central* (*resp. abelian*) *in $(A/\theta)/(\alpha/\theta)$.*

Proof. In the case of centrality, using (C3) repetitively, we obtain

$$\begin{aligned} &C(\beta/\alpha, 1_{A/\alpha}; 0_{A/\alpha}) \text{ in } A/\alpha \\ &\quad \Leftrightarrow\ C(\beta, 1_A; \alpha) \text{ in } A \\ &\quad \Leftrightarrow\ C(\beta/\theta, 1_{A/\theta}; \alpha/\theta) \text{ in } A/\theta \\ &\quad \Leftrightarrow\ C\big((\beta/\theta)/(\alpha/\theta), 1_{(A/\theta)/(\alpha/\theta)}; 0_{(A/\theta)/(\alpha/\theta)}\big) \text{ in } (A/\theta)/(\alpha/\theta). \end{aligned}$$

A similar argument works for abelianness, too. □

An algebraic structure A is called *abelian* if $\zeta_A = 1_A$, or, equivalently, if the congruence 1_A is abelian. It is called *nilpotent* (resp. *solvable*) if and only if there is a chain of congruences

$$0_A = \alpha_0 \le \alpha_1 \le \cdots \le \alpha_n = 1_A$$

such that α_{i+1}/α_i is a central (resp. abelian) congruence of A/α_i, for all $i \in \{0, 1, \ldots, n-1\}$. The length of the smallest such series is called the *length* of nilpotence (resp. solvability).

Similarly to group theory, one can define the series

$$\gamma_0 = 1_A, \qquad \gamma_{i+1} = [\gamma_i, 1_A],$$

and

$$\gamma^0 = 1_A, \qquad \gamma^{i+1} = [\gamma^i, \gamma^i],$$

and prove that an algebraic structure A is nilpotent (resp. solvable) of length n if and only if $\gamma_n = 0_A$ (resp. $\gamma^n = 0_A$). Note that both definitions use a special type of commutators: nilpotence uses commutators $[\alpha, 1_A]$, solvability uses commutators $[\alpha, \alpha]$.

In groups, the commutator and the corresponding notions of abelianness and centrality coincide with the classical terminology. In loops, the situation is more complicated [**45**]. In a wider setting, the commutator behaves well in all congruence-modular varieties [**26**]; for example, it is commutative (note that its definition is asymmetric with respect to α, β). For racks, the commutator in general lacks many desired properties, such as commutativity (Proposition 5.5 and Example 5.6), nevertheless, the notions of abelianness and centrality seem to have a very good meaning.

We also point out that there is no general principle providing a natural generating set for the congruence commutator, such as the element-wise commutators in groups. Analogies are known in several special cases, including loops [**45**] and quasigroups [**5**].

5. The commutator in racks.

5.1. From universal algebra to racks.

The crucial fact is that in racks, or more generally, in ltt left quasigroups, the centralizing relation for congruences is related to the properties of the corresponding relative displacement groups.

Lemma 5.1. *Let Q be a left quasigroup, α, β its congruences, and consider the following conditions*:

(1) $C(\alpha, \beta; 0_Q)$;

(2) $[\mathrm{Dis}_\alpha, \mathrm{Dis}_\beta] = 1$ *and* Dis_β *acts α-semiregularly on Q.*

Then (1) *implies* (2), *and if Q is an ltt left quasigroup then* (2) *implies* (1).

Proof. (1) $\Rightarrow$ (2). For the first property, it is sufficient to show that generators of the groups Dis_α and Dis_β commute. Let $a\,\alpha\, b$ and $c\,\beta\, d$. Let $f = L_{u_1}^{k_1}\cdots L_{u_m}^{k_m}$ and $g = L_{v_1}^{l_1}\cdots L_{v_n}^{l_n}$ be elements of $\mathrm{LMlt}(Q)$. We want to show that

$$(fL_aL_b^{-1}f^{-1})(gL_cL_d^{-1}g^{-1}) = (gL_cL_d^{-1}g^{-1})(fL_aL_b^{-1}f^{-1}).$$

Denote by Y the formal expression $L_{y_1}^{k_1}\cdots L_{y_m}^{k_m}$, and Z the formal expression $L_{z_1}^{l_1}\cdots L_{z_n}^{l_n}$, with inverses defined accordingly, and consider the $(m+n+5)$-ary term

$$t(x_0, x_1, x_2, x_3, x_4, \bar{y}, \bar{z}) = ZL_{x_2}L_{x_3}^{-1}Z^{-1}YL_{x_0}L_{x_1}^{-1}Y^{-1}ZL_{x_3}L_{x_2}^{-1}Z^{-1}(x_4).$$

Then, for any $e \in Q$, we have

$$\begin{aligned} t^Q(b, b, c, d, e, \bar{u}, \bar{v}) &= gL_cL_d^{-1}g^{-1}fL_bL_b^{-1}f^{-1}gL_dL_c^{-1}g^{-1}(e) \\ &= e \\ &= gL_cL_c^{-1}g^{-1}fL_bL_b^{-1}f^{-1}gL_cL_c^{-1}g^{-1}(e) = t^Q(b, b, c, c, e, \bar{u}, \bar{v}). \end{aligned}$$

Using $TC(t, \alpha, \beta, 0_Q)$, we replace a for b and obtain

$$\begin{aligned} t^Q(a, b, c, d, e, \bar{u}, \bar{v}) &= gL_cL_d^{-1}g^{-1}fL_aL_b^{-1}f^{-1}gL_dL_c^{-1}g^{-1}(e) \\ &= gL_cL_c^{-1}g^{-1}fL_aL_b^{-1}f^{-1}gL_cL_c^{-1}g^{-1}(e) = t^Q(a, b, c, c, e, \bar{u}, \bar{v}). \end{aligned}$$

By all possible choices of e we obtain

$$gL_cL_d^{-1}g^{-1}fL_aL_b^{-1}f^{-1}gL_dL_c^{-1}g^{-1} = fL_aL_b^{-1}f^{-1},$$

which was our goal.

Next, we show the semiregularity property. Lemma 3.1 says that Dis_β consists of all mappings $L_{a_n}^{k_n}\cdots L_{a_1}^{k_1}L_{b_1}^{-k_1}\cdots L_{b_n}^{-k_n}$ such that $k_i \in \{\pm 1\}$ and $a_i\,\beta\,b_i$ for all $i = 1,\dots,n$. Given a mapping $g \in \mathrm{Dis}_\beta$ in this form, consider the $(2n+1)$-ary term

$$t(x_0,x_1,\dots,x_{2n}) = L_{x_n}^{k_n}\cdots L_{x_1}^{k_1}L_{x_{n+1}}^{-k_1}\cdots L_{x_{2n}}^{-k_n}(x_0).$$

Now, assume that for some $a \in Q$

$$t^Q(a,a_1,\dots,a_n,b_1,\dots,b_n) = g(a) = a = t^Q(a,a_1,\dots,a_n,a_1,\dots,a_n).$$

Using $TC(t,\alpha,\beta,0_Q)$, we can replace a for an arbitrary b such that $b\,\alpha\,a$ and obtain

$$t^Q(b,a_1,\dots,a_n,b_1,\dots,b_n) = g(b) = b = t^Q(b,a_1,\dots,a_n,a_1,\dots,a_n).$$

(2) ⇒ (1). It is sufficient to verify $TC(t,\alpha,\beta,0_Q)$ for every term

$$t(x_0,\dots,x_n) = L_{s_1(x_{i_1})}^{\varepsilon_1}\cdots L_{s_{m-1}(x_{i_{m-1}})}^{\varepsilon_{m-1}}(s_m(x_{i_m}))$$

as in (4.1). Without loss of generality, we can assume that x_0 occurs only once in t.

Consider $a\,\alpha\,b$ and $u_i\,\beta\,v_i$ for $i = 1,\dots,n$ and assume that $t^Q(a,u_1,\dots,u_n) = t^Q(a,v_1,\dots,v_n)$. The goal is to show that $t^Q(b,u_1,\dots,u_n) = t^Q(b,v_1,\dots,v_n)$. Observe that $s(u_i)\,\beta\,s(v_i)$ for every unary term s. We consider two cases.

