THE ALGEBRAIC THEORY OF RACKS AND QUANDLES

DAVID STANOVSKÝ AND PETR VOJTĚCHOVSKÝ

0.1. **Introduction.** The primary motivation for the development of the theory of racks and quandles comes from constructions of knot invariants [10, 11, 12, 22, 24], describing set-theoretic solutions to the quantum Yang-Baxter equation [13, 14], constructions of Hopf algebras [1], or the abstract theory of quasigroups and loops [28].

Among the many motivations behind quandles, perhaps the most interesting is the one coming from knot theory: one can color arcs of a knot using quandle elements as colors, imposing certain condition for colors at each crossings; the number of colorings is an invariant, and the three axioms of quandles correspond to invariance with respect to the three Reidemeister moves [22].

Our notes are meant as a counterpart to the book [12] which explains thoroughly the knot theoretic aspects, but mostly avoids the algebraic aspects.

Our notes are not exhaustive: see more algebraic theory in [1] (the theory of extensions), ... TODO: list of other interesting results

We concentrate on: representation theorems, isomorphism theorems for the representations, enumeration.

1. The fundamentals

1.1. **Notation.** We adopt the left notation in all aspects. I.e., mapping apply on the left, $f(x)$, mappings compose leftwards, $(gf)(x) = g(f(x))$, therefore conjugation is naturally considered as gag^{-1}, so that composition of the inner automorphisms corresponds to multiplication in the group, and the commutator is defined as $[a, b] = aba^{-1}b^{-1}$. For the same reason, it is natural to prefer action of left translations. In particular, we will implictly consider left racks and left quandles, defined by left seld-distributivity.

Let a group G act on a set X. For $e \in X$, the stabilizer of e will be denoted G_e, the orbit of e will be denoted Ge.

Addition and multiplication will implicitly refer to a group operations. Unspecified binary operations will be usually denoted by $*$. Rack and quandle operations will be usually denoted by $\triangleright$.

1.2. **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 $Q = (Q, *, \ldots)$ where $*$ is a binary operation and $\ldots$ stands for a (possibly empty) list of other operations.

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

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

be the *left translation* by a and the *right translation* by a, respectively.

We will often use the following observation: for every $a \in Q$ and $\alpha \in \mathrm{Aut}(Q, *)$,

$$\alpha L_a \alpha^{-1} = L_{\alpha(a)} \qquad (L^\alpha)$$

and dually for right translations.

Date: December 15, 2022.

1.3. **Division in binary algebraic structures.** 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

$$x \backslash^{*} (x * y) = y = x * (x \backslash^{*} y).$$

Dually, we can define *right division* by $b \,/_{*}\, a = R_a^{-1}(b)$ and *right quasigroups*.

If all left and right translations are bijective, there is an ambiguity in terminology. We will use the following convention: For left quasigroups $Q = (Q, *, \backslash^{*})$ where all right translations are also permutations, we will use the adjective *latin*. A *quasigroup* is an algebraic structure $(Q, *, \backslash^{*}, /_{*})$ where $(Q, *, \backslash^{*})$ is a left quasigroup and $(Q, *, /_{*})$ is a right quasigroup. (The set of operations plays a role when it comes to derived notions such as substructures and congruences.)

Many universal algebraic concepts, such as subalgebras, homomorphisms and congruences, 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. (There is a collision with the standard setting of quasigroup theory, where both division operations are considered. This issue will be adressed in Section **??** on latin quandles.)

A *homomorphism* is a mapping preserving all operations. Note that a mapping between left quasigroups preserving $*$ also preserves $\backslash^{*}$. The *kernel* of a homomorphism f is the relation $\{(a, b) : f(a) = f(b)\}$. Equivalences invariant with respect to all operations are called *congruences*. Kernels of homomorphisms are congruences.

1.4. **Other important identities.** A binary algebraic structure $(Q, *)$ is called *medial* if

$$(x * y) * (u * v) = (x * u) * (y * v)$$

holds for every $x, y, u, v \in Q$, i.e., if $*$ is a homomorphism $Q^2 \to Q$. If $(Q, *, \backslash^{*})$ is a left quasigroup, then mediality in either operation implies mediality in the other one.

