hexagon:2611.00531v1

Which groups are automorphism groups of racks?

G. Militaru

Abstract

Every group is the automorphism group of a graph, of a magma, and even of a set-theoretic solution of the Yang–Baxter equation. We show that this is no longer true for racks and quandles: the quaternion group Q_8 is not the automorphism group of any rack, finite or infinite, and it is the smallest group with this property. In the terminology of László Babai, the categories of racks and of quandles are therefore neither universal nor finitely universal. More generally, a non-abelian group G is never the automorphism group of a rack if some element $z \neq 1$ belongs to every cyclic subgroup of G generated by a non-central element; this is the case, for instance, for all generalized quaternion groups and all Hamiltonian groups. We also prove that the dicyclic group Dic_n of order $4n$ is the automorphism group of a rack if and only if n is odd. On the positive side, we prove that the dihedral groups, the alternating groups, and the centralizers of finite families of pairwise commuting and pairwise non-conjugate non-identity permutations of a finite set are automorphism groups of finite quandles; in particular, every finite abelian group is the automorphism group of a finite quandle.

Key words: rack; quandle; automorphism group; representation problem; universal categories; set-theoretic Yang–Baxter equation; dicyclic group; Hamiltonian group

MSC 2020: Primary 20B25, 57K12; Secondary 16T25, 20D45, 08A35

Contents

1 Preliminaries **4**

2 Racks and quandles are not universal **7**

3 Groups which are automorphism groups of quandles **10**
3.1 Centralizers of commuting families of permutations 10
3.2 Augmented quandles 12
3.3 Dihedral groups, dicyclic groups and $SL(2, 3)$ 14
3.4 Conjugation quandles and alternating groups 17

4 Concluding remarks and open questions **19**

Introduction

Which abstract groups can be realized as the full automorphism group of a structure of a prescribed kind? This old question, known as the *representation problem* or *abstract group problem*, goes back to Kőnig [34] and has accompanied the development of algebra and combinatorics ever since. In Babai's terminology [4], an object $\mathcal{O}$ of a category $\mathcal{C}$ *represents* a group G if $\mathrm{Aut}(\mathcal{O}) \cong G$; the category $\mathcal{C}$ is

universal if every group is represented by an object of $\mathcal{C}$, and *finitely universal* if every finite group is represented by a "finite" object of $\mathcal{C}$ [5, Section 4.1]. The first and best known answer is Frucht's theorem [28]: the category of graphs is finitely universal, i.e. every finite group is the automorphism group of a finite graph. Two decades later, de Groot [19] and Sabidussi [45] proved, independently, that it is also universal. Under the name of the abstract group problem, the same question is the starting point of the theory of representations of groups and categories developed in [43]. For more details on this classical problem, which is still of current interest, see [4, 5, 39, 43] and the references therein.

Babai also pointed out that positive answers are the rule rather than the exception: even the category of fields is universal [5, Section 4.1]. The exceptions are therefore all the more interesting. The best known one concerns groups themselves: there is no group whose automorphism group is cyclic of order 3, so the category of groups is neither universal nor finitely universal. The reason is structural: the automorphism group of a group G always contains the normal subgroup $\mathrm{Inn}(G) \cong G/Z(G)$ of inner automorphisms, and this imposes strong restrictions on $\mathrm{Aut}(G)$. Another exception, of a different nature, is the category of all left non-degenerate solutions of the Frobenius–Separability equation, which is not universal either: the automorphism groups of these objects are precisely the centralizers of single maps, and not every group is of this form [2, Theorems 2.19 and 4.2].

In [39] we addressed the representation problem for the category $\mathcal{YB}$ of all set-theoretic solutions of the Yang–Baxter equation, and we showed that this category is universal and finitely universal [39, Theorem 2.18]. In the same spirit, the centralizer of any finite family of maps is the automorphism group of an idempotent solution of the braid equation [41, Theorem 3.1].

In this paper we consider the same problem for the category $\mathcal{R}\mathrm{ack}$ of all racks and the category $\mathcal{Q}\mathrm{nd}$ of all quandles. Via the *derived solutions* recalled below, $\mathcal{R}\mathrm{ack}$ is a full subcategory of $\mathcal{YB}$; nevertheless, unlike $\mathcal{YB}$, neither $\mathcal{R}\mathrm{ack}$ nor $\mathcal{Q}\mathrm{nd}$ is universal or finitely universal.

Racks and quandles are, by now, classical objects. Their axioms are the algebraic counterparts of the Reidemeister moves of knot diagrams: Joyce [33] and Matveev [38] associated, independently, a quandle with every knot and proved that it is an almost complete invariant of knots, while racks were developed by Fenn and Rourke [25] in connection with framed links. Racks are equally important in the theory of quantum groups: the braided vector spaces arising from groups, whose Nichols algebras are a key step in the classification of finite-dimensional pointed Hopf algebras, are described by racks and 2-cocycles [3, Theorem 4.14], and this led Andruskiewitsch and Graña to a classification of all finite simple racks [3, Theorems 3.9 and 3.12]. Quandles have recently been proposed also as a framework for the observables of physical theories [27]. For more details on the theory of racks and quandles, see the monographs [9, 23] and the references therein.

In view of their role in the theory of braided vector spaces, it is not surprising that racks also provide solutions of the celebrated quantum Yang–Baxter equation in its set-theoretic form. In fact, they are a natural and very rich source of bijective non-degenerate solutions of the braid equation: for instance, they are far more numerous than the solutions arising from skew left braces, as Table 1 below shows. If $(X, \triangleleft)$ is a rack, then

$$R\colon X \times X \to X \times X, \qquad R(x, y) := (y, x \triangleleft y)$$

is a bijective non-degenerate solution of the braid equation, as first observed in 1988 by Brieskorn [16] (see also [9, Remark 6.2]), and $\mathrm{Aut}(X, R) = \mathrm{Aut}(X, \triangleleft)$.

The automorphism groups of racks and quandles have been studied intensively, but in the opposite direction to the one considered in this paper: a rack or a quandle, usually constructed from a group

or a module, is given, and its automorphism group is computed. This has been done for the quandles of small order [22, 30, 37, 46], the dihedral quandles [22], the Alexander quandles [11, 26, 31], the conjugation and Takasaki quandles of groups [8, 10, 47],[1] the extensions of quandles [10, 12], and the quandles with one non-trivial column [17]; see also [9, Chapter 8] and the references therein. The representation problem asks the converse question:

Given a group G, is there a rack or a quandle whose automorphism group is isomorphic to G?

As far as we know, this question has not been considered before, and the answer turns out to be negative. As in the classical case of groups, the obstruction comes from the inner automorphisms: the inner automorphism group $\mathrm{Inn}(X)$ of a rack X is a normal subgroup of $\mathrm{Aut}(X)$ [33]. The proof is based on a simple observation (Lemma 2.1): if $G = \mathrm{Aut}(X)$ and $x \in X$, then every element of G which normalizes the stabilizer G_x and commutes with the right translation r_x belongs to $G_x\, Z(G)$. Applied to a point x which is moved by a suitable central element of G, this gives a general obstruction (Theorem 2.2), and we obtain:

Theorem A. *(1) Let G be a non-abelian group and assume that there exists $1 \neq z \in G$ such that $z \in \langle g \rangle$, for all $g \in G \setminus Z(G)$. Then G is not isomorphic to the automorphism group of any rack, finite or infinite. This is the case for the groups $Q_{2^m} \times E \times A$, where Q_{2^m} is a generalized quaternion group, E is an elementary abelian 2-group and A is an abelian group whose elements have odd order; in particular, no Hamiltonian group is the automorphism group of a rack.*

(2) The dicyclic group Dic_n of order $4n$, $n \geq 2$, is isomorphic to the automorphism group of a rack if and only if n is odd; in this case, Dic_n is the automorphism group of a quandle with $n + 4$ elements.

(3) The quaternion group Q_8 is the smallest group which is not isomorphic to the automorphism group of a rack or of a quandle.

Consequently, the categories of racks and of quandles are neither universal nor finitely universal.

Theorem A is proved in Section 2 (Corollary 2.3, Corollary 2.4, Corollary 2.5 and Corollary 2.6) and Section 3 (Proposition 3.9 and Corollary 3.3). It also shows that a Frucht-type theorem for non-degenerate solutions of the braid equation, if it exists, cannot be obtained from racks. For comparison, Q_8 is the automorphism group of a degenerate (bipartite) solution on a set with 11 elements [39, Example 2.22]. The obstruction of Theorem A is subtle: for instance, the groups $\mathrm{Dic}_6 \cong C_3 \rtimes Q_8$ and $SL(2,\, 3) \cong Q_8 \rtimes C_3$ both have order 24 and a unique involution, but only the second one is the automorphism group of a quandle. On the positive side, we prove in Section 3:

Theorem B. *(1) Let $g_1, \ldots, g_k$ be pairwise commuting and pairwise non-conjugate permutations of a set Z, all different from Id_Z. Then the centralizer $\mathrm{Aut}(g_1, \ldots, g_k)$ of $g_1, \ldots, g_k$ in $\mathrm{Sym}(Z)$ is the automorphism group of a quandle on a set with $|Z| + k$ elements. In particular, every finite abelian group $C_{n_1} \times \cdots \times C_{n_k}$ is the automorphism group of a quandle with $k + n_1 + \cdots + n_k$ elements.*

(2) For any $n \geq 3$, the dihedral group D_n of order $2n$ is the automorphism group of a quandle with $n + 2$ elements.

(3) Every alternating group A_n and every symmetric group S_n is the automorphism group of a finite quandle.

(4) The group $SL(2,\, 3)$ is the automorphism group of a quandle with 8 elements.

[1] For instance, $\mathrm{Aut}\big(\mathrm{Conj}(G)\big) = \mathrm{Aut}(G)$ if and only if $Z(G) = 1$ [10, Corollary 4.4].

Theorem B is proved in Section 3: part (1) in Proposition 3.1 and Corollary 3.2, part (2) in Proposition 3.7, part (3) in Corollary 3.13 and part (4) in Proposition 3.10. Part (1) is the analogue for quandles of [41, Theorem 3.1], where the centralizer of an arbitrary finite family of maps is realized as the automorphism group of an idempotent solution of the braid equation. In view of Theorem A, such a result cannot hold for arbitrary finite families of permutations: for instance, Q_8 is the centralizer in $\mathrm{Sym}(Q_8)$ of the left translations by two generators of Q_8. Part (2) should be compared with [22, Theorem 2.1]: the automorphism group of the dihedral quandle with n elements is the affine group $\mathrm{Aff}(\mathbb{Z}_n)$, which is isomorphic to D_n only for $n \in \{3, 4, 6\}$; adding two points to the dihedral quandle we get rid of all the extra automorphisms. The quandles of parts (2) and (4), as well as those of Theorem A(2), are augmented quandles in the sense of Joyce and Fenn–Rourke, for which we give a general criterion (Proposition 3.4); the quandles of part (3) are conjugation quandles of groups with trivial center (Proposition 3.11). We end the paper with some open questions (Section 4).