Case 1: $0 = i_r$ for $r < m$. Consider the following two mappings which belong to Dis_β by Lemma 3.1:

$$\begin{aligned} g &= L_{s_{m-1}(u_{i_{m-1}})}^{-\varepsilon_{m-1}}\cdots L_{s_r(a)}^{-\varepsilon_r}\cdots L_{s_1(u_{i_1})}^{-\varepsilon_1}L_{s_1(v_{i_1})}^{\varepsilon_1}\cdots L_{s_r(a)}^{\varepsilon_r}\cdots L_{s_{m-1}(v_{i_{m-1}})}^{\varepsilon_{m-1}},\\ h &= L_{s_{m-1}(u_{i_{m-1}})}^{-\varepsilon_{m-1}}\cdots L_{s_r(b)}^{-\varepsilon_r}\cdots L_{s_1(u_{i_1})}^{-\varepsilon_1}L_{s_1(v_{i_1})}^{\varepsilon_1}\cdots L_{s_r(b)}^{\varepsilon_r}\cdots L_{s_{m-1}(v_{i_{m-1}})}^{\varepsilon_{m-1}}.\end{aligned}$$

The assumption is equivalent to $g(s_m(v_{i_m})) = s_m(u_{i_m})$, the goal is equivalent to $h(s_m(v_{i_m})) = s_m(u_{i_m})$. We prove that $g = h$, thus settling the goal:

$$\begin{aligned} g &= L_{s_{m-1}(u_{i_{m-1}})}^{-\varepsilon_{m-1}}\cdots L_{s_r(a)}^{-\varepsilon_r}\underbrace{\cdots L_{s_1(u_{i_1})}^{-\varepsilon_1}L_{s_1(v_{i_1})}^{\varepsilon_1}\cdots}_{\in\mathrm{Dis}_\beta}\underbrace{L_{s_r(a)}^{\varepsilon_r}L_{s_r(b)}^{\varepsilon_r}}_{\in\mathrm{Dis}_\alpha}L_{s_r(b)}^{-\varepsilon_r}\cdots L_{s_{m-1}(v_{i_{m-1}})}^{\varepsilon_{m-1}}\\ &= L_{s_{m-1}(u_{i_{m-1}})}^{-\varepsilon_{m-1}}\cdots L_{s_r(a)}^{-\varepsilon_r}\underbrace{L_{s_r(a)}^{\varepsilon_r}L_{s_r(b)}^{\varepsilon_r}}_{\in\mathrm{Dis}_\alpha}\underbrace{\cdots L_{s_1(u_{i_1})}^{-\varepsilon_1}L_{s_1(v_{i_1})}^{\varepsilon_1}\cdots}_{\in\mathrm{Dis}_\beta}L_{s_r(b)}^{-\varepsilon_r}\cdots L_{s_{m-1}(v_{i_{m-1}})}^{\varepsilon_{m-1}} = h,\end{aligned}$$

using Lemma 3.1 and the assumption that $[\mathrm{Dis}_\alpha,\mathrm{Dis}_\beta] = 1$ to commute the two underbraced mappings.

Case 2: $0 = i_m$, i.e., the variable x_0 is the rightmost variable of t. Similarly, consider the mapping

$$g = L^{-\varepsilon_{m-1}}_{s_{m-1}(u_{i_{m-1}})} \cdots L^{-\varepsilon_1}_{s_1(u_{i_1})} L^{\varepsilon_1}_{s_1(v_{i_1})} \cdots L^{\varepsilon_{m-1}}_{s_{m-1}(v_{i_{m-1}})} \in \mathrm{Dis}_\beta.$$

The assumption is equivalent to $g(s_m(a)) = s_m(a)$, the goal is equivalent to $g(s_m(b)) = s_m(b)$. Since $a\,\alpha\,b$, then also $s_m(a)\,\alpha\,s_m(b)$, and we can apply α-semiregularity of Dis_β to finish the case. □

Now, it becomes easy to characterize the commutator in ltt left quasigroups by properties of the corresponding subgroups.

Proposition 5.2. *Let Q be an ltt left quasigroup and let α, β be its congruences. Then $[\alpha, \beta]$ is the smallest congruence δ such that $[\mathrm{Dis}_{\alpha/\delta}, \mathrm{Dis}_{\beta/\delta}] = 1$ and $\mathrm{Dis}_{\beta/\delta}$ acts α/δ-semiregularly on Q/δ.*

Equivalently, we could state the former condition as $[\mathrm{Dis}_\alpha, \mathrm{Dis}_\beta] \leq \mathrm{Dis}^\delta$.

Proof. Since $[\alpha, \beta] \leq \alpha \wedge \beta$, we can assume that $\delta \leq \alpha \wedge \beta$. Using observation (C3) for $\theta = \delta$, we obtain that $C(\alpha, \beta; \delta)$ if and only if $[\mathrm{Dis}_{\alpha/\delta}, \mathrm{Dis}_{\beta/\delta}] = 1$ and $\mathrm{Dis}_{\beta/\delta}$ acts α/δ-semiregularly on Q/δ. □

While our characterization is not convenient to calculate the actual value of the commutator in general, it is useful in the derived concepts of abelianness and centrality, since they require the commutator to be zero. Using Proposition 5.2 with $\beta = \alpha$ (resp. $\beta = 1_Q$) and $\delta = 0$, we immediately obtain one of our main results, Theorem 1.1.

5.2. Commutator in faithful quandles.

In general, the semiregularity condition in Proposition 5.2 is necessary (even in the special case $\alpha = \beta = 1_Q$ defining abelianness, see [**33**]). However, for faithful quandles, semiregularity follows from the commutativity condition, and the characterization of $C(\alpha, \beta; \delta)$ simplifies.

Lemma 5.3. *Let Q be a faithful quandle, α its congruence and $N \leq \mathrm{Dis}(Q)$. If $[N, \mathrm{Dis}_\alpha] = 1$, then N acts α-semiregularly on Q.*

Proof. Consider $h \in N$ and $a \in Q$ such that $h(a) = a$. Take any $b\,\alpha\,a$. Then

$$\begin{aligned} L_b &= L_b L_a^{-1} L_a = L_b L_a^{-1} L_{h(a)} \\ &= \underbrace{L_b L_a^{-1}}_{\in \mathrm{Dis}_\alpha} \underbrace{h}_{\in N} L_a h^{-1} = \underbrace{h}_{\in N} \underbrace{L_b L_a^{-1}}_{\in \mathrm{Dis}_\alpha} L_a h^{-1} = h L_b h^{-1} = L_{h(b)}. \end{aligned}$$

Since Q is faithful, we obtain that $h(b) = b$. □

Corollary 5.4. *Let Q be a faithful quandle and α its congruence. Then*

(1) *α is abelian if and only if Dis_α is abelian.*

(2) *α is central if and only if Dis_α is central in $\mathrm{Dis}(Q)$.*

For general commutator, we must assume that every factor is faithful, so that we can properly use Corollary 5.4. This assumption holds, for example, in every finite latin quandle, or in every quandle that has CDSg.

Proposition 5.5. *Let Q be a quandle such that every factor of Q is faithful, and let α, β be its congruences. Then*

$$[\alpha,\beta]=[\beta,\alpha]=\mathrm{con}_{[\mathrm{Dis}_\alpha,\mathrm{Dis}_\beta]}=\mathcal{O}_{[\mathrm{Dis}_\alpha,\mathrm{Dis}_\beta]}.$$

Proof. Proposition 5.2 and Lemma 5.3 apply to every triple of congruences, since every factor of Q is faithful. Hence $[\alpha,\beta]$ is the smallest congruence δ such that $[\mathrm{Dis}_\alpha,\mathrm{Dis}_\beta]\leq \mathrm{Dis}^\delta$ and we see that the commutator is commutative.

Let $\omega=\mathrm{con}_{[\mathrm{Dis}_\alpha,\mathrm{Dis}_\beta]}$. Proposition 3.5(1) for $N=[\mathrm{Dis}_\alpha,\mathrm{Dis}_\beta]$ says that $[\mathrm{Dis}_\alpha,\mathrm{Dis}_\beta]\leq \mathrm{Dis}^\omega$. Now consider any congruence δ satisfying $[\mathrm{Dis}_\alpha,\mathrm{Dis}_\beta]\leq \mathrm{Dis}^\delta$. Since the operator con is monotone, we have $\omega\leq \mathrm{con}_{\mathrm{Dis}^\delta}=\delta$ by Proposition 3.7. Hence $[\alpha,\beta]=\omega$.

Let $\gamma=\mathcal{O}_N$. Then according to Lemma 2.4 then $N\leq \mathrm{Dis}^\gamma$ and so $C(\alpha,\beta,\gamma)$ holds. Then $[\alpha,\beta]=\mathrm{con}_N\leq\gamma$. Hence by Proposition 3.5(4), the equality holds. □

In general, the commutator is not commutative, not even in the special case $[\alpha,1_Q]$. Indeed, the Cayley kernel causes troubles.

Example 5.6. On one hand, $[\alpha,\lambda_Q]=0_Q$ in every quandle and for every α, since $\mathrm{Dis}_{\lambda_Q}=1$ and it satisfies the conditions of Lemma 5.1 trivially. In particular $[1_Q,\lambda_Q]=0_Q$. There are examples of non-faithful connected quandles where $[\lambda_Q,1_Q]\neq 0_Q$, that is, where $\mathrm{Dis}(Q)$ does not act λ_Q-semiregularly, such as SmallQuandle(30,4), (36,58) and (45,29) in the RIG library.

5.3. The center of a rack.

We will use Theorem 1.1 to calculate the center of a rack. One natural property to expect is that every central pair *mediates* with all other pairs, i.e., if $a\,\zeta_Q\,b$ then $(u*a)*(b*v)=(u*b)*(a*v)$ for every u,v. (A rack is medial if and only if all pairs mutually mediate.)

Lemma 5.7. *Let Q be a rack. Then*

$$\mathrm{con}_{Z(\mathrm{Dis}(Q))}=\{(a,b):\ (u*a)*(b*v)=(u*b)*(a*v)\ \textit{for every}\ u,v\in Q\}.$$

Proof. Observe that $(u*a)*(b*v)=(u*b)*(a*v)$ for every u,v if and only if $L_{u*a}L_b=L_{u*b}L_a$ for every u, which is equivalent to

$$L_aL_u^{-1}L_b=L_bL_u^{-1}L_a \qquad (\dagger)$$

using equation (2.2).

($\subseteq$) If $a\,\mathrm{con}_{Z(\mathrm{Dis}(Q))}\,b$, then $L_bL_a^{-1}\in Z(\mathrm{Dis}(Q))$, and thus $L_aL_u^{-1}L_bL_a^{-1}=L_bL_a^{-1}L_aL_u^{-1}=L_bL_u^{-1}$ for every u, and (†) follows immediately.