A binary algebraic structure $(Q, *)$ is called *involutory* if $L_a^2 = 1$ for every a, i.e., if the identity

$$x * (x * y) = y$$

holds for every $x, y \in Q$. Equivalently, if $* = \backslash^{*}$. Therefore, the question whether to include $\backslash^{*}$ on the list of operations is irellevant for involutory structures.

???

1.5. **Racks and quandles.** A *rack* is a left quasigroup in which all left translations are automorphisms. (Strictly speaking, we shall explicitly use the term *left rack*, however, the adjective is usually dropped by our convention to use the left notation.)

Rack operations will be denoted implicitly by $\triangleright$, following e.g. [1, **?**]. Our choice is motivated by the prevailing idea that vertical bar is used on the acting side, e.g. in the symbol for normal subgroups, $N \lhd G$, or semidirect product, $N \rtimes K$. Other options exist in literature. Ocassionally, the triangle is facing the other direction [12, 22]. Symmetric operators, such as $*$ or $\circ$, are also used.

Racks are axiomatized by three identities,

This can be expressed as an identity,

$$x \backslash^{\triangleright} (x \triangleright y) = y = x \triangleright (x \backslash^{\triangleright} y)$$

and

$$x \triangleright (y \triangleright z) = (x \triangleright y) \triangleright (x \triangleright z), \tag{1.1}$$

the latter called *left self-distributivity.*

An idempotent rack (i.e., where $x \triangleright x = x$ holds) is called a *quandle.* Latin racks are quandles: substituting $x = y$ in the left distributive law, we obtain $x \triangleright (x \triangleright z) = (x \triangleright x) \triangleright (x \triangleright z)$, and right cancellation yields idempotence.

Substructures of racks and quandles are called *subracks* and *subquandles.*

Every definable subset X of a rack Q is a subrack such that $a \triangleright x \in X$ for every $a \in Q$ and $x \in X$. Indeed, since L_a is an automorphism, it preserves every definable subset.

1.6. **Basic constructions.**

Example 1.1. *Permutation racks.* Let Q be a set, f a permutation of Q, and define

$$a \triangleright b = f(b), \qquad a \backslash^{\triangleright} b = f^{-1}(b).$$

Then $(Q, \triangleright, \backslash^{\triangleright})$ is a medial rack, to be called a *permutation rack.*

If $f = 1$, i.e., $a \triangleright b = b$, we talk about *projection quandle* (ocassionally called *trivial quandle*). If $Q = \mathbb{Z}$, $f(x) = x + 1$, or $Q = \mathbb{Z}_n$, $f(x) = x + 1 \bmod n$, we talk about *cyclic* permutation rack.

Example 1.2. *Affine racks.* Let A be an abelian group, f, g its endomorphisms and $c \in A$. We define

$$a * b = f(a) + g(b) + c.$$

The resulting binary algebra $\mathrm{Aff}(A, f, g, c) = (A, *)$ is called *affine* over the group A. It is easy to show that

- it is a left (resp. right) quasigroup iff g (resp. f) is an automorphism,
- it is medial iff $fg = gf$,
- it is left distributive iff $fg = gf$, $f = f(f + g)$ and $f(c) = 0$,
- it is idempotent $g = 1 - f$ and $c = 0$.

In case of quandles, we will use a shorter notation $\mathrm{Aff}(A, f) = \mathrm{Aff}(A, 1 - f, f, 0)$ (ocassionally, the name *Alexander quandles* is used, see the discussion in Section **??**), the operations are then

$$a \triangleright b = (1 - f)(a) + f(b), \qquad a \backslash^{\triangleright} b = (1 - f^{-1})(a) + f^{-1}(b).$$

Example 1.3. *Conjugation quandles.* Let G be a group and $C \subseteq G$ a subset closed with respect to conjugation. Then $(C, \triangleright)$ with $a \triangleright b = aba^{-1}$ is a quandle, called *conjugation quandle.*

Example 1.4. *Coset quandles and principal quandles.* Let G be a group, H a subgroup and $f \in \mathrm{Aut}(G)$ which fixes H pointwise. Define an operation $\triangleright$ on the cosets by

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

It is easy to check that $\mathcal{Q}(G, H, f) = (G/H, \triangleright)$ is a quandle, called the *coset quandle* (the construction can be traced back to Joyce [22] and Galkin [**?**]). If $H = 1$, we talk about *principal quandles* (ocassionally, the name *generalized Alexander quandles* is used). If G is abelian, we obtain affine quandles. Coset quandles are homogeneous, i.e., the automorphism group acts transitively. As we shall se in Section **??**, every homogeneous quandle can be represented as a coset quandle.