1 Preliminaries

Given a set X, $\mathrm{Sym}(X)$ denotes the symmetric group on X, i.e. the group of all bijections $X \to X$, and $\tau_X \colon X \times X \to X \times X$, $\tau_X(x, y) := (y, x)$, is the flip map. For a map $R \colon X \times X \to X \times X$ we use the usual notation $R^{12} := R \times \mathrm{Id}_X$ and $R^{23} := \mathrm{Id}_X \times R$. The map R is called a solution of the *braid equation* if

$$R^{12}R^{23}R^{12} = R^{23}R^{12}R^{23}. \tag{1.1}$$

A *morphism* of solutions $\sigma \colon (X, R) \to (X', R')$ is a map $\sigma \colon X \to X'$ such that $(\sigma \times \sigma) \circ R = R' \circ (\sigma \times \sigma)$. We denote by $\mathcal{BR}$ the category of all solutions of the braid equation, i.e. its objects are the pairs (X, R) consisting of a set X and a solution R of the braid equation on X. The *automorphism group* $\mathrm{Aut}(X, R)$ of (X, R) is the group of all bijections $\sigma \colon X \to X$ which are morphisms of solutions $(X, R) \to (X, R)$. A map R is a solution of the braid equation if and only if $\tau_X \circ R$ is a solution of the Yang–Baxter equation, and $(X, R) \mapsto (X, \tau_X \circ R)$ is an isomorphism between $\mathcal{BR}$ and the category $\mathcal{YB}$ of all set-theoretic solutions of the Yang–Baxter equation, which preserves the automorphism groups [39, Section 1]. For this reason, in what follows we shall work only with the braid equation.

Following [2, Definition 1.1], the *centralizer* of a family $(f_i)_{i \in I}$ of maps $f_i \colon Z \to Z$ is the subgroup of $\mathrm{Sym}(Z)$ given by

$$\mathrm{Aut}(f_i,\, i \in I) := \{\beta \in \mathrm{Sym}(Z) \,|\, \beta \circ f_i = f_i \circ \beta, \text{ for all } i \in I\}.$$

We use the standard notation from group theory. Let G be a group. If G acts on a set X, then G_x and Gx denote the stabilizer and the orbit of $x \in X$; a subgroup of $\mathrm{Sym}(X)$ acts on X in the obvious way. For a subgroup $K \leq G$ and a subset $S \subseteq G$, we denote by $N_G(K)$, $C_G(S)$ and $Z(G)$ the normalizer of K, the centralizer of S and the center of G. Moreover, $\mathrm{core}_G(K) := \bigcap_{g \in G} gKg^{-1}$ is the core of K, i.e. the kernel of the action of G on the set G/K of left cosets, and $\kappa_g \colon G \to G$, $\kappa_g(h) := ghg^{-1}$, is the inner automorphism of G defined by $g \in G$. An *involution* of G is an element of order 2. As usual, C_n, D_n, S_n and A_n denote the cyclic group of order n, the dihedral group of order $2n$, the symmetric group and the alternating group of degree n.

Racks and quandles. A *magma* [15, Definition 1] is a set X endowed with a binary operation $(x, y) \mapsto x \triangleleft y$. For $x \in X$ we denote by l_x, $r_x \colon X \to X$ the left and right translations of the magma $(X, \triangleleft)$, i.e.

$$l_x(y) := x \triangleleft y, \qquad r_x(y) := y \triangleleft x, \qquad \text{for all } y \in X.$$

A morphism of magmas $\varphi\colon (X, \triangleleft) \to (X', \triangleleft')$ is a map $\varphi\colon X \to X'$ such that

$$\varphi(x \triangleleft y) = \varphi(x) \triangleleft' \varphi(y), \qquad \text{for all } x, y \in X.$$

The bijective endomorphisms of a magma $(X, \triangleleft)$ are its automorphisms; they form a subgroup of $\mathrm{Sym}(X)$, denoted by $\mathrm{Aut}(X, \triangleleft)$, or simply by $\mathrm{Aut}(X)$. Since $\varphi(x \triangleleft y) = \varphi\big(r_y(x)\big)$ and $\varphi(x) \triangleleft \varphi(y) = r_{\varphi(y)}\big(\varphi(x)\big)$, a bijection $\varphi\colon X \to X$ is an automorphism of $(X, \triangleleft)$ if and only if

$$\varphi \circ r_y \circ \varphi^{-1} = r_{\varphi(y)}, \qquad \text{for all } y \in X. \tag{1.2}$$

The category of magmas is universal and finitely universal [39, Remark 1.2]; the results of this paper show that this is no longer true for the magmas satisfying the identities which define racks or quandles.

A *rack* is a magma $(X, \triangleleft)$ whose right translations are automorphisms of $(X, \triangleleft)$; that is, for any $z \in X$, the right translation r_z is a bijection and

$$(x \triangleleft y) \triangleleft z = (x \triangleleft z) \triangleleft (y \triangleleft z), \qquad \text{for all } x, y \in X. \tag{1.3}$$

A rack $(X, \triangleleft)$ is called a *quandle* if $x \triangleleft x = x$, for all $x \in X$, and it is called *trivial* if $x \triangleleft y = x$, for all $x, y \in X$; the automorphism group of a trivial rack is $\mathrm{Sym}(X)$. Applying (1.2) to the bijections $\varphi = r_z$, we obtain that a magma $(X, \triangleleft)$ whose right translations are bijective is a rack if and only if

$$r_z \circ r_y \circ r_z^{-1} = r_{r_z(y)}, \qquad \text{for all } y, z \in X. \tag{1.4}$$

A morphism of racks is a morphism of the underlying magmas. We denote by $\mathcal{R}\mathrm{ack}$ the category of racks and by $\mathcal{Q}\mathrm{nd}$ its full subcategory of quandles. For a rack $(X, \triangleleft)$, the subgroup of $\mathrm{Aut}(X)$ generated by the right translations r_z, $z \in X$, is called the *inner automorphism group* of X and is denoted by $\mathrm{Inn}(X)$; by (1.2), $\mathrm{Inn}(X)$ is a normal subgroup of $\mathrm{Aut}(X)$. For more details on racks and quandles we refer to [9, 23].

Let $(X, \triangleleft)$ be a rack. Then the map

$$R = R^{\triangleleft}\colon X \times X \to X \times X, \qquad R(x, y) := (y, x \triangleleft y), \tag{1.5}$$

is a bijective non-degenerate [24, Definition 1.1] solution of the braid equation, called the *derived solution* of the rack $(X, \triangleleft)$ [16] (see also [9, Remark 6.2]). Let $(X', \triangleleft')$ be another rack and $\varphi\colon X \to X'$ a map. Since

$$(\varphi \times \varphi)\big(R^{\triangleleft}(x, y)\big) = \big(\varphi(y), \varphi(x \triangleleft y)\big) \qquad \text{and} \qquad R^{\triangleleft'}\big(\varphi(x), \varphi(y)\big) = \big(\varphi(y), \varphi(x) \triangleleft' \varphi(y)\big),$$

φ is a morphism of solutions $(X, R^{\triangleleft}) \to (X', R^{\triangleleft'})$ if and only if it is a morphism of racks. Hence $(X, \triangleleft) \mapsto (X, R^{\triangleleft})$ is a fully faithful functor, injective on objects,

$$\mathcal{R}\mathrm{ack} \hookrightarrow \mathcal{BR}, \tag{1.6}$$

which identifies $\mathcal{R}\mathrm{ack}$ with a full subcategory of $\mathcal{BR}$, and hence of $\mathcal{YB}$. In particular, for any rack $(X, \triangleleft)$ we have

$$\mathrm{Aut}(X, R^{\triangleleft}) = \mathrm{Aut}(X, \triangleleft). \tag{1.7}$$

Thus all the results below on automorphism groups of racks can be equivalently stated for the derived solutions of racks.

Remark 1.1. The embedding (1.6) has a left adjoint $\mathcal{F}\colon \mathcal{BR} \to \mathcal{R}\mathrm{ack}$. Its existence follows from Freyd's adjoint functor theorem [13, Corollary 8.17], exactly as in [1, Section 3]; it is the rack version of [36, Theorem 9], [48, Theorem 4.5] and [7, Theorem 3.20]. Explicitly, for a solution (X, R) of the braid equation, written as $R(x, y) = (x \cdot y, x * y)$, $\mathcal{F}(X, R)$ is the rack generated by the set X with the relations

$$x \cdot y = y \qquad \text{and} \qquad x * y = x \triangleleft y, \qquad \text{for all } x, y \in X,$$

i.e. the quotient of the free rack on X [25] by the smallest congruence containing these relations. The canonical map $\eta\colon X \to \mathcal{F}(X, R)$ is a morphism of solutions from (X, R) to the derived solution of $\mathcal{F}(X, R)$, and it is universal: for any rack $(Y, \triangleleft)$ and any morphism of solutions $\theta\colon (X, R) \to (Y, R^{\triangleleft})$ there exists a unique morphism of racks $u\colon \mathcal{F}(X, R) \to Y$ such that $u \circ \eta = \theta$. Consequently, η is injective if and only if (X, R) is isomorphic to a subsolution of the derived solution of a rack. This is not always the case: for $R = \mathrm{Id}_{X\times X}$ we have $x \cdot y = x$, the relations give $\eta(x) = \eta(y)$, for all x, $y \in X$, and $\mathcal{F}(X, \mathrm{Id}_{X\times X})$ is the rack with one element.