($\supseteq$) First note that (†) is equivalent to $L_u^{-1}L_aL_b^{-1}=L_b^{-1}L_aL_u^{-1}$. Now, use this identity and its inverse to conclude that $L_uL_v^{-1}L_aL_b^{-1}=L_uL_b^{-1}L_aL_v^{-1}=L_aL_b^{-1}L_uL_v^{-1}$ for every u,v. □

To handle the semiregularity condition, we define an equivalence σ_Q on Q by

$$a\,\sigma_Q\,b \;\Leftrightarrow\; \mathrm{Dis}(Q)_a = \mathrm{Dis}(Q)_b.$$

Here $\mathrm{Dis}(Q)_x$ denotes the stabilizer of x in $\mathrm{Dis}(Q)$.

Lemma 5.8. *Let Q be a rack. Then $\mathrm{Dis}(Q)$ acts α-semiregularly on Q if and only if $\alpha \le \sigma_Q$.*

Proof. By definition, $\mathrm{Dis}(Q)$ acts α-semiregularly on Q if and only if $f(a) = a \Leftrightarrow f(b) = b$ for every $f \in \mathrm{Dis}(Q)$ and every $a\,\alpha\,b$. This is equivalent to saying that the stabilizers $\mathrm{Dis}(Q)_a$ and $\mathrm{Dis}(Q)_b$ coincide for every $a\,\alpha\,b$, which is equivalent to $\alpha \le \sigma_Q$. □

Proposition 5.9. *Let Q be a rack. Then $\zeta_Q = \mathrm{con}_{Z(\mathrm{Dis}(Q))} \cap \sigma_Q$.*

Proof. Let $\xi = \mathrm{con}_{Z(\mathrm{Dis}(Q))} \cap \sigma_Q$. First, we prove that ξ is a congruence of Q. It is an intersection of two equivalences, hence it is an equivalence. Let $a\,\xi\,b$ and $c \in Q$. Since $\mathrm{con}_{Z(\mathrm{Dis}(Q))}$ is a congruence, it remains to prove that $(c*a)\,\sigma_Q\,(c*b)$ and $(a*c)\,\sigma_Q\,(b*c)$ (for left division, the proof is analogical). For the former claim, assume that $f(c*a) = c*a$, $f \in \mathrm{Dis}(Q)$, or equivalently, $L_c^{-1} f L_c(a) = a$. Since $L_c^{-1} f L_c \in \mathrm{Dis}(Q)$ and $a\,\sigma_Q\,b$, we have $L_c^{-1} f L_c(b) = b$, and thus $f(c*b) = c*b$. For the latter claim, assume that $f(a*c) = a*c$, $f \in \mathrm{Dis}(Q)$, or equivalently, $L_a^{-1} f L_a(c) = c$. Then

$$L_b^{-1} f L_b(c) = L_b^{-1} f \underbrace{L_b L_a^{-1}}_{\in Z(\mathrm{Dis}(Q))} L_a(c) = L_b^{-1} \underbrace{L_b L_a^{-1}}_{\in Z(\mathrm{Dis}(Q))} f L_a(c) = L_a^{-1} f L_a(c) = c,$$

and thus $f(b*c) = b*c$. We used the assumption that $a\,\mathrm{con}_{Z(\mathrm{Dis}(Q))}\,b$, which means that $L_b L_a^{-1} \in Z(\mathrm{Dis}(Q))$.

In the next step, we show that every central congruence α is contained in ξ. Indeed, by Theorem 1.1, $\mathrm{Dis}_\alpha \le Z(\mathrm{Dis}(Q))$, hence $\alpha \le \mathrm{con}_{\mathrm{Dis}_\alpha} \le \mathrm{con}_{Z(\mathrm{Dis}(Q))}$ using Proposition 3.6 (the first inequality follows from the closure property, the second inequality from monotonicity). Lemma 5.8 assures that $\alpha \le \sigma_Q$.

Finally, we verify that ξ is a central congruence. To show that Dis_ξ is central in $\mathrm{Dis}(Q)$, it is sufficient to look at the generators $L_a L_b^{-1}$, $a\,\xi\,b$. Then $a\,\mathrm{con}_{Z(\mathrm{Dis}(Q))}\,b$, hence $L_a L_b^{-1} \in Z(\mathrm{Dis}(Q))$. Since $\xi \le \sigma_Q$, Lemma 5.8 assures that $\mathrm{Dis}(Q)$ acts ξ-regularly. □

Corollary 5.10. *Let Q be a faithful quandle. Then $\zeta_Q = \mathrm{con}_{Z(\mathrm{Dis}(Q))}$.*

Proof. Let Q be faithful. We prove that $\mathrm{con}_{Z(\mathrm{Dis}(Q))} \le \sigma_Q$. By Lemma 5.8, we shall prove that $\mathrm{Dis}(Q)$ acts $\mathrm{con}_{Z(\mathrm{Dis}(Q))}$-semiregularly on Q. We have

$$\big[\mathrm{Dis}(Q), \mathrm{Dis}_{\mathrm{con}_{Z(\mathrm{Dis}(Q))}}\big] \le \big[\mathrm{Dis}(Q), Z(\mathrm{Dis}(Q))\big] = 1,$$

and thus semiregularity follows from Lemma 5.3. □

Corollary 5.11. *Let Q be a medial rack. Then $\zeta_Q = \sigma_Q$.*

Proof. If Q is medial, then $\mathrm{Dis}(Q)$ is abelian, and thus $\mathrm{con}_{Z(\mathrm{Dis}(Q))} = 1_Q$. □

5.4. The $\mathcal{O}_N$ and λ_Q congruences.

Lemma 5.12. *Let Q be a rack and $N \in \mathrm{Norm}(Q)$ abelian (resp. central in $\mathrm{Dis}(Q)$). Then $\mathcal{O}_N$ is an abelian (resp. central) congruence of Q. In particular $Z(\mathrm{Dis}(Q)) \leq \mathrm{Dis}^{\zeta_Q}$.*

Proof. According to Theorem 1.1, we need to check that $\mathrm{Dis}_{\mathcal{O}_N}$ is abelian (resp. central in $\mathrm{Dis}(Q)$) and that $\mathrm{Dis}_{\mathcal{O}_N}$ (resp. $\mathrm{Dis}(Q)$) acts $\mathcal{O}_N$-semiregularly on Q.

First, observe that $\mathrm{Dis}_{\mathcal{O}_N} \leq N$. By Proposition 3.5(4), $\mathcal{O}_N \leq \mathrm{con}_N$, and applying the Galois connection we obtain $\mathrm{Dis}_{\mathcal{O}_N} \leq \mathrm{Dis}_{\mathrm{con}_N} \leq N$.

Consequently, $\mathrm{Dis}_{\mathcal{O}_N}$ is abelian (resp. central in $\mathrm{Dis}(Q)$), since so is N. Let $f \in \mathrm{Dis}_{\mathcal{O}_N}$ (resp. $f \in \mathrm{Dis}(Q)$) and consider $a \in Q$ such that $f(a) = a$. For any $b \, \mathcal{O}_N \, a$, take $g \in N$ such that $b = g(a)$. Then $f(b) = f(g(a)) = g(f(a)) = g(a) = b$, where $fg = gf$ follows from abelianness (resp. centrality) of N.

In particular $\mathcal{O}_{Z(\mathrm{Dis}(Q))} \leq \zeta_Q$, so using Lemma 2.4 $Z(\mathrm{Dis}(Q)) \leq \mathrm{Dis}^{\zeta_Q}$. □

Proposition 5.13. *Medial racks are nilpotent of length at most 2.*

Proof. If Q is a medial rack, then $\mathrm{Dis}(Q)$ is abelian, and the chain $0_Q \leq \mathcal{O}_Q \leq 1_Q$ is a witness. The congruence $\mathcal{O}_Q$ is central by Lemma 5.12 for $N = \mathrm{Dis}(Q)$. The factor $Q/\mathcal{O}_Q$ is a permutation rack, and thus abelian: for $[a], [b], [c] \in Q/\mathcal{O}_Q$, we have $[a] * [c] = [a * c] = [b * c] = [b] * [c]$, because $b * c = L_b L_a^{-1}(a * c)$. □

The Cayley kernel is always abelian: indeed, $\mathrm{Dis}_{\lambda_Q} = 1$, hence it is abelian and acts λ_Q-semiregularly. However, it may not be central.

Example 5.14. Consider the quandle Q with the multiplication table

$$\begin{array}{|cccc|}\hline 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ \hline \end{array}.$$

Indeed, $\mathrm{Dis}(Q) = \langle f \rangle$ where $f = (3\ 4)$, but it does not act λ_Q-semiregularly, since $f(1) = 1$, $1 \, \lambda_Q \, 3$ and $f(3) = 4$.

6. Nilpotent and solvable racks.

6.1. Nilpotence and solvability of racks, and of their associated groups.

The two lemmas below prove our second main result, Theorem 1.2. In the two proofs, let $\Gamma^{(n)}$ denote the n-th member of the derived series, and $\Gamma_{(n)}$ the n-th subgroup of the lower central series, of a given group. The subgroups $\Gamma^{(n)}$ and $\Gamma_{(n)}$ correspond to the group congruences γ^n and γ_n, respectively.