1.7. **Cayley representation.** Let Q be a left quasigroup. The *Cayley representation* is the mapping $L_Q : Q \to Sym(Q)$, $a \mapsto L_a$. If Q is a rack, L_Q is a homomorphism with respect to the conjugation operation on $Sym(Q)$, but, unlike for groups, L_Q is not necessarily one-to-one. The kernel congruence 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.* Every faithful rack is thus isomorphic to a conjugation quandle (the image of the Cayley representation). Note that every faithful rack is a quandle, since, in racks, $L_{a \triangleright a} = L_a$ for every a by (L^{α}).

1.8. **The smallest idempotent congruence.** We introduce powers by

$$a^k = \underbrace{a \triangleright (a \triangleright (\ldots \triangleright (a \triangleright a)))}_{k}.$$

An easy induction shows that, in a rack Q,

$$a^k \triangleright b = a \triangleright b, \qquad \text{and} \qquad b \triangleright a^k = (b \triangleright a)^k$$

for every $a, b \in Q$ and every $k \in \mathbb{N}$.

Let ι_k be the smallest congruence such that the corresponding factor satisfies the identity $x^{k+1} \approx x$. Indeed, $\iota_k \subseteq \iota_\ell$ if and only if $\ell \mid k$. In particular, $\iota_k \subseteq \iota_1$ for every k, and $\iota = \iota_1$ is the smallest idempotent congruence.

Proposition 1.5. [27] *Let Q be a rack and $k \geq 1$. Then*

(1) *ι_k is the smallest equivalence on the set Q containing all pairs (a, a^{k+1}), $a \in Q$;*
(2) *$\iota_k \leq \lambda_Q$.*
(3) *$a \,\iota_k\, b$ if and only if $a^m = b^n$ for some m, n such that $k \mid m - n$;*

Proof. (1) Clearly ι_k must contain all pairs (a, a^{k+1}), $a \in Q$. We prove that the equivalence α generated by these pairs is a congruence: $a \triangleright b = a^{k+1} \triangleright b$ and since $b \triangleright a^{k+1} = (b \triangleright a)^{k+1}$, we also have $(b \triangleright a, (b \triangleright a)^{k+1}) \in \iota_k$.

(2) is an obvious consequence of (1).

(3) ($\Rightarrow$) Assume that $(a, b) \in \iota_k$. Since ι_k is generated as an equivalence by the set $\{(a, a^{k+1}) : a \in Q\}$, there are $c_0, \ldots, c_\ell$ such that $a = c_0$, $b = c_\ell$ and either $c_i = c_{i+1}^{k+1}$, or $c_i^{k+1} = c_{i+1}$ for every $i = 0, \ldots, \ell - 1$. We proceed by induction on ℓ. If $\ell = 0, 1$, it is trivial. So, assume that $a^m = c_{\ell-1}^n$ for some m, n with $k \mid m - n$. If $c_{\ell-1} = b^{k+1}$, then

$$b^{n+k} = (b^{k+1})^n = c_{\ell-1}^n = a^m$$

and $k \mid m - (n + k)$. If $c_{\ell-1}^{k+1} = b$, then

$$a^{m+k} = (a^m)^{k+1} = (c_{\ell-1}^n)^{k+1} = (c_{\ell-1}^{k+1})^n = b^n$$

and, again, $k \mid m + k - n$.