Remark 1.2. Racks and skew left braces both form varieties of algebras which produce bijective non-degenerate solutions of the braid equation, so it is natural to ask which of them produces more solutions. By the above discussion, two racks are isomorphic if and only if their derived solutions are isomorphic; hence the number of isomorphism classes of derived solutions of racks (resp. of quandles) on a set with n elements is the number $r(n)$ of racks (resp. the number $q(n)$ of quandles) of order n up to isomorphism. These numbers were computed for $n \leq 13$ by Vojtěchovský and Yang [50, Tables 1 and 2][2]; for $n \leq 7$ we confirmed them with an independent computer program, based on the Cauchy–Frobenius lemma. They are recorded in Table 1, together with the number $s(n)$ of isomorphism classes of solutions of the braid equation on a set with n elements which arise from skew left braces, i.e. which are isomorphic to the solution R_B associated to a skew left brace B [29, Theorem 3.1]. For $n \leq 6$, the numbers $s(n)$ were computed in [40, Tables 3 and 5], where the corresponding Yang–Baxter solutions $\tau_X \circ R_B$ are counted, and $s(7) = 1$, since there is only one skew left brace of order 7 up to isomorphism [29, Table 5.1].

n	1	2	3	4	5	6	7
derived solutions of racks, $r(n)$	1	2	6	19	74	353	2080
derived solutions of quandles, $q(n)$	1	1	3	7	22	73	298
solutions arising from skew left braces, $s(n)$	1	1	1	2	1	6	1

Table 1: Isomorphism classes of solutions of the braid equation on a set with n elements: derived solutions of racks and of quandles, and solutions arising from skew left braces.

Thus the derived solutions of racks are much more numerous than the solutions arising from skew left braces: for instance, for $n = 7$ there are 2080 isomorphism classes of derived solutions of racks, and only one isomorphism class of solutions arising from skew left braces.

Dicyclic groups. For $n \geq 2$, the *dicyclic group* of order $4n$, also called the binary dihedral group, is the group given by generators and relations

$$\mathrm{Dic}_n := \langle a, b \,|\, a^{2n} = 1,\ b^2 = a^n,\ bab^{-1} = a^{-1} \rangle,$$

see [44, pp. 347–348]. For $n = 2^{m-2}$, with $m \geq 3$, Dic_n is the *generalized quaternion group* Q_{2^m} of order 2^m [18]; in particular, $\mathrm{Dic}_2 = Q_8$ is the quaternion group. The group Dic_n has $4n$ elements,

[2] In [50] racks are defined by the left self-distributive law $x * (y * z) = (x * y) * (x * z)$. A magma $(X, \triangleleft)$ is a rack in our sense if and only if $(X, *)$, with $x * y := y \triangleleft x$, is a rack in the sense of [50], and the two structures have the same isomorphisms.

the subgroup $\langle a\rangle$ is cyclic of order $2n$, and every element of Dic_n can be written uniquely as a^k or $a^k b$, with $0 \le k < 2n$ [14, Proposition 1.1]; that is, $\mathrm{Dic}_n = \langle a\rangle \sqcup \langle a\rangle b$. The relation $bab^{-1} = a^{-1}$ gives $ba^k = a^{-k}b$, for all $k \in \mathbb{Z}$. The following elementary properties of the dicyclic groups are well known; see, for instance, [14, Section 1], where the center of Dic_n and the orders of its elements are computed. Since they will be used several times, we include a short proof for the reader's convenience.

Lemma 1.3. *Let $G := \mathrm{Dic}_n$, $n \ge 2$, and $z := a^n$. Then:*

(1) every element $g \in G \setminus \langle a\rangle$ has order 4, $g^2 = z$, and g acts on $\langle a\rangle$ by inversion, i.e. $g\,a^k\,g^{-1} = a^{-k}$, for all $k \in \mathbb{Z}$;

(2) z is the unique involution of G, and $Z(G) = \langle z\rangle$;

(3) every subgroup of $\langle a\rangle$ is a normal subgroup of G, and $C_G(a^k) = \langle a\rangle$, for all $a^k \notin \langle z\rangle$;

(4) $C_G(b) = \langle b\rangle = \{1,\, z,\, b,\, zb\}$, and the conjugacy class of b in G is $\{a^{2j}b \,|\, j \in \mathbb{Z}\}$.

Proof. (1) Let $g = a^j b$. Using $ba^k = a^{-k}b$ and $b^2 = a^n = z$, we obtain

$$g\,a^k\,g^{-1} = a^j\,(b\,a^k\,b^{-1})\,a^{-j} = a^{-k} \qquad \text{and} \qquad g^2 = a^j\,(b\,a^j\,b^{-1})\,b^2 = z.$$

As z has order 2, g has order 4.

(2) The cyclic group $\langle a\rangle$ of order $2n$ has a unique involution, namely $z = a^n$, and by (1) the elements of $G\setminus\langle a\rangle$ are not involutions. An element a^k is central if and only if it commutes with b, i.e. $a^{-k} = a^k$, i.e. $a^k \in \langle z\rangle$. By (1), no element $g \in G \setminus \langle a\rangle$ is central, since $gag^{-1} = a^{-1} \ne a$, as $n \ge 2$. Hence $Z(G) = \langle z\rangle$.

(3) By (1), $g\langle a^k\rangle g^{-1} = \langle a^{-k}\rangle = \langle a^k\rangle$, for all $g \in G \setminus \langle a\rangle$; this proves the first statement, since $\langle a\rangle$ is abelian. If $a^k \notin \langle z\rangle$, then $a^{-k} \ne a^k$; hence, by (1), no element of $G \setminus \langle a\rangle$ commutes with a^k, and $C_G(a^k) = \langle a\rangle$.

(4) As in the proof of (2), a^j commutes with b if and only if $a^j \in \langle z\rangle$; moreover, $a^j b$ commutes with b if and only if a^j does. Hence $C_G(b) = \{1,\, z,\, b,\, zb\}$, which is the cyclic subgroup generated by b, as $b^2 = z$ and $b^3 = zb$. Finally, for all $j \in \mathbb{Z}$ we have

$$a^j\,b\,a^{-j} = a^{2j}b \qquad \text{and} \qquad (a^j b)\,b\,(a^j b)^{-1} = a^j\,b\,a^{-j} = a^{2j}b,$$

which proves the last statement. □

2 Racks and quandles are not universal

In this section we prove a general obstruction for a group to be the automorphism group of a rack (Theorem 2.2), and we apply it to the Hamiltonian groups and to the dicyclic groups. The key ingredient is the following lemma: if $G = \mathrm{Aut}(X)$, then the elements of G which normalize the stabilizer of a point $x \in X$ and commute with the right translation r_x are central, up to an element of the stabilizer.

Lemma 2.1. *Let $(X, \triangleleft)$ be a rack, $G := \mathrm{Aut}(X)$ and $x \in X$. Then:*

(1) $r_x \in C_G(G_x)$, i.e. the right translation r_x commutes with all elements of the stabilizer G_x;

(2) for any $m \in N_G(G_x) \cap C_G(r_x)$ there exists $\zeta \in Z(G)$ such that $m \in \zeta\,G_x$ and $\zeta(y) = y$, for all $y \in X \setminus Gx$. In particular,

$$N_G(G_x) \cap C_G(r_x) \subseteq G_x\,Z(G). \tag{2.1}$$

Proof. (1) By the definition of a rack, $r_x \in G$. If $\varphi \in G_x$, then (1.2) gives $\varphi \circ r_x \circ \varphi^{-1} = r_{\varphi(x)} = r_x$.

(2) Let $m \in N_G(G_x) \cap C_G(r_x)$ and let $O := Gx$ be the orbit of x. We define $\psi\colon X \to X$ by

$$\psi(\varphi(x)) := \varphi(m(x)), \text{ for all } \varphi \in G, \qquad \text{and} \qquad \psi(y) := y, \text{ for all } y \in X \setminus O.$$

The map ψ is well defined: if $\varphi(x) = \varphi'(x)$, with φ, $\varphi' \in G$, then $\varphi^{-1}\varphi' \in G_x$, hence $m^{-1}\varphi^{-1}\varphi' m \in G_x$, since m normalizes G_x; that is, $\varphi(m(x)) = \varphi'(m(x))$. The same construction, applied to $m^{-1} \in N_G(G_x) \cap C_G(r_x)$, gives the inverse of ψ; thus $\psi \in \mathrm{Sym}(X)$. Moreover, ψ commutes with all elements of G: for g, $\varphi \in G$ we have

$$\psi(g\varphi(x)) = g\varphi(m(x)) = g(\psi(\varphi(x))),$$

and ψ is the identity on $X \setminus O$, which is a G-invariant subset of X.

We prove now that ψ is an automorphism of $(X, \triangleleft)$, i.e. that ψ satisfies (1.2). Let $y \in X$. Since $r_y \in G$ commutes with ψ, we have $\psi \circ r_y \circ \psi^{-1} = r_y$, so we have to show that $r_{\psi(y)} = r_y$. This is obvious for $y \in X \setminus O$. For $y = \varphi(x) \in O$, we apply (1.2) to the automorphisms φm and φ, and we use that m commutes with r_x:

$$r_{\psi(\varphi(x))} = r_{\varphi m(x)} = (\varphi m) \circ r_x \circ (\varphi m)^{-1} = \varphi \circ r_x \circ \varphi^{-1} = r_{\varphi(x)}.$$

Thus $\psi \in G$ and, since ψ commutes with all elements of G, we obtain that $\zeta := \psi \in Z(G)$. By construction, ζ is the identity on $X \setminus Gx$ and $\zeta(x) = m(x)$, i.e. $\zeta^{-1}m \in G_x$. Hence $m \in \zeta\, G_x \subseteq G_x\, Z(G)$, which proves (2.1). □

We can now prove the main result of this section.

Theorem 2.2. *Let G be a group and $1 \neq z \in Z(G)$ such that, for every subgroup $K \leq G$ with $z \notin K$ and every $c \in C_G(K)$, we have*

$$N_G(K) \cap C_G(c) \not\subseteq K\, Z(G). \tag{2.2}$$

Then there is no rack $(X, \triangleleft)$, finite or infinite, such that $\mathrm{Aut}(X) \cong G$.

Proof. Assume that $(X, \triangleleft)$ is a rack such that $\mathrm{Aut}(X) \cong G$; we identify $G = \mathrm{Aut}(X) \leq \mathrm{Sym}(X)$. Since $z \neq \mathrm{Id}_X$, there exists $x \in X$ such that $z(x) \neq x$, i.e. $z \notin K := G_x$. By Lemma 2.1(1), $c := r_x \in C_G(K)$, and by Lemma 2.1(2), $N_G(K) \cap C_G(c) \subseteq K\, Z(G)$. This contradicts (2.2). □

The hypothesis of Theorem 2.2 can be easily checked in many cases. The first one is the following:

Corollary 2.3. *Let G be a non-abelian group and assume that there exists $1 \neq z \in G$ such that $z \in \langle g \rangle$, for all $g \in G \setminus Z(G)$. Then G is not isomorphic to the automorphism group of any rack, finite or infinite.*

Proof. The element z commutes with all $g \in G \setminus Z(G)$, since $z \in \langle g \rangle$, and with all central elements; hence $z \in Z(G)$. Let $K \leq G$ be a subgroup with $z \notin K$, and let $c \in C_G(K)$. By assumption, K contains no element of $G \setminus Z(G)$, i.e. $K \subseteq Z(G)$; hence $N_G(K) = G$ and $K\, Z(G) = Z(G)$. Assume that (2.2) does not hold. Then

$$C_G(c) = N_G(K) \cap C_G(c) \subseteq Z(G).$$

In particular, $c \in Z(G)$, hence $G = C_G(c) \subseteq Z(G)$, i.e. G is abelian, a contradiction. Thus (2.2) holds, and the conclusion follows from Theorem 2.2. □

Recall that a *Hamiltonian group* is a non-abelian group all of whose subgroups are normal. By the theorem of Dedekind [20] (for finite groups) and Baer [6], the Hamiltonian groups are precisely the groups $Q_8 \times E \times A$, where E is an elementary abelian 2-group and A is an abelian group all of whose elements have odd order.