Lemma 6.1. *Let Q be a rack. If Q is nilpotent (resp. solvable) of length n, then $\mathrm{Dis}(Q)$ is a nilpotent (resp. solvable) group of length $\leq 2n - 1$.*

Proof. We proceed by induction on the length n. For $n = 1$, the rack Q is abelian, hence $\mathrm{Dis}(Q)$ is an abelian group and the statement holds. In the induction step, assume that the statement holds for all racks that are nilpotent (resp. solvable) of length $\leq n - 1$. Consider a chain of congruences

$$0_Q = \alpha_0 \leq \alpha_1 \leq \cdots \leq \alpha_n = 1_Q$$

such that α_{i+1}/α_i is central (resp. abelian) in Q/α_i, for every i. In particular, α_1 is central (resp. abelian) in Q and the rack Q/α_1 is nilpotent (resp. solvable) of length $n-1$, as witnessed by the series

$$0_{Q/\alpha_1} = \alpha_1/\alpha_1 \leq \alpha_2/\alpha_1 \leq \cdots \leq \alpha_n/\alpha_1 = 1_{Q/\alpha_1}$$

(see Lemma 4.3). By the induction assumption, $\mathrm{Dis}(Q/\alpha_1)$ is nilpotent (resp. solvable) of length $\leq 2n-3$. Now, consider the series $\Gamma_{(i)}$ (resp. $\Gamma^{(i)}$) in $\mathrm{Dis}(Q)$ and project it into $\mathrm{Dis}(Q/\alpha_1)$. Since $\pi_{\alpha_1}(\Gamma_{(2n-3)}) = 1$, we obtain that $\Gamma_{(2n-3)} \leq \mathrm{Ker}(\pi_{\alpha_1}) = \mathrm{Dis}^{\alpha_1}$ (resp. analogically for $\Gamma^{(2n-3)}$). Now, in case of nilpotence, we have

$$\begin{aligned}\Gamma_{(2n-1)} &= \big[[\Gamma_{(2n-3)}, \mathrm{Dis}(Q)], \mathrm{Dis}(Q)\big]\\ &\leq \big[[\mathrm{Dis}^{\alpha_1}, \mathrm{Dis}(Q)], \mathrm{Dis}(Q)\big] \leq [\mathrm{Dis}_{\alpha_1}, \mathrm{Dis}(Q)] = 1,\end{aligned}$$

using Proposition 3.3(1) in the penultimate step, and centrality of Dis_{α_1} (by Theorem 1.1) in the ultimate step. In case of solvability, we have

$$\begin{aligned}\Gamma^{(2n-1)} &= \big[[\Gamma^{(2n-3)}, \Gamma^{(2n-3)}], [\Gamma^{(2n-3)}, \Gamma^{(2n-3)}]\big]\\ &\leq \big[[\mathrm{Dis}^{\alpha_1}, \mathrm{Dis}^{\alpha_1}], [\mathrm{Dis}^{\alpha_1}, \mathrm{Dis}^{\alpha_1}]\big] \leq [\mathrm{Dis}_{\alpha_1}, \mathrm{Dis}_{\alpha_1}] = 1,\end{aligned}$$

using Proposition 3.3(1), and abelianness of Dis_{α_1}. □

The bound on the length is tight already for $n = 2$. For example, one can check in the RIG library that non-principal latin quandles of size 27 are nilpotent of length 2, but their displacement groups are nilpotent of length 3; and non-principal latin quandles of size 28 are solvable of length 2, but their displacement groups are solvable of length 3.

Lemma 6.2. *Let Q be a rack. If* $\mathrm{Dis}(Q)$ *is nilpotent* (*resp. solvable*) *of length n, then Q is nilpotent* (*resp. solvable*) *of length $\leq n+1$.*

Proof. We proceed by induction. For $n = 1$, the group $\mathrm{Dis}(Q)$ is abelian, and Proposition 5.13 assures that Q is nilpotent (and thus solvable, too) of length ≤ 2. In the induction step, assume that the statement holds for all racks with the displacement group nilpotent (resp. solvable) of length $\leq n-1$.

First, observe that, for any $N \in \mathrm{Norm}(Q)$, $\pi_{\mathcal{O}_N}(N) = 1$: indeed, for every $f \in N$ and $a \in Q$, we have $f(a)\, \mathcal{O}_N\, a$, hence f acts identically on $Q/\mathcal{O}_N$. Therefore, $N \leq \mathrm{Ker}(\pi_{\mathcal{O}_N}) = \mathrm{Dis}^{\mathcal{O}_N}$.

Now, take $N = \Gamma_{(n-1)}$ (resp. $N = \Gamma^{(n-1)}$). Since N is central (resp. abelian) in $\mathrm{Dis}(Q)$, the congruence $\mathcal{O}_N$ is also central (resp. abelian), by Lemma 5.12. From the observation we obtain that $N \leq \mathrm{Dis}^{\mathcal{O}_N}$. Therefore, the group $\mathrm{Dis}(Q/\mathcal{O}_N) \simeq \mathrm{Dis}(Q)/\mathrm{Dis}^{\mathcal{O}_N}$ is nilpotent (resp. solvable) of length $\leq n-1$, and by the induction assumption, $Q/\mathcal{O}_N$ is nilpotent (resp. solvable) of length $m \leq n$. Let

$$0_{Q/\mathcal{O}_N} = \mathcal{O}_N/\mathcal{O}_N \leq \alpha_1/\mathcal{O}_N \leq \cdots \leq \alpha_m/\mathcal{O}_N = 1_{Q/\mathcal{O}_N}$$

be the chain of congruences that witnesses nilpotence (resp. solvability). Then the chain

$$0_Q \leq \mathcal{O}_N \leq \alpha_1 \leq \cdots \leq \alpha_m = 1_Q$$

witnesses that Q is nilpotent (resp. solvable) of length $\leq n+1$, using Lemma 4.3. □

The bound on the length is tight already for $n=1$. For example, the 3-element quandle with two orbits has an abelian displacement group, but its action is not semiregular, hence Q cannot be abelian [**33**].

According to [**43**], finite (left and right) distributive quasigroups have nilpotent displacement groups, so we have the following corollary.

Corollary 6.3. *Finite distributive quasigroups are nilpotent.*

6.2. Prime decomposition for nilpotent quandles.

Theorem 1.2 allows to transfer certain properties from groups to racks.

Proposition 6.4. *Every subquandle and every quotient of a nilpotent (resp. solvable) quandle is nilpotent (resp. solvable). The direct product of finitely many nilpotent (resp. solvable) quandles is nilpotent (resp. solvable).*

Proof. Let Q be a nilpotent (resp. solvable) quandle. By Theorem 1.2, the group $\mathrm{Dis}(Q)$ is nilpotent (resp. solvable).

Consider a subquandle S of Q, and let $H = \langle L_a L_b^{-1} : \ a,b \in S\rangle \leq \mathrm{Dis}(Q)$. Then H is nilpotent (resp. solvable), and $H \to \mathrm{Dis}(S)$, $h \mapsto h|_S$, is a surjective group homomorphism. Hence $\mathrm{Dis}(S)$ is nilpotent (resp. solvable), and so is S by Theorem 1.2.

Consider a congruence α of Q. Then $\pi_\alpha : \mathrm{Dis}(Q) \to \mathrm{Dis}(Q/\alpha)$ is a surjective group homomorphism. Hence $\mathrm{Dis}(Q/\alpha)$ is nilpotent (resp. solvable), and so is Q/α by Theorem 1.2.

Let $\{Q_i : 1 \leq i \leq n\}$ be a set of quandles, $Q = \prod_{i=1}^n Q_i$ and let α_i be the kernel of the canonical mapping $Q \to Q_i$. Then $\bigcap_{i=1}^n \mathrm{Dis}^{\alpha_i} = 1$ and so the group homomorphism

$$\mathrm{Dis}(Q) \longrightarrow \prod_{i=1}^n \mathrm{Dis}(Q_i), \quad h \mapsto (\pi_{\alpha_1}(h), \ldots, \pi_{\alpha_n}(h))$$

is injective. Using again Theorem 1.2, if the quandles $\{Q_i : 1 \leq i \leq n\}$ are nilpotent (resp. solvable), then so it is $\prod_{i=1}^n \mathrm{Dis}(Q_i)$. Hence $\mathrm{Dis}(Q)$ is nilpotent (resp. solvable) and so it is Q. □

The following fact was proved in Bianco's PhD thesis [**7**]. For reader's convenience, we include his proof.

Proposition 6.5 ([**7**, Corollary 5.2]). *Let Q be a connected rack of prime power size p^k. Then* $\mathrm{Dis}(Q)$ *is a p-group.*

Proof. According to [**22**, Theorem A.2], if G is a finite group, C a conjugacy class of prime power size p^n and $G = \langle C\rangle$, then $G/O_p(G)$ is cyclic, where $O_p(G)$ denotes the p-core of G. In particular, set $G = \mathrm{LMlt}(Q)$ and $C = \{L_a : a \in Q\}$. By [**2**, Lemma 1.29], $|C|$ divides $|Q|$, hence it is a prime power, and thus $G/O_p(G)$ is cyclic.

Therefore, $G' \leq O_p(G)$ is a p-group. According to [**31**, Proposition 3.2], $G' = \mathrm{Dis}(Q)$ for connected quandles. □

An immediate consequence of Proposition 6.5 and Theorem 1.2 is that connected racks of prime power size are nilpotent. Now, we are ready to prove the third main result, Theorem 1.4, about the primary decomposition of nilpotent quandles.

Proof of Theorem 1.4. ($\Leftarrow$) Connected quandles of prime power size are nilpotent, and their product is nilpotent, too, by Proposition 6.4.