($\Leftarrow$) Assume that $a^m = b^n$ for some m, n with $k \mid m - n$. Then also $a^{m+u} = (a^m)^{u+1} = (b^n)^{u+1} = b^{n+u}$ for every $u \geq 0$. Let m', n', q be such that $m = m'k + q$ and $n = n'k + q$. Since

$$(a, a^{k+1}) \in \iota_k,\ (a^{k+1}, a^{2k+1}) \in \iota_k,\ \ldots,\ (a^{m'k+1}, a^{(m'+1)k+1}) \in \iota_k,$$

we have $(a, a^{m'k+k+1}) \in \iota_k$ and similarly $(b, b^{n'k+k+1}) \in \iota_k$. Since

$$a^{m'k+k+1} = a^{m+(k+1-q)} = b^{n+(k+1-q)} = b^{n'k+k+1},$$

we obtain $(a, b) \in \iota_k$. □

In particular,

$$\iota = \{(a, b) :\ a^m = b^n \text{ for some } m, n\} \leq \lambda_Q$$

and it is the smallest equivalence containing all pairs $(a, a \triangleright a)$.

Corollary 1.6. *Let Q be a rack. Then every block of ι is a subrack, which is a cyclic permutation rack.*

1.9. **Racks are quandles with an automorphism.** (IS IT INTERESTING???

Proposition 1.7. [27] *The variety of racks is term equivalent to the variety of algebraic structures* $(Q,*,\backslash^*,f)$ *such that*

1. $(Q,*,\backslash^*)$ *is a quandle;*
2. f *is an automorphism of* $(Q,*,\backslash^*)$*;*
3. $f(x)*y = x*y$ *for all* $x,y\in Q$.

In one direction, $x*y = x\triangleright y^n$ *and* $f(x)=x\triangleright x$*. In the other direction,* $x\triangleright y = f(x*y)$.

Proof. First we show that if $(Q,\triangleright,\backslash^\triangleright)$ is a rack, then $(Q,*,\backslash^*,f)$ with $x*y = x\triangleright y^n$ and $f(x)=x\triangleright x$ satisfies the three conditions. OLD PROOF (REDO): Note that $xy^n\approx(xy)^n$ and $(x^m)^n\approx x^{m+n-1}$. Hence $A(\circ)$ satisfies LD, since $x\circ(y\circ z)=x(yz^n)^n\approx x\cdot y((z)^n)^n\approx x\cdot yz^{2n-1}\approx_{LI} x\cdot y^nz^{2n-1}\approx_{LD}(xy^n)(xz^{2n-1})\approx(xy^n)(xz^n)^n=(x\circ y)\circ(x\circ z)$. Also, $A(\circ)$ satisfies n-LS, because $x\circ\ldots\circ x\circ y = x(x(\ldots(xy)^n\ldots)^n)^n\approx x\ldots x(((y^n)^n)\ldots)^n\approx x\ldots xy^{n^2-n+1}\approx_{LS} y^{n^2-n+1}\approx_{LS} y$. Clearly, $A(\circ)$ is idempotent, since $x\circ x = x^{n+1}\approx x$.

Now, $f^n(x)\approx_{LI} x^{n+1}\approx_{LS} x$, so f is a permutation of order n and $f(x\circ y)=(xy^n)(xy^n)\approx_{LD} x(y^ny^n)\approx_{LI}(xx)(y^{2n-1})\approx(xx)(yy)^n = f(x)\circ f(y)$ shows that it is a homomorphism. Finally, $f(x)\circ y=(xx)y^n\approx_{LI} xy^n = x\circ y$.

In the other direction, we show that $x\triangleright y = f(x*y)$ defines a rack operation. OLD PROOF (REDO): We have $x\bullet(y\bullet z)=f(x\circ f(y\circ z))\approx_{(2)} f(x)\circ(f^2(y)\circ f^2(z))\approx_{(3)} f^2(x)\circ(f^2(y)\circ f^2(z))\approx_{LD}(f^2(x)\circ f^2(y))\circ(f^2(x)\circ f^2(z))\approx_{(2)} f(f(x\circ y)\circ f(x\circ z))=(x\bullet y)\bullet(x\bullet z)$ and $x\bullet\ldots\bullet x\bullet y\approx_{(2)} f(x)\circ f^2(x)\circ\ldots\circ f^n(x)\circ f^n(y)\approx_{(3)} f(x)\circ f(x)\circ\ldots\circ f(x)\circ f^n(y)\approx_{LS} f^n(y)\approx_{(2)} y$. $\square$