Corollary 2.4. *Let $m \geq 3$, let E be an elementary abelian 2-group and A an abelian group all of whose elements have odd order (E and A can be infinite). Then the group $Q_{2^m} \times E \times A$ is not isomorphic to the automorphism group of any rack. In particular, no Hamiltonian group is isomorphic to the automorphism group of a rack.*

Proof. Let $Q := Q_{2^m} = \mathrm{Dic}_{2^{m-2}}$ and $G := Q \times E \times A$. By Lemma 1.3(2), Q has a unique involution z_0 and $Z(Q) = \langle z_0 \rangle$; hence $Z(G) = \langle z_0 \rangle \times E \times A$. We show that $z := (z_0, 1, 1)$ satisfies the hypothesis of Corollary 2.3. Let $g = (q, e, t) \in G \setminus Z(G)$, i.e. $q \notin \langle z_0 \rangle$. Then q is neither trivial nor an involution, so its order is 2^s, with $s \geq 2$, and $q^{2^{s-1}} = z_0$, since z_0 is the unique involution of Q. Let o be the order of t, which is odd. Since $e^2 = 1$, $t^o = 1$ and 2^{s-1} is even, we obtain

$$g^{o\,2^{s-1}} = (z_0^o,\, e^{o\,2^{s-1}},\, t^{o\,2^{s-1}}) = (z_0,\, 1,\, 1) = z.$$

Thus $z \in \langle g \rangle$, for all $g \in G \setminus Z(G)$, and the conclusion follows from Corollary 2.3. The last statement follows from the theorem of Dedekind and Baer recalled above. □

If n is even but not a power of 2, then the dicyclic group Dic_n does not satisfy the hypothesis of Corollary 2.3: if $d > 1$ is the largest odd divisor of n, then $a^{2n/d}$ is a non-central element of odd order d, and the cyclic subgroup that it generates does not contain the involution $z = a^n$. Nevertheless, Theorem 2.2 can still be applied.

Corollary 2.5. *Let $n \geq 2$ be an even integer. Then the dicyclic group Dic_n is not isomorphic to the automorphism group of any rack, finite or infinite.*

Proof. Let $G := \mathrm{Dic}_n$ and $z := a^n$; by Lemma 1.3(2), z is the unique involution of G and $Z(G) = \langle z \rangle$. Let $K \leq G$ be a subgroup with $z \notin K$, and let $c \in C_G(K)$. Then K contains no involution, so it has odd order; by Lemma 1.3(1), $K \subseteq \langle a \rangle$, hence K is a normal subgroup of G, by Lemma 1.3(3). Thus

$$N_G(K) \cap C_G(c) = C_G(c),$$

while $K\,Z(G) = K \times \langle z \rangle$ has order $2|K|$, with $|K|$ odd, and therefore contains no element of order 4. On the other hand, $C_G(c)$ contains an element of order 4. Indeed, if $c \notin \langle a \rangle$, then c itself has order 4, by Lemma 1.3(1); if $c \in \langle a \rangle$, then $C_G(c)$ contains the cyclic group $\langle a \rangle$, whose order $2n$ is divisible by 4, as n is even. Hence (2.2) holds, and the conclusion follows from Theorem 2.2. □

In the terminology of Babai recalled in the Introduction, we obtain:

Corollary 2.6. *The category of racks and the category of quandles are neither universal nor finitely universal: the quaternion group Q_8 is not represented by any rack, finite or infinite. The same holds for the class of derived solutions $R(x, y) = (y, x \triangleleft y)$ of racks, regarded as a class of solutions of the braid equation.*

Proof. By Corollary 2.5, applied for $n = 2$, the group $\mathrm{Dic}_2 = Q_8$ is not isomorphic to $\mathrm{Aut}(X)$, for any rack $(X, \triangleleft)$; in particular, for any quandle. The last statement follows from (1.7). □

Remark 2.7. Theorem 2.2 and its corollaries also apply to a class of involutive solutions. Let

$$R\colon X\times X\to X\times X,\qquad R(x,\,y)=(\sigma_x(y),\,\sigma^{-1}_{\sigma_x(y)}(x)),$$

be an involutive left non-degenerate solution of the braid equation [24], where $\sigma_x\in\mathrm{Sym}(X)$, for all $x\in X$, and assume that $\sigma_{\sigma_x(y)}=\sigma_y$, for all $x,\,y\in X$. The braid equation gives

$$\sigma_x\circ\sigma_y=\sigma_{\sigma_x(y)}\circ\sigma_{\sigma^{-1}_{\sigma_x(y)}(x)},\qquad\text{for all } x,\,y\in X.$$

The assumption, applied to the elements u and $\sigma_u^{-1}(x)$, gives $\sigma_x=\sigma_{\sigma_u^{-1}(x)}$, for all $u,\,x\in X$; hence the right hand side above is $\sigma_y\circ\sigma_x$, i.e. the permutations σ_x commute pairwise. Therefore

$$\sigma_z\circ\sigma_y\circ\sigma_z^{-1}=\sigma_y=\sigma_{\sigma_z(y)},\qquad\text{for all } y,\,z\in X,$$

which is exactly (1.4) for the magma $(X,\,\triangleleft)$ given by $x\triangleleft y:=\sigma_y(x)$; thus $(X,\,\triangleleft)$ is a rack. Moreover, a bijection φ of X is an automorphism of $(X,\,R)$ if and only if $\varphi\circ\sigma_x\circ\varphi^{-1}=\sigma_{\varphi(x)}$, for all $x\in X$ (the condition on the second component of R follows from this one), i.e. if and only if $\varphi\in\mathrm{Aut}(X,\,\triangleleft)$, by (1.2). Hence $\mathrm{Aut}(X,\,R)=\mathrm{Aut}(X,\,\triangleleft)$; for instance, the automorphism group of such a solution is never isomorphic to a Hamiltonian group, or to a dicyclic group Dic_n with n even. This does not contradict [39, Theorem 2.18], where every group is realized as the automorphism group of an involutive solution of the braid equation: the bipartite solutions used there are degenerate.

On the other hand, for an arbitrary bijective non-degenerate solution $(X,\,R)$ of the braid equation, $\mathrm{Aut}(X,\,R)$ is only a subgroup of the automorphism group of its derived rack [49, 35], which in general does not contain the inner automorphisms of the derived rack; hence Theorem 2.2 does not apply (see Section 4).

3 Groups which are automorphism groups of quandles

In this section we show that several classical families of groups are automorphism groups of quandles: the centralizers of commuting families of permutations, in particular all finite abelian groups (Subsection 3.1), the dihedral groups, the dicyclic groups Dic_n with n odd and the group $SL(2,\,3)$ (Subsection 3.3), and the alternating groups (Subsection 3.4).

3.1 Centralizers of commuting families of permutations

The next result is the analogue for quandles of [41, Theorem 3.1]. For $k=1$, $Y=\{0\}$ and $Z=\{1,\dots,n\}$, the quandle $(X,\,\triangleleft)$ below is the quandle P_n^σ with one non-trivial column of Cazet [17], with $\sigma=g_1$, and Proposition 3.1 recovers [17, Theorem 3.4].

Proposition 3.1. *Let Z be a set, $Y=\{y_1,\dots,y_k\}$ a set with $k\geq 1$ elements disjoint from Z, and $g_1,\dots,g_k\in\mathrm{Sym}(Z)\setminus\{\mathrm{Id}_Z\}$ pairwise commuting permutations. On $X:=Y\sqcup Z$ we define the binary operation*

$$x\triangleleft y_i:=\begin{cases}x, & \text{if } x\in Y,\\ g_i(x), & \text{if } x\in Z,\end{cases}\qquad\qquad x\triangleleft z:=x,\ \text{for all } x\in X,\ z\in Z;$$

that is, the right translations are

$$r_{y_i}=\mathrm{Id}_Y\sqcup g_i,\qquad r_z=\mathrm{Id}_X,\qquad \text{for all } i=1,\dots,k \text{ and } z\in Z,$$

where $\alpha \sqcup \beta$ denotes the bijection of $X = Y \sqcup Z$ which is equal to $\alpha \in \mathrm{Sym}(Y)$ on Y and to $\beta \in \mathrm{Sym}(Z)$ on Z. Then $(X, \triangleleft)$ is a quandle, and the map

$$H_g := \Big\{(\alpha, \beta) \in \mathrm{Sym}(Y) \times \mathrm{Sym}(Z) \,\big|\, \beta \circ g_i \circ \beta^{-1} = g_j \text{ whenever } \alpha(y_i) = y_j\Big\} \to \mathrm{Aut}(X),$$
$$(\alpha, \beta) \mapsto \alpha \sqcup \beta,$$

is an isomorphism of groups. If, moreover, $g_1, \ldots, g_k$ are pairwise non-conjugate in $\mathrm{Sym}(Z)$, then

$$\mathrm{Aut}(X) = \{\mathrm{Id}_Y \sqcup \beta \,|\, \beta \in \mathrm{Aut}(g_1, \ldots, g_k)\} \cong \mathrm{Aut}(g_1, \ldots, g_k).$$

Proof. All the right translations are bijections, and $r_x(x) = x$, for all $x \in X$. We check (1.4), i.e. $r_u \circ r_y \circ r_u^{-1} = r_{r_u(y)}$, for all $u, y \in X$:

- if $u \in Z$, then $r_u = \mathrm{Id}_X$, and both sides are equal to r_y;
- if $u = y_i$ and $y = y_j$, then $r_{y_i}(y_j) = y_j$ and, since g_i and g_j commute,
$$r_{y_i} \circ r_{y_j} \circ r_{y_i}^{-1} = \mathrm{Id}_Y \sqcup g_i\, g_j\, g_i^{-1} = \mathrm{Id}_Y \sqcup g_j = r_{y_j};$$
- if $u = y_i$ and $y \in Z$, then $r_{y_i}(y) = g_i(y) \in Z$, and both sides are equal to Id_X.