($\Rightarrow$) The proof is based on the minimal representation of connected quandles, see [**31**, Section 4] for all undefined notions. According to [**35**, Theorem 7.1] or [**31**, Proposition 3.5], every connected quandle Q is isomorphic to the coset quandle $\mathcal{Q}_{\mathrm{Hom}}(\mathrm{Dis}(Q), \mathrm{Dis}(Q)_e, \widehat{L}_e)$ where $e \in Q$ is chosen arbitrarily and $\widehat{L}_e$ denotes the inner automorphism given by L_e. Since Q is faithful, $\mathrm{Dis}(Q)_e = \mathrm{Fix}(\widehat{L}_e)$, the set of fixed points of $\widehat{L}_e$: indeed, for $g \in \mathrm{Dis}(Q)$, we have $L_e g = g L_e$ if and only if $e * g(a) = g(e * a) = g(e) * g(a)$ for every $a \in Q$, which is equivalent to $L_e = L_{g(e)}$, which in turn is equivalent to $g(e) = e$ by faithfulness.

Now, if Q is nilpotent, then so is $\mathrm{Dis}(Q)$, and it decomposes as the direct product of its Sylow subgroups, $\mathrm{Dis}(Q) \simeq \prod S_p$, where S_p is the p-Sylow subgroup of $\mathrm{Dis}(Q)$. Sylow subgroups are invariant under automorphisms of $\mathrm{Dis}(Q)$, therefore $\widehat{L}_e$ decomposes as the product of the restrictions of $\widehat{L_e}$ to the Sylow subgroup, and the subgroup $\mathrm{Fix}(\widehat{L}_e)$ decomposes, too. Therefore,

$$Q \simeq \mathcal{Q}_{\mathrm{Hom}}\Big(\prod S_p, \prod \mathrm{Fix}(\widehat{L}_e|_{S_p}), \prod \widehat{L}_e|_{S_p}\Big) \simeq \prod \mathcal{Q}_{\mathrm{Hom}}\big(S_p, \mathrm{Fix}(\widehat{L}_e|_{S_p}), \widehat{L}_e|_{S_p}\big),$$

which is a product of connected quandles of prime power size. □

7. Abelian and central extensions.

7.1. Constructing extensions.

Let Q be a left quasigroup, A an abelian group and ϕ, ψ, θ mappings

$$\phi : Q \times Q \to \mathrm{End}(A), \quad \psi : Q \times Q \to \mathrm{Aut}(A), \quad \theta : Q \times Q \to A. \tag{7.1}$$

Define an operation on the set $Q \times A$ by

$$(a, s) * (b, t) = (a * b, \phi_{a,b}(s) + \psi_{a,b}(t) + \theta_{a,b}),$$

for every $a, b \in Q$ and $s, t \in A$. The resulting left quasigroup

$$Q \times_{\phi,\psi,\theta} A = (Q \times A, *, \backslash)$$

will be called an *abelian extension* of Q by the triple (ϕ, ψ, θ). If ϕ, ψ are constant mappings, we will say that $Q \times_{\phi,\psi,\theta} A$ is a *central extension* of Q. The mapping $Q \times_{\phi,\psi,\theta} A \to Q$, $(a, s) \mapsto a$, is a homomorphism, called *canonical projection.* (Our terminology is justified by Propositions 7.5, 7.8 and Remark 7.10.)

Lemma 7.1. *Let Q be a rack, A an abelian group and ψ, ϕ, θ as in* (7.1). *Then the abelian extension $E = Q \times_{\phi,\psi,\theta} A$ is a rack if and only if*

$$\psi_{a,b*c}(\theta_{b,c}) + \theta_{a,b*c} = \psi_{a*b,a*c}(\theta_{a,c}) + \phi_{a*b,a*c}(\theta_{a,b}) + \theta_{a*b,a*c}, \tag{7.2}$$

$$\psi_{a,b*c}\psi_{b,c} = \psi_{a*b,a*c}\psi_{a,c}, \tag{7.3}$$

$$\psi_{a,b*c}\phi_{b,c} = \phi_{a*b,a*c}\psi_{a,b}, \tag{7.4}$$

$$\phi_{a,b*c} = \phi_{a*b,a*c}\phi_{a,b} + \psi_{a*b,a*c}\phi_{a,c} \tag{7.5}$$

for every $a, b, c \in Q$. The extension E is a quandle if and only if, additionally, Q is a quandle and

$$\theta_{a,a} = 0 \quad \text{and} \quad \phi_{a,a} + \psi_{a,a} = 1. \tag{7.6}$$

Proof. Straightforward computation (see also [**2**, Section 2]). □

The concept of abelian extensions for racks appeared in [**2**, Section 2.3] in the following terminology. A triple (A, ϕ, ψ) satisfying (7.3), (7.4), (7.5) is called a *Q-module*; it is called a *quandle Q-module* if it also satisfies (7.6). Then, a mapping θ satisfying (7.2) is called a *2-cocycle* over the Q-module, and the extension $Q \times_{\phi,\psi,\theta} A$ is called an *affine module over Q*. The expression

$$\beta_{a,b}(s,t) = \phi_{a,b}(s) + \psi_{a,b}(t) + \theta_{a,b}$$

defines a *dynamical cocycle*. Therefore, the concept of abelian extensions is a special case of the general concept of *extensions by dynamical cocycles*, denoted $Q \times_\beta A$, where the operation on $Q \times A$ is defined by $(a,s) * (b,t) = (a * b, \beta_{a,b}(s,t))$ for some dynamical cocycle β. Extensions by dynamical cocycles capture precisely homomorphisms with uniform kernels [**2**, Corollary 2.5].

Example 7.2. A surjective homomorphism $E \to Q$ whose kernel is contained in λ_E is often called shortly a *covering* of Q [**20**]. As noted in Section 5.4, the kernel of a covering is always abelian, but not necessarily central. Uniform coverings can be represented as *extensions by constant cocycles* [**2**, Proposition 2.11]. Central extensions with $\varphi_{a,b} = 0$ and $\psi_{a,b} = 1$ are special cases that were studied extensively in [**18**], [**19**] under the name "abelian extensions". The relation of various types of coverings to general universal algebraic concepts is the topic of our subsequent paper [**11**].

Example 7.3. The *semiregular extensions* $\mathrm{Ext}(A, f, d_a : a \in A)$ from [**33**] are special cases of central extensions where Q is a projection quandle, $\phi_{a,b} = 1 - f$, $\psi_{a,b} = f$ and $\theta_{a,b} = d_a - d_b$. Semiregular extensions are proved to represent abelian quandles.

Example 7.4. *Galkin quandles* studied in [**15**], [**17**] are special cases of abelian extensions where $Q = \mathrm{Aff}(\mathbb{Z}_3, -1)$, A is an arbitrary abelian group, $u \in A$ and

$$\phi_{a,b} = \begin{cases} 2 & a = b \\ -1 & a \neq b \end{cases}, \quad \psi_{a,b} = -1, \quad \theta_{a,b} = \begin{cases} u & a + 2 = b \\ 0 & a + 2 \neq b \end{cases}.$$

In [**2**], [**14**], [**32**], abelian extensions are studied from the viewpoint of cohomology theory. In [**14**], they are used to construct knot invariants. Here we ask a different question: which surjective rack homomorphisms can be represented by abelian and central extensions? We start with an observation that the kernel of the canonical projection of an abelian (resp. central) extension is an abelian (resp. central) congruence.

Proposition 7.5. *Let $E = Q \times_{\phi,\psi,\theta} A$ be an abelian (resp. central) extension of a rack Q. Then the kernel of the canonical projection $E \to Q$ is an abelian (resp. central) congruence.*

Proof. The kernel congruence α is defined by $(a, s)\ \alpha\ (b, t)$ if and only if $a = b$. Using Theorem 1.1, it is sufficient to prove that Dis_α is abelian (resp. central) and acts α-semiregularly on E (resp. $\mathrm{Dis}(E)$ does). It is straightforward to calculate that

$$L_{(a,s)}L^{-1}_{(a,t)}(c, r) = (c, \phi_{a,a\backslash c}(s - t) + r).$$

We see that any two displacements $L_{(a,s)}L^{-1}_{(a,t)}$ and $L_{(b,r)}L^{-1}_{(b,u)}$ commute, and thus Dis_α is an abelian group. Let $h \in \mathrm{Dis}_\alpha$. Then $h(c, r) = (c, x_{h,c} + r)$ where $x_{h,c} \in A$ is an element which only depends on h and c. Hence, if $h(c, r) = (c, r)$, then $x_{h,c} = 0$, and thus $h(c, s) = (c, s)$ for every $s \in A$. Therefore, Dis_α acts α-semiregularly on E.

If ϕ and ψ are constant mappings, we have

$$\begin{aligned}
&L_{(a,s)}L^{-1}_{(a,t)}(d, r) = (d, \phi(s - t) + r),\\
&L_{(b,u)}L^{-1}_{(c,v)}(d, r) = (b \cdot (c\backslash d), \phi(u - v) + \theta_{b,c\backslash d} - \theta_{c,c\backslash d} + r).
\end{aligned}$$

We see that these mappings commute, hence Dis_α is central in $\mathrm{Dis}(Q)$. A similar argument shows that $\mathrm{Dis}(E)$ acts α-semiregularly on E. □

7.2. Representing by extensions.

Consider a surjective quandle homomorphism $f : E \to Q$. Equivalently, consider a quandle E and its congruence α, and put $Q = E/\alpha$. We will say that f (resp. α) *admits a representation* by an abelian or central extension if $E \simeq Q \times_{\phi,\psi,\theta} A$ for suitable A, ϕ, ψ, θ. Under which conditions do we obtain such a representation?

Indeed, the blocks of the kernel of f (resp. α itself) must have equal size, i.e., the congruence must be uniform (cf. Proposition 2.5). Another natural constraint was given in Proposition 7.5.