2. Groups of translations and connectedness

The (left) *multiplication group* of a rack Q is the permutation group generated by left translations,

$$\mathrm{LMlt}(Q)=\langle L_a \mid a\in Q\rangle.$$

We define the *displacement group* as the subgroup

$$\mathrm{Dis}(Q)=\langle L_aL_b^{-1}\mid a,b\in Q\rangle.$$

(Alternative terminology [22]: $\mathrm{LMlt}(Q)$ is the *inner automorphism group*, $\mathrm{Dis}(Q)$ is the *transvection group*, translations are called *inner mappings*.) Using self-distributivity and (L^α), we see that

$$\mathrm{LMlt}(Q)'\le\mathrm{Dis}(Q)\le\mathrm{LMlt}(Q)\le\mathrm{Aut}(Q),$$

and that all three subgroups are normal in $\mathrm{Aut}(Q)$. Many properties of racks are determined by the properties of their multiplication and displacement groups.

Proposition 2.1. *Let Q be a rack. Then*

1. *for any* $e\in Q$, $\mathrm{Dis}(Q)=\langle L_aL_e^{-1}\mid a\in Q\rangle$ *and* $\mathrm{LMlt}(Q)/\mathrm{Dis}(Q)$ *is cyclic.*
2. $\mathrm{Dis}(Q)=\{L_{a_1}^{k_1}\ldots L_{a_n}^{k_n}:\ a_1,\ldots,a_n\in Q$ *and* $\sum_{i=1}^n k_i=0\}$;
3. *if Q is a quandle, then the natural actions of* $\mathrm{LMlt}(Q)$ *and* $\mathrm{Dis}(Q)$ *on Q have the same orbits.*

Proof. (1) $L_aL_b^{-1}=(L_aL_e^{-1})(L_bL_e^{-1})^{-1}$ for every $a,b\in Q$. It follows that $\mathrm{LMlt}(Q)/\mathrm{Dis}(Q)=\langle[L_e]\rangle$.

(2) Let S be the set on the right-hand side of the expression. Since the generators of $\mathrm{Dis}(Q)$ belong to S, we have $\mathrm{Dis}(Q)\subseteq S$. For the other inclusion, we note that every $\alpha\in S$ can be written as $L_{a_1}^{k_1}\ldots L_{a_n}^{k_n}$, where not only $\sum_i k_i=0$ but also $k_i=\pm1$. Assuming such a decomposition, we prove by induction on n that $\alpha\in\mathrm{Dis}(Q)$. If $n=0$ then α is the identity, the case $n=1$ does not occur, and if $n=2$ we have either $\alpha=L_aL_b^{-1}\in\mathrm{Dis}(Q)$, or $\alpha=L_a^{-1}L_b=L_{a\backslash_\triangleright b}L_a^{-1}\in\mathrm{Dis}(Q)$. Suppose that $n>2$.

If $k_1 = k_n$ then there is $1 < m < n$ such that $\sum_{i<m} k_i = 0$ and $\sum_{i\geq m} k_i = 0$. Let $\beta = L_{a_1}^{k_1} \dots L_{a_{m-1}}^{k_{m-1}}$ and $\iota = L_{a_m}^{k_m} \dots L_{a_n}^{k_n}$. Then, by the induction assumption, $\beta, \iota \in \mathrm{Dis}(Q)$, and so $\alpha = \beta\iota \in \mathrm{Dis}(Q)$.

If $k_1 \neq k_n$ then

$$\alpha = L_a^k \beta L_b^{-k} = L_a^k (\beta L_b^{-k} \beta^{-1}) \beta = (L_a^k L_{\beta(b)}^{-k}) \beta$$

for some $a, b \in Q$, $k \in \{\pm 1\}$ and $\beta = L_{a_2}^{k_2} \dots L_{a_{n-1}}^{k_{n-1}}$ such that $\sum_{2\leq i\leq n-1} k_i = 0$. Since both $L_a^k L_{\beta(b)}^{-k}$ and β belong to $\mathrm{Dis}(Q)$, we get $\alpha \in \mathrm{Dis}(Q)$.