Thus $(X, \triangleleft)$ is a quandle.

Since $g_i \neq \mathrm{Id}_Z$, for all i, we have
$$Z = \{x \in X \,|\, r_x = \mathrm{Id}_X\}.$$
Let $\varphi \in \mathrm{Aut}(X)$. By (1.2), $r_{\varphi(x)} = \varphi \circ r_x \circ \varphi^{-1}$; hence $r_x = \mathrm{Id}_X$ if and only if $r_{\varphi(x)} = \mathrm{Id}_X$, and therefore $\varphi(Z) = Z$ and $\varphi(Y) = Y$. Thus any automorphism of X is of the form $\varphi = \alpha \sqcup \beta$, for some $\alpha \in \mathrm{Sym}(Y)$ and $\beta \in \mathrm{Sym}(Z)$. For such a bijection φ, the condition (1.2) is trivially satisfied for $y \in Z$, while for $y = y_i$, with $\alpha(y_i) = y_j$, it becomes

$$\mathrm{Id}_Y \sqcup \beta\, g_i\, \beta^{-1} = \mathrm{Id}_Y \sqcup g_j.$$

Hence $\alpha \sqcup \beta \in \mathrm{Aut}(X)$ if and only if $(\alpha, \beta) \in H_g$. Since $(\alpha, \beta) \mapsto \alpha \sqcup \beta$ is an injective morphism of groups $\mathrm{Sym}(Y) \times \mathrm{Sym}(Z) \to \mathrm{Sym}(X)$, this proves the first statement.

If $g_1, \ldots, g_k$ are pairwise non-conjugate, then $\beta\, g_i\, \beta^{-1} = g_j$ implies $i = j$. Hence $(\alpha, \beta) \in H_g$ if and only if $\alpha = \mathrm{Id}_Y$ and $\beta \in \mathrm{Aut}(g_1, \ldots, g_k)$, and the proof is finished. □

Corollary 3.2. *Let $n_1, \ldots, n_k \geq 2$. Then the abelian group $C_{n_1} \times \cdots \times C_{n_k}$ is isomorphic to the automorphism group of a quandle with $k + n_1 + \cdots + n_k$ elements. In particular, every finite abelian group is isomorphic to the automorphism group of a finite quandle.*

Proof. Let $Z := O_1 \sqcup \cdots \sqcup O_k$, with $|O_j| = n_j$, let $c_j \in \mathrm{Sym}(Z)$ be a cycle of length n_j with support O_j, and let
$$g_i := c_1\, c_2 \cdots c_i, \qquad \text{for all } i = 1, \ldots, k.$$
The cycles c_j have disjoint supports, so the permutations g_i commute pairwise. They are pairwise non-conjugate, since g_i moves exactly $n_1 + \cdots + n_i$ points. As $g_1, \ldots, g_k$ and $c_1, \ldots, c_k$ generate the same subgroup of $\mathrm{Sym}(Z)$, we have

$$\mathrm{Aut}(g_1, \ldots, g_k) = \mathrm{Aut}(c_1, \ldots, c_k).$$

Let $\beta \in \mathrm{Aut}(c_1, \dots, c_k)$. Since β commutes with c_j, it maps the support O_j of c_j onto itself, and its restriction to O_j commutes with the n_j-cycle $c_{j|O_j}$; hence $\beta_{|O_j}$ is a power of $c_{j|O_j}$. Conversely, every product of powers of the cycles c_j commutes with all of them. Therefore

$$\mathrm{Aut}(c_1, \dots, c_k) = \langle c_1 \rangle \times \cdots \times \langle c_k \rangle \cong C_{n_1} \times \cdots \times C_{n_k},$$

and the conclusion follows from Proposition 3.1. Finally, the trivial group is the automorphism group of the quandle with one element. □

Corollary 3.3. *The quaternion group Q_8 is the smallest group which is not isomorphic to the automorphism group of a rack, of a quandle, or of the derived solution of a rack.*

Proof. By Corollary 2.6, Q_8 is not the automorphism group of a rack. The groups of order at most 8, other than Q_8, are the abelian ones, the symmetric group S_3 and the dihedral group D_4. The abelian groups are covered by Corollary 3.2, and S_3 is the automorphism group of the trivial quandle with 3 elements. Finally, applying Proposition 3.1 for $k = 1$, $Z = \{1, 2, 3, 4\}$ and $g_1 = (1\ 2)(3\ 4)$, we obtain a quandle with 5 elements whose automorphism group is isomorphic to the centralizer of $(1\ 2)(3\ 4)$ in S_4, i.e. to D_4 [39, Example 2.7]. By (1.7), the same holds for the derived solutions of racks. □

3.2 Augmented quandles

Every rack X is determined by the action of $\mathrm{Inn}(X)$ on X and by the equivariant map $x \mapsto r_x$; this is the point of view of augmented racks and quandles [33, Section 9], [25], [9, Definition 7.66]. We use it in order to realize a given group G as the automorphism group of a quandle on which G acts by inner automorphisms.

Let G be a group, $H_1, \dots, H_s$ subgroups of G, and $c_i \in Z(H_i)$, for all $i = 1, \dots, s$. Let

$$X := \bigsqcup_{i=1}^{s} G/H_i$$

be the disjoint union of the sets of left cosets, with the natural action of G, and let $\partial\colon X \to G$ be the map given by

$$\partial(gH_i) := g\, c_i\, g^{-1}, \qquad \text{for all } g \in G,\ i = 1, \dots, s.$$

The map ∂ is well defined, since c_i commutes with all elements of H_i, and it is G-equivariant, i.e. $\partial(gx) = g\, \partial(x)\, g^{-1}$, for all $g \in G$ and $x \in X$. We define

$$x \triangleleft y := \partial(y)\, x, \qquad \text{for all } x, y \in X. \tag{3.1}$$

We say that two pairs (H, c) and (H', c'), consisting of a subgroup and an element of G, are *conjugate* in G if there exists $g \in G$ such that $H' = gHg^{-1}$ and $c' = g\, c\, g^{-1}$.

Proposition 3.4. *With the above notation, assume that $\bigcap_{i=1}^{s} \mathrm{core}_G(H_i) = 1$, i.e. G acts faithfully on X, and that G is generated by the conjugates of $c_1, \dots, c_s$. Then $(X, \triangleleft)$ is a quandle, $\mathrm{Inn}(X) = G$ as subgroups of $\mathrm{Sym}(X)$, and*

$$\mathrm{Aut}(X) = \{\varphi \in N_{\mathrm{Sym}(X)}(G) \mid \partial \circ \varphi = \theta_\varphi \circ \partial\}, \qquad \textit{where } \theta_\varphi(g) := \varphi\, g\, \varphi^{-1}. \tag{3.2}$$

Assume, moreover, that:

(a) if $\theta \in \mathrm{Aut}(G)$ and $\pi \in S_s$ are such that the pair $\big(\theta(H_i),\, \theta(c_i)\big)$ is conjugate in G to $\big(H_{\pi(i)},\, c_{\pi(i)}\big)$, for all $i = 1, \dots, s$, then θ is an inner automorphism of G;

(b) the only G-equivariant bijections $\psi\colon X \to X$ such that $\partial \circ \psi = \partial$ are the actions of the elements of $Z(G)$.

Then $\mathrm{Aut}(X) = G$.

Proof. The right translations are $r_y(x) = \partial(y)\, x$, i.e. r_y is the action of $\partial(y) \in G$ on X; in particular, they are bijections. For $x = gH_i$ we have

$$x \triangleleft x = \partial(x)\, x = g\, c_i\, g^{-1} g H_i = g\, c_i H_i = x,$$

since $c_i \in H_i$. Moreover, for all y, $z \in X$, the equivariance of ∂ gives

$$r_{r_z(y)} = \partial\big(\partial(z)\, y\big) = \partial(z)\, \partial(y)\, \partial(z)^{-1} = r_z \circ r_y \circ r_z^{-1},$$

i.e. (1.4) holds. Thus $(X, \triangleleft)$ is a quandle, and $\mathrm{Inn}(X)$ is the subgroup of $\mathrm{Sym}(X)$ generated by the elements $\partial(y)$, $y \in X$, i.e. by the conjugates of $c_1, \dots, c_s$; by assumption, this subgroup is G.

Let $\varphi \in \mathrm{Sym}(X)$. By (1.2), $\varphi \in \mathrm{Aut}(X)$ if and only if

$$\varphi\, \partial(y)\, \varphi^{-1} = \partial(\varphi(y)), \qquad \text{for all } y \in X.$$

If this holds, then the conjugation by φ maps the generating set $\partial(X)$ of G into G, hence $\varphi\, G\, \varphi^{-1} \subseteq G$; the same holds for the automorphism φ^{-1}, so $\varphi \in N_{\mathrm{Sym}(X)}(G)$, and the above condition reads $\theta_\varphi \circ \partial = \partial \circ \varphi$. The converse is clear, and (3.2) is proved.

Assume now that (a) and (b) hold, and let $\varphi \in \mathrm{Aut}(X)$ and $\theta := \theta_\varphi \in \mathrm{Aut}(G)$. Since $\varphi(gx) = \theta(g)\, \varphi(x)$, for all $g \in G$ and $x \in X$, the bijection φ maps G-orbits onto G-orbits. Let $\pi \in S_s$ be such that $\varphi(G/H_i) = G/H_{\pi(i)}$, and write $\varphi(H_i) = g_i H_{\pi(i)}$, with $g_i \in G$. The stabilizer of the point $\varphi(H_i)$ is, on the one hand, $\theta(H_i)$, and, on the other hand, $g_i H_{\pi(i)} g_i^{-1}$. Moreover, by (3.2),

$$\theta(c_i) = \theta\big(\partial(H_i)\big) = \partial\big(\varphi(H_i)\big) = \partial(g_i H_{\pi(i)}) = g_i\, c_{\pi(i)}\, g_i^{-1}.$$

Thus the pair $\big(\theta(H_i),\, \theta(c_i)\big)$ is conjugate to $\big(H_{\pi(i)},\, c_{\pi(i)}\big)$, for all i, and (a) gives $\theta = \kappa_g$, for some $g \in G$. Let $\psi := g^{-1}\varphi$, where g^{-1} acts on X. Then $\psi \in \mathrm{Aut}(X)$ and $\theta_\psi = \kappa_{g^{-1}} \circ \theta = \mathrm{Id}_G$, i.e. ψ is G-equivariant, and $\partial \circ \psi = \theta_\psi \circ \partial = \partial$. By (b), ψ is the action of an element of $Z(G)$, hence $\varphi = g\psi \in G$. Since $G = \mathrm{Inn}(X) \subseteq \mathrm{Aut}(X)$, we obtain $\mathrm{Aut}(X) = G$. □

The following lemma gives a convenient sufficient condition for (b).