But there are more such examples. One sort of troubles comes from the following fact. The blocks of an abelian extension are subquandles which are affine, all of them over the same group. The blocks of a uniform abelian congruence are subquandles which are abelian. However, this is a weaker condition: according to [**33**, Theorem 2.2], abelian quandles embed into affine quandles, but they are not necessarily affine. And even if the blocks were affine, then not necessarily over the same abelian group.

Example 7.6. Let R be an abelian quandle which is not affine (e.g., the three-element quandle with two orbits). Then the congruence 1_R is uniform and abelian, but it does not admit a representation by an abelian extension. This can be turned into a proper uniform congruence by taking any direct product $Q \times R$.

Example 7.7. Let $(Q_i, *_i, \backslash_i)$, $i \in I$, be quandles with disjoint underlying sets. Put $Q = \bigcup Q_i$ and define an operation on Q by $a * b = a *_i b$ if both $a, b \in Q_i$, and $a * b = b$ otherwise; similarly for left division. It is straightforward to check that $(Q, *, \backslash)$ is a quandle, and if all Q_i are connected, they form the orbits of Q. Now, assume that all Q_i are affine. Then the congruence $\mathcal{O}_Q$ is abelian, since $\mathrm{Dis}_{\mathcal{O}_Q}$ is abelian and acts $\mathcal{O}_Q$-semiregularly on Q. But if they are affine over different groups, the congruence $\mathcal{O}_Q$ does not admit a representation by an abelian extension.

The former problem can be avoided by the assumption that the blocks are connected, since connected abelian quandles are affine by [**31**, Theorem 7.3]. For the latter problem, we need some homogeneity assumption. One natural condition is that Q/α is connected, which forces the blocks to be isomorphic by Proposition 2.5.

Finite latin quandles satisfy both assumptions for every congruence. Here are other examples: the RIG library contains non-latin quandles where all subquandles are connected, SmallQuandle(28,k) for $k = 3, 4, 5, 6$.

Now we prove a representation result for central congruences. Somewhat weaker assumptions are actually sufficient.

Proposition 7.8. *Let E be a quandle, and $N \in \mathrm{Norm}(E)$ central in $\mathrm{Dis}(E)$ such that $E/\mathcal{O}_N$ is connected. Then E is isomorphic to a central extension $E/\mathcal{O}_N \times_{\phi,\psi,\theta} A$ for some ϕ, ψ, θ.*

Proof. Denote $\alpha = \mathcal{O}_N$. According to Lemma 5.12, α is a central congruence, and so Dis_α is central and $\mathrm{Dis}(E)$ acts α-semiregularly on E by Theorem 1.1.

Pick $e \in E$. We define group operations on $[e]$ in the following way: for $a, b \in [e]$, take any $f \in \mathrm{Dis}(Q)$ such that $f(e) = a$, and let $a+b = f(b)$ and $-a = f^{-1}(e)$. The operations are well defined, since $\mathrm{Dis}(E)$ acts α-semiregularly: hence, if $f_1(e) = a = f_2(e)$, then f_1 and f_2 coincide on $[e]$, and thus $f_1(b) = f_2(b)$ and $f_1^{-1}(e) = f_2^{-1}(e)$.

First, observe that $A = ([e], +, -, e)$ is an abelian group. For associativity, take $a = f(e)$, $b = g(e)$ and $c = h(e)$ with $f, g, h \in \mathrm{Dis}(E)$ and calculate

$$a + (b + c) = f(b + c) = f(g(c)) = f(g(h(e))) = f(g(e)) + h(e) = f(b) + c = (a + b) + c.$$

For commutativity, take $a = f(e)$ and $b = g(e)$ with $f, g \in \mathrm{Dis}_\alpha$, and use commutativity of Dis_α to calculate

$$a + b = f(b) = f(g(e)) = g(f(e)) = g(a) = b + a.$$

Next, observe that L_e is its automorphism of A: for $a = f(e)$ and $b = g(e)$, we calculate

$$L_e(a) + L_e(b) = L_e f L_e^{-1}(e) + L_e g L_e^{-1}(e) = L_e f L_e^{-1} L_e g L_e^{-1}(e) = L_e(fg(e)) = L_e(a + b).$$

Finally, the subquandle $[e]$ is equal to $\mathrm{Aff}(A, L_e)$: for $a = f(e)$ and $b = g(e)$ with $f, g \in N$, we calculate

$$\begin{aligned} a - L_e(a) + L_e(b) &= f(e) - L_e f L_e^{-1}(e) + L_e g L_e^{-1}(e) = f L_e f^{-1} L_e^{-1} L_e g L_e^{-1}(e) \\ &= L_{f(e)} g(e) = a * b. \end{aligned}$$

For every block $[a]$ of α, consider $h_{[a]} \in \mathrm{Dis}(E)$ such that $h_{[a]}$ maps the block $[a]$ into the block $[e]$ (such mappings exist due to connectedness of E/α). Now, consider a dynamical cocycle

$$\beta_{[a],[b]}(s,t) = h_{[a*b]} L_{h_{[a]}^{-1}(s)} h_{[b]}^{-1}(t).$$

We will show that

$$\varphi : E \to E/\alpha \times_\beta A, \qquad a \mapsto ([a], h_{[a]}(a))$$

is an isomorphism. It is bijective, because the mappings $h_{[a]}$ are bijective on every block (cf. the proof of Proposition 2.5). For $a, b \in E$, we have

$$\begin{aligned}\varphi(a) * \varphi(b) = ([a], h_{[a]}(a)) * ([b], h_{[b]}(b)) &= \big([a*b], \beta_{[a],[b]}(h_{[a]}(a), h_{[b]}(b))\big)\\ &= \big([a*b], h_{[a*b]} L_{h_{[a]}^{-1}(h_{[a]}(a))} h_{[b]}^{-1}(h_{[b]}(b))\big)\\ &= \big([a*b], h_{[a*b]} L_a(b)\big) = \varphi(a*b).\end{aligned}$$

Now, set

$$\theta_{[a],[b]} = \beta_{[a],[b]}(e,e) \quad \text{and} \quad \psi_{[a],[b]}(t) = -\beta_{[a],[b]}(e,e) + \beta_{[a],[b]}(e,t).$$

We prove that the mappings ψ actually do not depend on a, b. For $t = f(e)$ with $f \in \mathrm{Dis}(Q)$, expand

$$\beta_{[a],[b]}(e,t) = h_{[a*b]} L_{h_{[a]}^{-1}(e)} h_{[b]}^{-1}(f(e)) = h_{[a*b]} h_{[a]}^{-1} L_e h_{[a]} h_{[b]}^{-1} f L_e^{-1}(e)$$

in order to obtain a mapping from $\mathrm{Dis}(Q)$ acting on e, and calculate

$$\begin{aligned}\psi_{[a],[b]}(t) &= -\beta_{[a],[b]}(e,e) + \beta_{[a],[b]}(e,t)\\ &= \left(h_{[a*b]} h_{[a]}^{-1} L_e h_{[a]} h_{[b]}^{-1} L_e^{-1}\right)^{-1} \left(h_{[a*b]} h_{[a]}^{-1} L_e h_{[a]} h_{[b]}^{-1} f L_e^{-1}\right)(e)\\ &= L_e f L_e^{-1}(e) = L_e(t).\end{aligned}$$

In particular, $\psi = \psi_{[a],[b]} = L_e$ is an automorphism of A (as proved earlier).

Finally, we show that $\beta_{[a],[b]}(s,t) = (1-\psi)(s) + \psi(t) + \theta_{[a],[b]}$, thus completing the proof that E is isomorphic to a central extension. Again, for $s = f(e)$ and $t = g(e)$ with $f, g \in N$, we calculate

$$\begin{aligned}(1-\psi)(s) + \psi(t) + \theta_{[a],[b]} &= f(e) - L_e f L_e^{-1}(e) + L_e g L_e^{-1}(e) + h_{[a*b]} h_{[a]}^{-1} L_e h_{[a]} h_{[b]}^{-1} L_e^{-1}(e)\\ &= f(L_e f^{-1} L_e^{-1})(L_e g L_e^{-1})(h_{[a*b]} h_{[a]}^{-1} L_e h_{[a]} h_{[b]}^{-1} L_e^{-1})(e)\\ &= L_{f(e)} \underbrace{g}_{\in N} \underbrace{L_e^{-1} h_{[a*b]} h_{[a]}^{-1} L_e}_{\in \mathrm{Dis}(E)} \underbrace{h_{[a]} h_{[b]}^{-1}}_{\in \mathrm{Dis}(E)}(e)\\ &= \underbrace{L_{f(e)} L_e^{-1}}_{\in \mathrm{Dis}_\alpha} \underbrace{h_{[a*b]} h_{[a]}^{-1}}_{\in \mathrm{Dis}(E)} L_e h_{[a]} h_{[b]}^{-1} g(e)\end{aligned}$$

$$\begin{aligned} &= h_{[a*b]}h_{[a]}^{-1}L_{f(e)}L_e^{-1}L_e h_{[a]}h_{[b]}^{-1}g(e) = h_{[a*b]}h_{[a]}^{-1}L_s h_{[a]}h_{[b]}^{-1}(t) \\ &= \beta_{[a],[b]}(s,t) \end{aligned}$$

(in the second step, note that all mappings are in $\mathrm{Dis}(Q)$; later, we used centrality of N and of Dis_α). □

Corollary 7.9. *Let E be a quandle and α its central congruence such that E/α is connected and Dis_α acts transitively on every block of α. Then E is isomorphic to a central extension $E/\alpha \times_{\phi,\psi,\theta} A$.*

Proof. Apply Proposition 7.8 to $N = \mathrm{Dis}_\alpha$. Indeed, $\mathrm{Dis}_\alpha \in \mathrm{Norm}(E)$ is central in $\mathrm{Dis}(Q)$ by Theorem 1.1, and $\alpha = \mathcal{O}_{\mathrm{Dis}_\alpha}$ by Proposition 3.3(3) and the transitivity condition. □

Remark 7.10. Proposition 7.8 applies to any central congruence of any latin quandle. This has been known for a long time in the setting of quasigroup theory. Our definition of central extensions is a special case of the general definition from [**26**, Section 7] for arbitrary algebraic structures. If A is an algebraic structure in a congruence modular variety, then any central congruence of A admits a representation by a central extension [**26**, Proposition 7.1]. In particular, this applies to any quasigroup $(Q, *, \backslash, /)$; however, the right division operation is essential, congruences must be central with respect to terms in all three operations. Therefore, the two results are equivalent only in the finite case. We also refer to a similar result for loops [**46**, Theorem 4.2].