(3) Let x, y be two elements in a single orbit of $\mathrm{LMlt}(Q)$ such that $y = \alpha(x)$ with $\alpha = L_{a_1}^{k_1} \dots L_{a_n}^{k_n} \in \mathrm{LMlt}(Q)$. With $k = k_1 + \cdots + k_n$, we have $\beta = L_y^{-k}\alpha \in \mathrm{Dis}(Q)$ by (1), and $\beta(x) = L_y^{-k}\alpha(x) = L_y^{-k}(y) = y$. □

Proposition 2.2. *Let Q be a rack. Then*

1. $\mathrm{Dis}(Q)$ *is trivial if and only if Q is a permutation rack.*
2. $\mathrm{Dis}(Q)$ *is abelian if and only if Q is medial.*

Proof. (1) $\mathrm{Dis}(Q)$ is trivial if and only if $L_a L_b^{-1} = 1$ for all $a, b \in Q$, i.e., all translations are equal, to some permutation f.

(2) Interpreting the medial law in terms of translations, we see that Q is medial if and only if $L_{x\triangleright y} L_z = L_{x\triangleright z} L_y$ for every $x, y, z \in Q$. Expanding $L_{x\triangleright y} = L_x L_y L_x^{-1}$, and similarly for $L_{x\triangleright z}$, we obtain that Q is medial iff

$$L_y L_x^{-1} L_z = L_z L_x^{-1} L_y \tag{2.1}$$

for every $x, y, z \in Q$. ($\Leftarrow$) If $\mathrm{Dis}(Q)$ is abelian then $L_y L_x^{-1} L_z L_y^{-1} = L_z L_y^{-1} L_y L_x^{-1} = L_z L_x^{-1}$ for every $x, y, z \in Q$, and we obtain (2.1). ($\Rightarrow$) Conversely, starting with (2.1), we obtain $L_y^{-1} L_x L_z^{-1} = L_z^{-1} L_x L_y^{-1}$ for every $x, y, z \in Q$, and thus $L_x L_y^{-1} L_u L_v^{-1} = L_u L_y^{-1} L_x L_v^{-1} = L_u L_v^{-1} L_x L_y^{-1}$ for every $x, y, u, v \in Q$, proving that $\mathrm{Dis}(Q)$ is abelian. □

2.1. **Connected racks.** We will refer to the orbits of transitivity of the group $\mathrm{LMlt}(Q)$ simply as *the orbits of Q*, and denote

$$Qe = \{\alpha(e) : \alpha \in \mathrm{LMlt}(Q)\}$$

the orbit containing an element $e \in Q$. Notice that orbits are subracks of Q: for $\alpha(e), \beta(e) \in Qe$ with $\alpha, \beta \in \mathrm{LMlt}(Q)$, we have $\alpha(e) \triangleright \beta(e) = (L_{\alpha(e)}\beta)(e) \in Qe$ and $\alpha(e) \backslash^{\triangleright} \beta(e) = (L_{\alpha(e)}^{-1}\beta)(e) \in Qe$.

Note that the orbit decomposition is a congruence.

Observation: definable subsets are closed with respect to action of $\mathrm{LMlt}(Q)$, thus live inside orbits.

A rack is called *connected*, if it consists of a single orbit. Orbits (as subracks) are not necessarily connected.

Observe that latin quandles are connected.

Proposition 2.3. *If Q is a connected rack then* $\mathrm{LMlt}(Q)' = \mathrm{Dis}(Q)$.

Proof. It remains to prove that every generator $L_a L_b^{-1}$ of $\mathrm{Dis}(Q)$ belongs to $\mathrm{LMlt}(Q)'$. Let $\alpha \in \mathrm{LMlt}(Q)$ be such that $\alpha(a) = b$. Then $L_a L_b^{-1} = L_a L_{\alpha(a)}^{-1} = [L_a, \alpha] \in \mathrm{LMlt}(Q)'$. □

Indecomposable racks. Copy-paste from [Hayashi notes].

3. A group-theoretic representation

3.1. **Blackburn's representation, the Vojtechovsky-Yang isomorphism theorem.** See [2, 29].

3.2. **Representing connected quandles.** Particular case: homogeneous representation of connected racks, minimal representation, canonical correspondece [18, Section 3,4,5].