Lemma 3.5. *With the notation of Proposition 3.4, let G be finite and assume that:*

(1) the pairs $(H_i,\, c_i)$, $i = 1, \dots, s$, are pairwise non-conjugate in G;

(2) $N_G(H_i) \cap C_G(c_i) \subseteq H_i\, Z(G)$, for all $i = 1, \dots, s$;

(3) there exists i_0 such that $Z(G) \subseteq H_i$, for all $i \neq i_0$.

Then condition (b) of Proposition 3.4 holds.

Proof. Let $\psi\colon X \to X$ be a G-equivariant bijection such that $\partial\circ\psi = \partial$. Fix i and write $\psi(H_i) = gH_j$. Since ψ is G-equivariant, for any $h \in H_i$ we have

$$gH_j = \psi(H_i) = \psi(hH_i) = h\,\psi(H_i) = hgH_j,$$

i.e. $H_i \subseteq gH_jg^{-1}$. Moreover, ψ maps the orbit G/H_i bijectively onto the orbit G/H_j; as G is finite, $|H_i| = |H_j|$, and therefore $H_i = gH_jg^{-1}$. Using $\partial \circ \psi = \partial$, we also obtain

$$c_i = \partial(H_i) = \partial(\psi(H_i)) = \partial(gH_j) = g\,c_j\,g^{-1}.$$

Thus the pairs $(H_i,\, c_i)$ and $(H_j,\, c_j)$ are conjugate, and (1) gives $j = i$. Then $g \in N_G(H_i) \cap C_G(c_i)$ and, by (2), $g = h\zeta_i$, with $h \in H_i$ and $\zeta_i \in Z(G)$. Hence, for all $x \in G$,

$$\psi(xH_i) = x\,\psi(H_i) = xgH_i = x\,\zeta_i\,hH_i = \zeta_i\,xH_i,$$

i.e. ψ is, on the orbit G/H_i, the action of the element $\zeta_i \in Z(G)$. By (3), every $\zeta \in Z(G)$ acts trivially on G/H_i, for all $i \neq i_0$, since $\zeta\,xH_i = x\,\zeta H_i = xH_i$. Hence ψ is the action of ζ_{i_0} on the whole of X. □

Remark 3.6. Condition (2) of Lemma 3.5 is also necessary for the equality $\mathrm{Aut}(X) = G$ in Proposition 3.4: if $\mathrm{Aut}(X) = G$, then the stabilizer of the point $H_i \in G/H_i$ is H_i and r_{H_i} is the action of $\partial(H_i) = c_i$, so Lemma 2.1(2) gives $N_G(H_i) \cap C_G(c_i) \subseteq H_i\,Z(G)$. For connected quandles, a description of $\mathrm{Aut}(X)$ in terms of the group generated by the right translations and of its automorphisms is given in [32, Proposition 5.8]; Proposition 3.4 also applies to quandles which are not connected, as in Proposition 3.9 below.

3.3 Dihedral groups, dicyclic groups and $SL(2,\,3)$

For $n \geq 3$, let R_n be the dihedral quandle, i.e. the set $\mathbb{Z}_n$ with the operation $j \triangleleft k := 2k - j$. By [22, Theorem 2.1], $\mathrm{Aut}(R_n)$ is isomorphic to the affine group $\mathrm{Aff}(\mathbb{Z}_n) = \mathbb{Z}_n \rtimes \mathbb{Z}_n^\times$, which is isomorphic to D_n if and only if $\mathbb{Z}_n^\times = \{\pm 1\}$, i.e. $n \in \{3,\, 4,\, 6\}$; for $n = 4$, see also [10, Corollary 5.6]. Adding two points to R_n, we obtain a quandle whose automorphism group is D_n, for all $n \geq 3$.

Proposition 3.7. *Let $n \geq 3$ and $X := \mathbb{Z}_n \sqcup P$, where $P := \{p_1,\, p_{-1}\}$. For all $j,\, k \in \mathbb{Z}_n$ and $\varepsilon,\, \delta \in \{1,\, -1\}$ we define*

$$j \triangleleft k := 2k - j, \qquad p_\varepsilon \triangleleft k := p_{-\varepsilon}, \qquad j \triangleleft p_\varepsilon := j + \varepsilon, \qquad p_\varepsilon \triangleleft p_\delta := p_\varepsilon.$$

Then $(X,\, \triangleleft)$ is a quandle with $n + 2$ elements and $\mathrm{Aut}(X) = \mathrm{Inn}(X) \cong D_n$.

Proof. Let $t,\, s_k \in \mathrm{Sym}(\mathbb{Z}_n)$ be given by $t(j) := j + 1$ and $s_k(j) := 2k - j$, for all $j,\, k \in \mathbb{Z}_n$, and let τ be the transposition of P. Then the right translations of $(X,\, \triangleleft)$ are

$$r_k = s_k \sqcup \tau \qquad \text{and} \qquad r_{p_\varepsilon} = t^\varepsilon \sqcup \mathrm{Id}_P, \qquad \text{for all } k \in \mathbb{Z}_n,\ \varepsilon \in \{1,\, -1\},$$

where, as in Proposition 3.1, $\alpha \sqcup \beta$ denotes the bijection of $X = \mathbb{Z}_n \sqcup P$ which is equal to α on $\mathbb{Z}_n$ and to β on P. They are all bijections, and $r_x(x) = x$, for all $x \in X$. A straightforward computation shows that, for all $k,\, l \in \mathbb{Z}_n$,

$$s_k\,s_l\,s_k^{-1} = s_{2k-l}, \qquad s_k\,t\,s_k^{-1} = t^{-1}, \qquad t\,s_k\,t^{-1} = s_{k+1}. \tag{3.3}$$

We check (1.4), i.e. $r_u \circ r_y \circ r_u^{-1} = r_{r_u(y)}$, for all $u,\, y \in X$. Let $k,\, l \in \mathbb{Z}_n$ and $\varepsilon,\, \delta \in \{1,\, -1\}$. Using (3.3), we obtain:

- $r_k \circ r_l \circ r_k^{-1} = s_{2k-l} \sqcup \tau = r_{2k-l} = r_{r_k(l)}$;
- $r_k \circ r_{p_\varepsilon} \circ r_k^{-1} = t^{-\varepsilon} \sqcup \mathrm{Id}_P = r_{p_{-\varepsilon}} = r_{r_k(p_\varepsilon)}$;
- $r_{p_\varepsilon} \circ r_k \circ r_{p_\varepsilon}^{-1} = s_{k+\varepsilon} \sqcup \tau = r_{k+\varepsilon} = r_{r_{p_\varepsilon}(k)}$;
- $r_{p_\varepsilon} \circ r_{p_\delta} \circ r_{p_\varepsilon}^{-1} = t^{\delta} \sqcup \mathrm{Id}_P = r_{p_\delta} = r_{r_{p_\varepsilon}(p_\delta)}$.

Thus $(X, \triangleleft)$ is a quandle with $n+2$ elements.

For $c \in \mathbb{Z}_n$ and $\varepsilon \in \{1, -1\}$, let $\varphi_{c,\varepsilon} \in \mathrm{Sym}(X)$ be given by

$$\varphi_{c,\varepsilon}(j) := c + \varepsilon j, \qquad \varphi_{c,\varepsilon}(p_\delta) := p_{\varepsilon\delta}, \qquad \text{for all } j \in \mathbb{Z}_n,\ \delta \in \{1, -1\}.$$

Then $\varphi_{c,1} = r_{p_1}^c$ and $\varphi_{c,-1} = r_{p_1}^c \circ r_0$; hence $\varphi_{c,\varepsilon} \in \mathrm{Inn}(X) \subseteq \mathrm{Aut}(X)$, for all c and ε. Since

$$\varphi_{c,\varepsilon} \circ \varphi_{c',\varepsilon'} = \varphi_{c+\varepsilon c',\, \varepsilon\varepsilon'},$$

the $2n$ bijections $\varphi_{c,\varepsilon}$ form a subgroup of $\mathrm{Sym}(X)$, which is isomorphic to D_n: by restriction to $\mathbb{Z}_n$, it is identified with the group of the maps $j \mapsto c \pm j$, i.e. with the group of symmetries of a regular n-gon whose vertices are labelled by $\mathbb{Z}_n$.

Conversely, let $\varphi \in \mathrm{Aut}(X)$. By (1.2), $r_{\varphi(x)} = \varphi \circ r_x \circ \varphi^{-1}$, so r_x and $r_{\varphi(x)}$ have the same order, for all $x \in X$. Since r_k has order 2, for all $k \in \mathbb{Z}_n$, while r_{p_1} and $r_{p_{-1}}$ have order $n \geq 3$, we obtain $\varphi(P) = P$ and $\varphi(\mathbb{Z}_n) = \mathbb{Z}_n$. Let β be the restriction of φ to $\mathbb{Z}_n$, and let $\varepsilon \in \{1, -1\}$ be such that $\varphi(p_1) = p_\varepsilon$; then $\varphi(p_{-1}) = p_{-\varepsilon}$. Restricting to $\mathbb{Z}_n$ the condition (1.2), written for $y = p_1$, we obtain $\beta \circ t \circ \beta^{-1} = t^\varepsilon$, i.e.

$$\beta(j+1) = \beta(j) + \varepsilon, \qquad \text{for all } j \in \mathbb{Z}_n.$$

By induction, $\beta(j) = c + \varepsilon j$, where $c := \beta(0)$; hence $\varphi = \varphi_{c,\varepsilon}$. Therefore

$$\mathrm{Aut}(X) = \{\varphi_{c,\varepsilon} \,|\, c \in \mathbb{Z}_n,\, \varepsilon \in \{1, -1\}\} = \mathrm{Inn}(X) \cong D_n,$$

and the proof is finished. □

Remark 3.8. The quandle of Proposition 3.7 is the quandle given by (3.1) for the group $G = D_n = \langle \rho, \sigma \,|\, \rho^n = \sigma^2 = 1, \sigma\rho\sigma = \rho^{-1} \rangle$, $s = 2$, $H_1 = \langle \sigma \rangle$, $c_1 = \sigma$, $H_2 = \langle \rho \rangle$ and $c_2 = \rho$: the coset $\rho^j H_1$ corresponds to $j \in \mathbb{Z}_n$, and the cosets H_2 and σH_2 correspond to p_1 and p_{-1}. Moreover, the quandles of Proposition 3.1 and Proposition 3.7 are particular cases of the quandle structures on the disjoint union of two quandles constructed in [10, Proposition 9.2]; their automorphism groups are not considered there.