There is no direct analogy of Proposition 7.8 for abelian congruences, not even for finite latin quandles.

Example 7.11. The latin quandles SmallQuandle(28,11) and (28,12) in the RIG library have an abelian non-central congruence which does not admit a representation by an abelian extension. In both cases, the blocks are affine quandles over the group $\mathbb{Z}_7$, and the factor is the four-element latin quandle Q_4, whose multiplication table is below:

1	3	4	2
4	2	1	3
2	4	3	1
3	1	2	4

.

Consider a quandle Q_4-module over the group $\mathbb{Z}_7$, i.e., $\phi : Q_4^2 \to \mathrm{End}(\mathbb{Z}_7)$, $\psi : Q_4^2 \to \mathrm{Aut}(\mathbb{Z}_7)$ satisfying equations (7.3), (7.4), (7.5). Let β be the dynamical cocycle given by ϕ, ψ and an arbitrary admissible θ. Let $\gamma_a = \psi_{a/1,1}^{-1} = \psi_{1*a,1}^{-1}$ and

$$\tilde{\beta}_{a,b}(s,t) = \underbrace{\gamma_{a*b}\phi_{a,b}\gamma_a^{-1}}_{\nu_{a,b}}(s) + \underbrace{\gamma_{a*b}\psi_{a,b}\gamma_b^{-1}}_{\varepsilon_{a,b}}(t) + \gamma_{a*b}(\theta_{a,b}).$$

According to [**2**, Definition 2.6], β and $\tilde{\beta}$ are cohomologous, hence the corresponding extensions are isomorphic. We will show that ν, ε are constant mappings, and therefore cannot represent a non-central congruence.

Obviously, $\varepsilon_{a,1} = \varepsilon_{1,1}$ for every $a \in Q_4$. Using the cocycle conditions and abelianness of $\mathrm{Aut}(\mathbb{Z}_7)$, it is straightforward to verify that $\varepsilon_{1,1} = \varepsilon_{a,a} = \varepsilon_{1,a}$, $\varepsilon_{1*a,1*b} = \varepsilon_{a,b}$ and that $\nu_{1*a,1*b} = \nu_{a,b}$ for every $a, b \in Q_4$. For example, setting $b = c$ in (7.3), we obtain $\varepsilon_{a*b,a*b}\varepsilon_{a,b} = \varepsilon_{a,b}\varepsilon_{b,b}$, cancel $\varepsilon_{a,b}$ thanks to commutativity and use connectedness of Q_4 to conclude that all diagonal entries are equal. The other cases are proved similarly. So, accordingly,

$$\nu = \begin{bmatrix} 1-\lambda & \nu_0 & \nu_0 & \nu_0 \\ \nu_1 & 1-\lambda & \nu_2 & \nu_3 \\ \nu_1 & \nu_3 & 1-\lambda & \nu_2 \\ \nu_1 & \nu_2 & \nu_3 & 1-\lambda \end{bmatrix}, \qquad \varepsilon = \begin{bmatrix} \lambda & \lambda & \lambda & \lambda \\ \lambda & \lambda & k & l \\ \lambda & l & \lambda & k \\ \lambda & k & l & \lambda \end{bmatrix},$$

for some $k, l, \lambda \in \mathrm{Aut}(\mathbb{Z}_7)$ and $\nu_i \in \mathrm{End}(\mathbb{Z}_7)$ for $i = 0, \dots, 3$. We are left with seven parameters, so it becomes feasible to set a computer search over all options, checking the cocycle conditions for each choice. Over the group $\mathbb{Z}_7$, all solutions satisfy $k = l = \lambda$ and $\nu_i = 1 - \lambda$ for all i, hence both ν, ε are constant.

8. Applications.

8.1. Non-existence results.

As an application of the commutator theory, we will show a few non-existence results. As an ingredient, we will use a part of the classification of finite simple quandles [**2**], [**36**]: a finite simple abelian quandle is affine of prime power size (this is essentially the contents of [**2**, Theorem 3.9]).

Theorem 8.1.

(1) *There is no connected involutory quandle of size 2^k, for any $k \geq 1$.*

(2) *There is no connected involutory rack of size 2^k, for any $k > 1$.*

Proof. (1) Let Q be a connected involutory quandle of size 2^k. According to Proposition 6.5, $\mathrm{Dis}(Q)$ is a 2-group, hence nilpotent, and thus Q is nilpotent by Theorem 1.2. Therefore, it has a simple abelian factor Q/α, and thanks to Proposition 2.5, it has size 2^l, $l \leq k$. Finite simple abelian quandles are affine, and thus latin. But there is no latin involutory quandle of even order, because left translations in latin quandles have precisely one fixed point.

(2) Consider the smallest congruence α such that the factor is a quandle. It is uniform by Proposition 2.5, hence $|Q/\alpha| = 2^k$, which is impossible unless $k = 0$. Hence $\alpha = 1_Q$ and Q must be a permutation rack. But the only connected involutory permutation rack has two elements. □

Theorem 8.2 was originally proved by Stein [**48**, Theorem 9.9] in 1950s using a topological argument: from a graph of the corresponding latin square, he constructed a triangulated polyhedron, and discussed the parity of its Euler characteristic. In [**27**, Theorem 6.1], Galkin proved Stein's theorem using a shorter group-theoretical argument about the minimal representation. Our theory allows a direct inductive proof.

Theorem 8.2 ([**48**]). *There is no latin quandle of size* $\equiv 2 \pmod 4$.

Proof. Let Q be the smallest latin quandle of size $\equiv 2 \pmod 4$. If Q was simple, then it was abelian thanks to Corollary 1.3, hence affine of prime power order; but no prime power is $\equiv 2 \pmod 4$ with the exception of 2^1, but there is no latin quandle of order 2, which is a contradiction. So Q has a non-trivial congruence α which is uniform by Proposition 2.5. Let m denote the size of its blocks and n the size of its factor. Then $|Q| = m \cdot n \equiv 2 \pmod 4$, hence either m or n is $\equiv 2 \pmod 4$, and this contradicts that Q was the smallest with this property. □

8.2. Coloring knots and links.

Quandle coloring is a powerful invariant of knot (and link) equivalence, particularly from the computational perspective [**16**], [**25**]. Coloring by affine quandles is related to the Alexander invariant: the main result of [**3**] states that a link is colorable by an affine quandle if and only if its Alexander polynomial does not vanish. We extend the theorem to solvable quandles. The following lemma is essentially [**25**, Lemma 1].

Lemma 8.3. *Let c be a non-trivial coloring of a link L by a quandle Q, and assume that* $\mathrm{Im}(c)$ *generates Q. Then L is colorable by every simple factor of Q.*

Proof. Consider any simple factor $R = Q/\alpha$, and take the composition $c' = \pi \circ c$ where π is the natural projection $Q \to R$. Then c' is a coloring of L by R. If c' was trivial, then all colors used by c were in one block, B, of α. Since congruence blocks are subquandles and Q is generated by $\mathrm{Im}(c)$, we have $B = Q$, hence $\alpha = 1_Q$, which is a contradiction. □

Theorem 8.4. *Let L be a link with trivial Alexander polynomial, and Q be a finite connected solvable quandle. Then L is not colorable by Q.*

Proof. Let c be a non-trivial coloring and consider the subquandle S generated by $\mathrm{Im}(c)$. Proposition 6.4 implies that S is also solvable, and Lemma 8.3 says that L is colorable by every simple factor of S. However, all simple factors of a solvable quandle are abelian, hence affine. This contradicts [**3**, Theorem 1.2] which says that links with trivial Alexander polynomial admit no non-trivial coloring by an affine quandle. □

In particular, Corollary 1.3 implies that links with trivial Alexander polynomial are not colorable by any finite latin quandle. (It agrees with the data calculated in [**16**].)

8.3. Bruck loops.

This subsection is written for loop theory specialists, so we omit explaining the details of the definitions and facts, that can be found in [**12**].

Recall that, in loop theory, the classical notion of central nilpotence is equivalent to nilpotence in the sense of universal algebra, but the classical notion of solvability is strictly weaker than universal algebraic solvability [**45**]. In 1960's, Glauberman proved that Bruck loops of odd order are solvable in the weak sense [**29**, Theorem 14], that Bruck loops of prime power order p^k, $p \neq 2$, are nilpotent [**28**, Theorem 7], and with some effort, one can deduce from the results of [**28**], [**29**] the converse, that nilpotent

Bruck loops of odd order are isomorphic to a direct product of loops of prime power order.