(first appeared in [22] and Galkin)

4. Congruences

Outline:

- explain basic ideas from [7, 8],
- universal algebraic classification of congruences (strongly abelian = converings, abelian, central)
- perhaps mote details on coverings? [1, 8]

4.1. **Congruences vs. subgroups of Dis.** The Galois correspondence of [7].

4.2. **Special types of congruences.** [8, 7]

4.3. **Coverings and extensions.** summary of main results of [1, 8], extensions by constant cocycles

example: $\iota \leq \lambda$, hence every rack is a covering of a quandle (blocks are cyclic permutation racks); present an explicit form of extension by a cocycle

5. Affine racks

I.e., $x \triangleright y = f(x)+g(y)+c$ over an abelian group, f endomorphism, g automorphism, $(f+g)f = f$, $f(c) = 0$. This is a quandle iff $f + g = 1$ and $c = 0$.

general ideas (see [1, 13] ??)

detailed study [16, 17]

Focus on affine quandles:

- affine (in our sense) vs. Alexander (modules over $\mathbb{Z}[t, t^{-1}]$, cf. [16])
- connected [18, Section 5]
- abstract characterization, quotients, subquandles [20, 21] (no proofs)
- isomorphism theorem and enumeration (Nelson, Hou, Holmes) (TODO: even better proof)

6. Interesting classes of quandles

Idea: summary of results, very few proofs

6.1. **Principal quandles.**

Def: $Q(G, f)$

Affine are special case.

Proposition 6.1. *A principal quandle $Q(G, f)$ is connected if and only if $\langle xf(x)^{-1} : x \in G\rangle = G$.*

Proof. ☐

Note that $\langle xf(x)^{-1} : x \in G\rangle$ is always a normal subgroup of G. Hence if G is simple then all principal quandles are connected with the exception of $f = id$.

Isomorphism problem:

Proposition 6.2. *Let $Q(G, g)$, $Q(H, h)$ be principal quandles. Then (2) implies (1), and if they are connected, then (1) implies (2).*

1. *there is a quandle isomorphism $Q(G, g) \simeq Q(H, h)$,*
2. *there is a group isomorphism $\alpha : G \simeq H$ such that $\alpha g = h\alpha$.*

Proof. ☐

cf. iso problem for affine quandles - in general complicated!
cite other papers on iso problem (probably only our new paper for S_n, D_{2n} ?)
TODO: READ Bonatto's papers? [3]

6.2. **Latin quandles.**
homogeneous representation: [18, Section 6]
summarize main results of [28], refer there for details

6.3. **Medial quandles.**
summary of [19]

6.4. **Reductive quandles.**
[19] and other papers by J.P.Z., "multipermutation solutions", chracterization by dis, lmlt, universal algebraic conditions (strongly abelian)

6.5. **Simple quandles.**
Summary of the classification: old results [1, 23] presented in a novel way (Cvrcek, S.).
Simple affine quandles are finite [3].

7. Enumeration of small racks and quandles

Outline:

- application of the representation theory: up to size XX [29], asymptotic behavior [29], connected up to size 47 [18, Section 8], p [13], $2p$ [18, Section 9], p^2 [15]
- application of the structure theorems on reductivity: up to size XX [19, 29]
- Cite also newer papers [6, 4, 26], what are their methods? (coverings, ...). In [26], there is a good overview.
- better proof for p^2, p^3, pq

7.1. **Brute force.** It is easy to see that there are two racks of order 2, up to isomorphism, both are permutation racks.

It is also straightforward to verify that the following are all racks of order 3, up to isomorphism. The first three are quandles, the third one is isomorphic to $\mathrm{Aff}(\mathbb{Z}_3, -1)$.

	1	2	3
1	1	2	3
2	1	2	3
3	1	2	3

	1	2	3
1	1	3	2
2	1	2	3
3	1	2	3

	1	2	3
1	1	3	2
2	3	2	1
3	2	1	3

	1	2	3
1	2	3	1
2	2	3	1
3	2	3	1

	1	2	3
1	1	3	2
2	1	3	2
3	1	3	2

	1	2	3
1	1	2	3
2	1	3	2
3	1	3	2

Brute force is ok until cca 7-8 elements.