Like Q_8, the dicyclic groups have a unique involution. By Corollary 2.5, Dic_n is not the automorphism group of a rack if n is even. We show now that the situation is completely different if n is odd; for instance, for $n = 3$ we obtain a quandle with 7 elements whose automorphism group is the dicyclic group Dic_3 of order 12.

Proposition 3.9. *Let $n \geq 3$ be an odd integer and $G := \mathrm{Dic}_n$. Consider the quandle $(X, \triangleleft)$ given by (3.1) for $s = 2$ and*

$$H_1 := \langle a^2 \rangle, \quad c_1 := a^2, \qquad H_2 := \langle b \rangle, \quad c_2 := b.$$

Then X has $n+4$ elements and $\mathrm{Aut}(X, \triangleleft) = G \cong \mathrm{Dic}_n$. In particular, for $n \geq 2$, the dicyclic group Dic_n is isomorphic to the automorphism group of a rack if and only if n is odd.

Proof. Let $z := a^n$. Since n is odd, a^2 has order n; thus $|H_1| = n$, while $|H_2| = 4$, by Lemma 1.3(1), and X has $4n/n + 4n/4 = n + 4$ elements. We first check the assumptions of Proposition 3.4. As $|H_1|$ and $|H_2|$ are coprime, we have

$$\mathrm{core}_G(H_1) \cap \mathrm{core}_G(H_2) \subseteq H_1 \cap H_2 = 1.$$

The subgroup generated by a^2 and b contains $b^2 = a^n$; as n is odd, it also contains $a = (a^2)^{(n+1)/2}\, a^{-n}$, hence it is equal to G. Next, we check the conditions of Lemma 3.5:

- (1) holds, since $|H_1| = n \neq 4 = |H_2|$;
- (2) holds: as $n \geq 3$, we have $a^2 \notin \langle z \rangle$, hence $C_G(a^2) = \langle a \rangle$, by Lemma 1.3(3), and $\langle a \rangle = \langle a^2 \rangle \langle a^n \rangle = H_1\, Z(G)$, since n is odd; moreover, $C_G(b) = \langle b \rangle = H_2$, by Lemma 1.3(4);
- (3) holds for $i_0 = 1$, since $Z(G) = \langle z \rangle \subseteq \langle b \rangle = H_2$.

Finally, we check (a) of Proposition 3.4. Let $\theta \in \mathrm{Aut}(G)$ and $\pi \in S_2$ be as in (a). Since $|H_1| \neq |H_2|$, π is the identity, so $\theta(a^2)$ is conjugate to a^2 and $\theta(b)$ is conjugate to b. As $2n > 4$, the elements of order $2n$ of G belong to $\langle a \rangle$, by Lemma 1.3(1); hence $\theta(a) = a^u$, for some integer u coprime with $2n$, and $\theta(b) \notin \langle a \rangle$, i.e. $\theta(b) = a^v b$, for some $v \in \mathbb{Z}$. By Lemma 1.3(4), $v = 2j$ is even. By Lemma 1.3(1), the conjugacy class of a^2 is $\{a^2,\, a^{-2}\}$, hence $a^{2u} = a^{\pm 2}$, i.e. $u \equiv \pm 1 \pmod{n}$; since u and n are odd, this gives $u \equiv \pm 1 \pmod{2n}$. As $\kappa_b(a) = a^{-1}$ and $\kappa_b(a^{2j} b) = a^{-2j} b$, replacing θ by $\kappa_b \circ \theta$ if necessary, we may assume that $\theta(a) = a$. Then θ and κ_{a^j} coincide on a and on b, since $a^j\, b\, a^{-j} = a^{2j} b$; hence $\theta = \kappa_{a^j}$ is an inner automorphism. By Lemma 3.5 and Proposition 3.4, $\mathrm{Aut}(X) = G \cong \mathrm{Dic}_n$. The last statement follows from Corollary 2.5. □

The group $SL(2,\, 3)$ also has a unique involution, and its Sylow 2-subgroup is the quaternion group Q_8. Nevertheless, it is the automorphism group of a quandle with 8 elements, namely of a subquandle of the symplectic quandle on $\mathbb{F}_3^2$ [9, Example 6.12], [42].

Proposition 3.10. *Let $\mathbb{F}_3$ be the field with three elements, $X := \mathbb{F}_3^2 \setminus \{0\}$, and let $\omega(x,\, y) := x_1 y_2 - x_2 y_1$, for all $x = (x_1,\, x_2)^t$, $y = (y_1,\, y_2)^t \in \mathbb{F}_3^2$. Then X is a quandle with 8 elements with respect to the operation*

$$x \triangleleft y := x + \omega(x,\, y)\, y, \qquad \text{for all } x,\, y \in X,$$

and $\mathrm{Aut}(X, \triangleleft) \cong SL(2,\, 3)$.

Proof. Let $G := SL(2,\, 3)$, acting on X by matrix multiplication; this action is faithful and transitive, and the stabilizer of $e_1 := (1,\, 0)^t$ is the abelian group

$$U := \left\{ \left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right) \mid \lambda \in \mathbb{F}_3 \right\}.$$

For $y \in X$, the map $t_y \colon \mathbb{F}_3^2 \to \mathbb{F}_3^2$, $t_y(x) := x + \omega(x,\, y)\, y$, is a transvection; thus $t_y \in G$, and $x \triangleleft y = t_y(x) \in X$, for all $x \in X$. Since $\omega(gx,\, gy) = \det(g)\, \omega(x,\, y) = \omega(x,\, y)$, for all $g \in G$, we have

$$g\, t_y\, g^{-1} = t_{gy}, \qquad \text{for all } g \in G,\ y \in X.$$

Hence, identifying X with G/U via $ge_1 \mapsto gU$, the operation $\triangleleft$ is given by (3.1) for $s = 1$, $H_1 := U$ and

$$c_1 := u := t_{e_1} = \left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right) \in U.$$

Moreover, G is generated by the conjugates of u: the group $SL(2,\, 3)$ is generated by the elementary matrices, which are powers of $u = t_{e_1}$ and of its conjugate $t_{e_2} = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$, where $e_2 := (0,\, 1)^t$. By

Proposition 3.4, $(X, \triangleleft)$ is a quandle. We check now the conditions of Lemma 3.5: (1) and (3) are trivially fulfilled for $s = 1$, and (2) holds since the matrices which commute with u are the upper triangular matrices with equal diagonal entries, so that

$$C_G(u) = \{\pm I_2\}\, U = U\, Z(G).$$

It remains to check (a) of Proposition 3.4. We first show that every automorphism of G is the conjugation by an element of $GL(2, 3)$. The normal Sylow 2-subgroup of G is the quaternion group Q_8, generated by the matrices $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$, and a direct computation shows that the only matrices which commute with both of them are the scalar matrices. Consequently, $C_G(Q_8) = \{\pm I_2\} = Z(G)$, and the conjugation by the elements of $GL(2, 3)$ gives an injective morphism of groups $PGL(2, 3) \to \mathrm{Aut}(G)$, whose image has 24 elements. On the other hand, the restriction map $\mathrm{Aut}(G) \to \mathrm{Aut}(Q_8) \cong S_4$ is injective. Indeed, if $\theta \in \mathrm{Aut}(G)$ is the identity on Q_8, then, for all $g \in G$ and $q \in Q_8$,

$$\theta(g)\, q\, \theta(g)^{-1} = \theta(g\, q\, g^{-1}) = g\, q\, g^{-1},$$

so $g^{-1}\theta(g) \in C_G(Q_8) = Z(G)$. Thus $\theta(g) = g\,\mu(g)$, where $\mu\colon G \to Z(G) \cong C_2$ is a morphism of groups; since $G/[G, G] \cong C_3$, μ is trivial, and $\theta = \mathrm{Id}_G$. Hence $|\mathrm{Aut}(G)| \leq 24$, and every automorphism of G is the conjugation by some $g \in GL(2, 3)$.

Let now $\theta = \kappa_g$, with $g \in GL(2, 3)$, be as in (a); in particular, $\theta(u)$ is conjugate to u in G. Assume that $\det(g) = -1$ and write $g = g_0 d$, with $g_0 \in G$ and $d := \mathrm{diag}(1, -1)$. Since $d\, u\, d^{-1} = u^{-1}$, we obtain

$$\theta(u) = g_0\, (d\, u\, d^{-1})\, g_0^{-1} = g_0\, u^{-1}\, g_0^{-1},$$

so u^{-1} is conjugate to u in G. This is not possible: if $h\, u\, h^{-1} = u^{-1} = d\, u\, d^{-1}$, with $h \in G$, then $d^{-1}h$ commutes with u, hence it is an upper triangular matrix with equal diagonal entries and its determinant is 1, while $\det(d^{-1}h) = -1$. Thus $\det(g) = 1$, i.e. θ is an inner automorphism of G. By Lemma 3.5 and Proposition 3.4, $\mathrm{Aut}(X) = G = SL(2, 3)$. □

3.4 Conjugation quandles and alternating groups

Let G be a group and $C \subseteq G$ a union of conjugacy classes of G. Then C is a quandle with respect to the operation $x \triangleleft y := yxy^{-1}$; it is a subquandle of the conjugation quandle of G [9, Example 6.17]. The following result is a variant, for subquandles, of the description of the automorphism group of the conjugation quandle of a group with trivial center [10, Corollary 4.4].

Proposition 3.11. *Let G be a group with $Z(G) = 1$ and $C \subseteq G$ a union of conjugacy classes which generates G. Then the map*

$$\{\theta \in \mathrm{Aut}(G) \,|\, \theta(C) = C\} \to \mathrm{Aut}(C, \triangleleft), \qquad \theta \mapsto \theta_{|C},$$

is an isomorphism of groups. In particular, $\mathrm{Aut}(C, \triangleleft) \cong G$ if and only if every automorphism of G which preserves C is inner.