There is a strong link between the theory of latin quandles, and the theory of Bruck loops. There is a polynomial equivalence between the variety of latin quandles, and the variety of so called *Belousov–Onoi modules*, which consist of a Belousov–Onoi loop and its automorphism (see [**4**], or [**44**, Section 5.1]). Polynomial equivalence preserves all properties defined by polynomial operations, such as congruences, the centralizing relation $C(\alpha,\beta;\delta)$, and subsequently the notions of abelianness, solvability, etc. (see [**6**, Section 4.8] for details). Therefore, our Corollary 1.3 and Theorem 1.4 imply that Belousov–Onoi loops are solvable in the stronger sense, and that a finite Belousov–Onoi loop is nilpotent if and only if it decomposes to a direct product of loops of prime power size.

In the Belousov–Onoi correspondence, involutory latin quandles correspond to uniquely 2-divisible Bruck loops [**44**, Theorem 5.9]. Equivalently, in the finite case, to Bruck loops of odd order. Therefore, our theory strengthens the Glauberman's solvability theorem, and provides an alternative and complete proof of the prime decomposition theorem.

Corollary 8.5.

(1) *Bruck loops of odd order are solvable* (*in the stronger sense of universal algebra*).

(2) *A Bruck loop of odd order is nilpotent if and only if it is isomorphic to a direct product of Bruck loops of prime power order.*

Proof. Apply the polynomial equivalence of [**44**, Theorem 5.9] to Corollary 1.3 and Theorem 1.4. □

A curious reader might ask: the original Glauberman's proof of solvability involved his famous Z*-theorem, one of the key steps in the classification of finite simple groups, where is it hidden in our proof of the stronger theorem? The answer is, in Stein's proof that latin quandles have solvable left multiplication groups, which uses the classification of finite simple groups.

References

[1] E. Aichinger and N. Mudrinski, Some applications of higher commutators in Mal'cev algebras, Algebra Universalis, **63** (2010), 367–403.

[2] N. Andruskiewitsch and M. Graña, From racks to pointed Hopf algebras, Adv. Math., **178** (2003), 177–243.

[3] Y. Bae, Coloring link diagrams by Alexander quandles, J. Knot Theory Ramifications, **21** (2012), no. 10, 1250094, 13 pp.

[4] V. D. Belousov and V. I. Onoi, On loops isotopic to left distributive quasigroups, Mat. Issled., **7** (1972), no. 25/3, 135–152 (Russian).

[5] G. B. Belyavskaya, On commutators of quasigroup congruences, Bul. Acad. Ştiinţe Repub. Mold. Mat., (1998), no. 2, 91–101.

[6] C. Bergman, Universal Algebra: Fundamentals and Selected Topics, CRC Press, 2011.

[7] G. Bianco, On the transvection group of a rack, PhD thesis (2015), https://iris.unife.it/retrieve/handle/11392/2389091/123862/1015.pdf.

[8] G. Bianco and M. Bonatto, On connected quandles of prime power order, Beitr. Algebra Geom., (2020), doi:10.1007/s13366-020-00501-y.

[9] M. Bonatto, Principal and doubly homogeneous quandles, Monatsh. Math., **191** (2020), 691–717.

[10] M. Bonatto, Connected quandles of size pq and $4p$, arXiv:1907.07716.

[11] M. Bonatto and D. Stanovský, A universal algebraic approach to rack coverings, arXiv:1910.09317.

[12] R. H. Bruck, A Survey of Binary Systems, Ergeb. Math. Grenzgeb. Neue Folge, Heft 20. Reihe: Gruppentheorie, Springer Verlag, Berlin-Göttingen-Heidelberg, 1958.

[13] E. Bunch, P. Lofgren, A. Rapp and D. N. Yetter, On quotients of quandles, J. Knot Theory Ramifications, **19** (2010), 1145–1156.

[14] J. S. Carter, M. Elhamdadi, M. Graña and M. Saito, Cocycle knot invariants from quandle modules and generalized quandle homology, Osaka J. Math., **42** (2005), 499–541.

[15] W. E. Clark, M. Elhamdadi, X. Hou, M. Saito and T. Yeatman, Connected quandles associated with pointed abelian groups, Pacific J. Math., **264** (2013), 31–60.

[16] W. E. Clark, M. Elhamdadi, M. Saito and T. Yeatman, Quandle colorings of knots and applications, J. Knot Theory Ramifications, **23** (2014), no. 6, 1450035, 29 pp.

[17] W. E. Clark and X. Hou, Galkin quandles, pointed abelian groups, and sequence A000712, Electron. J. Combin., **20** (2013), no. 1, P45.

[18] W. E. Clark and M. Saito, Quandle identities and homology, In: Knots, Links, Spatial Graphs, and Algebraic Invariants, Contemp. Math., **689**, Amer. Math. Soc., Providence, RI, 2017, 23–35.

[19] W. E. Clark, M. Saito and L. Vendramin, Quandle coloring and cocycle invariants of composite knots and abelian extensions, J. Knot Theory Ramifications, **25** (2016), no. 5, 1650024, 34 pp.

[20] M. Eisermann, Quandle coverings and their Galois correspondence, Fund. Math., **225** (2014), 103–167.

[21] M. Elhamdadi and S. Nelson, Quandles: An Introduction to the Algebra of Knots, Stud. Math. Libr., **74**, Amer. Math. Soc., Providence, RI, 2015.

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

[23] P. Etingof, T. Schedler and A.Soloviev, Set-theoretical solutions to the quantum Yang–Baxter equation, Duke Math. J., **100** (1999), 169–209.

[24] V. Even and M. Gran, On factorization systems for surjective quandle homomorphisms, J. Knot Theory Ramifications, **23** (2014), no. 11, 1450060, 15 pp.

[25] A. Fish, A. Lisitsa and D. Stanovský, A combinatorial approach to knot recognition, In: Embracing Global Computing in Emerging Economies, Communications in Computer and Information Science, **514**, Springer, 2015, 64–78.

[26] R. Freese and R. McKenzie, Commutator Theory for Congruence Modular Varieties, London Math. Soc. Lecture Note Ser., **125**, Cambridge Univ. Press, 1987.

[27] V. M. Galkin, Left distributive finite order quasigroups, Mat. Issled., **51** (1979), 43–54 (Russian).

[28] G. Glauberman, On loops of odd order, J. Algebra, **1** (1964), 374–396.

[29] G. Glauberman, On loops of odd order II, J. Algebra, **8** (1968), 393–414.

[30] D. Hobby and R. McKenzie, The Structure of Finite Algebras, Contemp. Math., **76**, Amer. Math. Soc., Providence, 1988.

[31] A. Hulpke, D. Stanovský and P. Vojtěchovský, Connected quandles and transitive groups, J. Pure Appl. Algebra, **220** (2016), 735–758.

[32] N. Jackson, Extensions of racks and quandles, Homology Homotopy Appl., **7** (2005), 151–167.

[33] P. Jedlička, A. Pilitowska, D. Stanovský and A. Zamojska-Dzienio, Subquandles of affine quandles, J. Algebra, **510** (2018), 259–288.

[34] P. Jedlička, A. Pilitowska, D. Stanovský and A. Zamojska-Dzienio, The structure of medial quandles, J. Algebra, **443** (2015), 300–334.

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

[36] D. Joyce, Simple quandles, J. Algebra, **79** (1982), 307–318.

[37] K. A. Kearnes, Congruence modular varieties with small free spectra, Algebra Universalis, **42** (1999), 165–181.

[38] R. McKenzie and J. Snow, Congruence modular varieties: commutator theory and its uses, In: Structural Theory of Automata, Semigroups, and Universal Algebra, NATO Sci. Ser. II Math. Phys. Chem., **207**, Springer, Dordrecht, 2005, 273–329.

[39] H. Nagao, A remark on simple symmetric sets, Osaka J. Math., **16** (1979), 349–352.

[40] T. Nagy, Non-affine latin quandles of order 2^k, to appear in J. Algebra Appl., doi:10.1142/S0219498821501036.

[41] W. Rump, A decomposition theorem for square-free unitary solutions of the quantum Yang–Baxter equation, Adv. Math., **193** (2005), 40–55.

[42] J. D. H. Smith, Mal'cev Varieties, Lecture Notes in Math., **554**, Springer, 1976.

[43] J. D. H. Smith, Finite distributive quasigroups, Math. Proc. Cambridge Philos. Soc., **80** (1976), 37–41.

[44] D. Stanovský, A guide to self-distributive quasigroups, or Latin quandles, Quasigroups Related Systems, **23** (2015), 91–128.

[45] D. Stanovský and P. Vojtěchovský, Commutator theory for loops, J. Algebra, **399** (2014), 290–322.

[46] D. Stanovský and P. Vojtěchovský, Abelian extensions and solvable loops, Results Math., **66** (2014), 367–384.

[47] A. Stein, A conjugacy class as a transversal in a finite group, J. Algebra, **239** (2001), 365–390.

[48] S. K. Stein, On the foundations of quasigroups, Trans. Amer. Math. Soc., **85** (1957), 228–256.

[49] L. Vendramin, Rig, a GAP package for racks, quandles and Nichols algebras, Available at http://github.com/vendramin/rig/.

Marco Bonatto
IMAS-CONICET
University of Buenos Aires
Argentina
E-mail: marco.bonatto.87@gmail.com

David Stanovský
Department of Algebra
Faculty of Mathematics and Physics
Charles University
Prague, Czech Republic
E-mail: stanovsk@karlin.mff.cuni.cz