8. Other ideas

8.1. **Cycle structure.**
Hayashi, criterion to be latin [25]

8.2. **Mal'tsev conditions ?**
[9, 5]

8.3. **Etc. ?**

References

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

[2] S. Blackburn, *Enumerating finite racks, quandles and kei*, Electron. J. Combin. 20 (2013), no. 3, Paper 43, 9 pp.

[3] Bonatto, Marco *Principal and doubly homogeneous quandles.* Monatsh. Math. 191 (2020), no. 4, 691–717.

[4] Bonatto, Marco *Connected quandles of size pq and 4p.* Osaka J. Math. 59 (2022), no. 1, 145–175.

[5] Bonatto, Marco *Superconnected left quasigroups and involutory quandles.* Comm. Algebra 50 (2022), no. 9, 3978–3994.

[6] Bianco, Giuliano; Bonatto, Marco *On connected quandles of prime power order.* Beitr. Algebra Geom. 62 (2021), no. 3, 555–586.

[7] Marco Bonatto, David Stanovsk, Commutator theory for racks and quandles, J. Math. Soc. Japan 73/1 (2021), 41–75.

[8] Marco Bonatto, David Stanovsk, A universal algebraic approach to rack coverings, to appear in J. Knot Theory Ramifications.

[9] Bonatto, Marco; Fioravanti, Stefano *Mal'cev classes of left quasigroups and quandles.* Quasigroups Related Systems 29 (2021), no. 2, 177–192.

[10] J.S. Carter, *A survey of quandle ideas*, Introductory lectures on knot theory, 2253, Ser. Knots Everything, 46, World Sci. Publ., Hackensack, NJ, 2012.

[11] Clark W. E., Elhamdadi M., Saito M., Yeatman T., *Quandle colorings of knots and applications.* J. Knot Theory Ramifications 23/6 (2014), 1450035.

[12] M. Elhamdadi, S. Nelson, *Quandles: An Introduction to the Algebra of Knots*, Amer. Math. Soc., 2015.

[13] P. Etingof, A. Soloviev, R. Guralnik, *Indecomposable set-theoretical solutions to the Quantum Yang-Baxter Equation on a set with prime number of elements*, Journal of Algebra 242 (2001), 709–719.

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

[15] M. Graña, *Indecomposable racks of order* p^2, Beiträge Algebra Geom. 45 (2004), no. 2, 665–676.

[16] X. Hou, *Automorphism groups of Alexander quandles*, J. Algebra 344 (2011), 373–385.

[17] X. Hou, *Finite modules over* $\mathbb{Z}[t, t^{-1}]$, J. Knot Theory Ramifications 21 (2012), no. 8, 1250079, 28 pp.

[18] A. Hulpke, D. Stanovský, P. Vojtěchovský, *Connected quandles and transitive groups*, Journal of Pure and Applied Algebra 220 (2016), no. 2, 735–758.

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

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

[21] P. Jedlička, D. Stanovský, *Homomorphic images of affine quandles*, Algebra Universalis 82 (2021), 11 pp.

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

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

[24] S. Kamada, *Knot invariants derived from quandles and racks*, Invariants of knots and 3-manifolds (Kyoto, 2001), 103–117, Geom. Topol. Monogr., 4, Geom. Topol. Publ., Coventry, 2002.

[25] Lages, Antnio; Lopes, Pedro; Vojtchovsk, Petr *A sufficient condition for a quandle to be Latin.* J. Combin. Des. 30 (2022), no. 4, 251259.

[26] T. Nagy, *Nonaffine Latin quandles of order* 2^k. J. Algebra Appl. 20 (2021), no. 6, Paper No. 2150103, 12 pp.

[27] D. Stanovský, *Selfdistributive groupoids. A2. Non-idempotent left distributive left quasigroups*, Acta Univ. Carolinae Math. Phys. 52/2 (2011), 7–28.

[28] D. Stanovský, *A guide to self-distributive quasigroups, or latin quandles*, Quasigroups and Related Systems 23/1 (2015), 91–128.

[29] P. Vojtěchovský, S. Y. Yang, *Enumeration of racks and quandles up to isomorphism.* Math. Comp. 88 (2019), no. 319, 2523–2540.