Proof. If $\theta \in \mathrm{Aut}(G)$ and $\theta(C) = C$, then $\theta_{|C}$ is an automorphism of $(C, \triangleleft)$, and $\theta \mapsto \theta_{|C}$ is an injective morphism of groups, since C generates G. It remains to prove that it is surjective. Consider the morphism of groups

$$G \to \mathrm{Inn}(C), \qquad g \mapsto \kappa_{g|C}.$$

It is surjective, since $r_y = \kappa_{y|C}$, for all $y \in C$, and C generates G; it is injective, since its kernel is $C_G(C) = Z(G) = 1$. Let $\varphi \in \mathrm{Aut}(C, \triangleleft)$. By (1.2), the conjugation by φ maps $\mathrm{Inn}(C)$ onto itself; via the above isomorphism, it induces an automorphism θ of G such that

$$\kappa_{\theta(g)|C} = \varphi \circ \kappa_{g|C} \circ \varphi^{-1}, \qquad \text{for all } g \in G.$$

For $c \in C$, using (1.2) once more, we obtain

$$\kappa_{\theta(c)|C} = \varphi \circ r_c \circ \varphi^{-1} = r_{\varphi(c)} = \kappa_{\varphi(c)|C},$$

hence $\theta(c) = \varphi(c)$. Thus $\theta(C) = C$ and $\varphi = \theta_{|C}$. The last statement follows, since the inner automorphisms of G preserve C and form a subgroup of $\mathrm{Aut}(G)$ isomorphic to $G/Z(G) = G$. □

We apply Proposition 3.11 to the alternating groups. Recall that $Z(A_n) = 1$, for all $n \geq 4$, and that every automorphism of A_n is the conjugation by an element of S_n, for all $n \geq 4$, $n \neq 6$ [21, Section 8.2].

Proposition 3.12. *Let $n \geq 4$ and let $C \subseteq A_n$ be:*

(i) the conjugacy class in A_n of the n-cycle $(1\ 2 \cdots n)$, if n is odd;

(ii) the conjugacy class in A_n of the $(n-1)$-cycle $(1\ 2 \cdots n-1)$, if n is even and $n \neq 6$;

(iii) the union of the conjugacy classes in A_6 of $(1\ 2\ 3)$ and $(1\ 2\ 3\ 4\ 5)$, if $n = 6$.

Then $\mathrm{Aut}(C, \triangleleft) \cong A_n$. The quandle C has $(n-1)!/2$ elements in case (i), $n\,(n-2)!/2$ elements in case (ii), and 112 elements in case (iii).

Proof. We start with a well known fact. Let $g \in A_n$ be an n-cycle, if n is odd, or an $(n-1)$-cycle, if n is even. The conjugacy class of g in S_n has $(n-1)!$, respectively $n\,(n-2)!$ elements, hence $C_{S_n}(g) = \langle g \rangle \leq A_n$. If $\sigma \in S_n$ is an odd permutation, then $\sigma g \sigma^{-1}$ is not conjugate to g in A_n: otherwise, $\sigma g \sigma^{-1} = hgh^{-1}$, for some $h \in A_n$, and $h^{-1}\sigma \in C_{S_n}(g) \leq A_n$, a contradiction. Thus the conjugacy class of g in S_n is the union of two conjugacy classes of A_n with the same number of elements, which are interchanged by the conjugation with any odd permutation.

This proves the statement on the number of elements of C in the cases (i) and (ii). In the case (iii), the conjugacy class of $(1\ 2\ 3)$ in A_6 is the set T of all the 40 cycles of length 3, since $(1\ 2\ 3)$ commutes with the odd permutation $(4\ 5)$, and the conjugacy class C' of $(1\ 2\ 3\ 4\ 5)$ in A_6 has $144/2 = 72$ elements; hence $|C| = 112$.

The subgroup of A_n generated by C is normal and non-trivial, so it is equal to A_n: this is clear for $n \geq 5$, when A_n is simple, while for $n = 4$ the normal subgroups of A_4 are 1, the Klein group and A_4, and C consists of elements of order 3. By Proposition 3.11, it is enough to prove that every automorphism θ of A_n such that $\theta(C) = C$ is inner.

If $n \neq 6$, then θ is the conjugation by some $\sigma \in S_n$, and σ is even, since the conjugation by an odd permutation maps C onto a different conjugacy class of A_n. Hence θ is inner.

Let now $n = 6$, so that $C = T \sqcup C'$. Since θ preserves the orders of the elements, we have $\theta(T) = T$ and $\theta(C') = C'$. We show that θ is the conjugation by a permutation. For $i \in \{1, \ldots, 6\}$, let $M_i \cong A_5$ be the stabilizer of i in A_6, and let $L := \theta(M_i)$. Then $L \cong A_5$ and L contains cycles of length 3, since M_i does and $\theta(T) = T$. The orbits of L on $\{1, \ldots, 6\}$ have 1, 5 or 6 elements, since A_5 has no subgroups of index 2, 3 or 4. If L were transitive, then a cycle of length 3 of L, which fixes three points, would belong to the stabilizer in L of one of these points; but this stabilizer has order

$60/6 = 10$, a contradiction. Hence L fixes a point j, and $L = M_j$, as $|L| = |M_j|$. Since θ is bijective, we obtain a permutation $\pi \in S_6$ such that $\theta(M_i) = M_{\pi(i)}$, for all i. Let $\theta' := \kappa_\pi^{-1} \circ \theta$, where κ_π denotes the conjugation by π, restricted to A_6; then $\theta'(M_i) = M_i$, for all i. Since $gM_ig^{-1} = M_{g(i)}$, for all $g \in A_6$, we obtain

$$M_{\theta'(g)(i)} = \theta'(g)\, M_i\, \theta'(g)^{-1} = \theta'(g\, M_i\, g^{-1}) = \theta'(M_{g(i)}) = M_{g(i)},$$

hence $\theta'(g)(i) = g(i)$, for all i, i.e. $\theta'(g) = g$. Thus $\theta = \kappa_\pi$ and, as above, π is even, since $\theta(C') = C'$. Hence θ is inner, and the proof is finished. □

Corollary 3.13. *Every alternating group A_n and every symmetric group S_n is isomorphic to the automorphism group of a finite quandle.*

Proof. The symmetric group S_n is the automorphism group of the trivial quandle with n elements. The groups A_1 and A_2 are trivial, $A_3 \cong C_3$ is covered by Corollary 3.2, and for $n \geq 4$ we apply Proposition 3.12. □

Remark 3.14. For $n = 6$, the conjugacy class C' of (1 2 3 4 5) in A_6 is not enough: a computer check shows that $\mathrm{Aut}(C', \triangleleft)$ has order 720, so, by Proposition 3.11, C' is preserved by an automorphism of A_6 which is not inner. More generally, by Proposition 3.11, if G is a finite non-abelian simple group and C is a union of non-trivial conjugacy classes of G which is not preserved by any outer automorphism of G, then $\mathrm{Aut}(C, \triangleleft) \cong G$.

4 Concluding remarks and open questions

We have shown that, unlike the category of all set-theoretic solutions of the Yang–Baxter equation [39], the categories of racks and of quandles are neither universal nor finitely universal and that, as for groups, the reason is the presence of the inner automorphisms, which leads to the local condition (2.1). This raises the following natural problem: *which finite groups are represented by finite racks, respectively by finite quandles?* By Theorem 2.2, if a group G is the automorphism group of a rack, then for every $1 \neq z \in Z(G)$ there exist a subgroup $K \leq G$ with $z \notin K$ and an element $c \in C_G(K)$ such that

$$N_G(K) \cap C_G(c) \subseteq K\, Z(G).$$

We do not know whether this necessary condition is also sufficient for finite groups. For instance, a computer check shows that the groups $\mathrm{Dic}_3 \times C_2$ and $Q_8 \times C_4$ satisfy it, but we do not know whether they are automorphism groups of racks. The condition is empty for groups with trivial center: *is every finite group with trivial center the automorphism group of a finite rack, or of a finite quandle?* It is also natural to ask whether there exists a group which is the automorphism group of a rack, but not of a quandle; all the groups realized in Section 3 are automorphism groups of quandles.

For the quandles of Corollary 3.2 and of Propositions 3.7, 3.9, 3.10 and 3.12 we have $\mathrm{Inn}(X) = \mathrm{Aut}(X)$. This is no accident for simple groups: since $\mathrm{Inn}(X)$ is a normal subgroup of $\mathrm{Aut}(X)$, a finite non-abelian simple group G can only be represented by a rack X such that $G = \mathrm{Aut}(X) = \mathrm{Inn}(X)$. Indeed, if $\mathrm{Inn}(X) = 1$, then X is a trivial rack and $\mathrm{Aut}(X) = \mathrm{Sym}(X)$, which is not a non-abelian simple group. By Proposition 3.11, such a rack exists as soon as G has a union of non-trivial conjugacy classes which is not preserved by any outer automorphism of G, as for the alternating groups in Proposition 3.12. *Is every finite non-abelian simple group the automorphism group of a finite quandle?* Following Babai [5], one can also ask quantitative questions: given a finite group G which is represented by a finite rack, what is the smallest size of such a rack? Since $\mathrm{Aut}(X)$ is a

subgroup of $\mathrm{Sym}(X)$, this size is at least the minimal degree of a faithful permutation representation of G; for instance, the quandles of Proposition 3.7 and Proposition 3.9 have $n+2$, respectively $n+4$ elements.

Finally, as explained in Remark 2.7, Theorem 2.2 does not apply to arbitrary bijective non-degenerate solutions of the braid equation, which leaves open the question raised in [39, Section 3]. The first test case is the following: *is the quaternion group Q_8 isomorphic to the automorphism group of a bijective non-degenerate solution of the braid equation?* More generally, *is the category of bijective non-degenerate solutions of the braid equation universal, or finitely universal?* By Theorem 2.2 and Remark 2.7, a positive answer would require solutions which are neither derived solutions of racks nor involutive solutions with $\sigma_{\sigma_x(y)} = \sigma_y$, for all x, $y \in X$.

Acknowledgements

Claude Opus 5.5 (Anthropic) was used throughout the preparation of this paper: to find references, to carry out the computer verifications, to explore and develop constructions and proofs, and for drafting and proofreading. All statements, proofs and computational results were checked by the author, who takes full responsibility for them.

References

[1] A.L. Agore, A. Chirvasitu and G. Militaru, *A categorical approach to the set-theoretic Yang–Baxter equation*, arXiv:2610.15347. 6

[2] A.L. Agore, A. Chirvasitu and G. Militaru, *The set-theoretic Yang–Baxter equation, Kimura semigroups and functional graphs*, Res. Math. Sci. **12** (2025), Paper No. 34. 2, 4

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

[4] L. Babai, *On the abstract group of automorphisms*, in: Combinatorics (Swansea, 1981), London Math. Soc. Lecture Note Ser. 52, Cambridge University Press, Cambridge, 1981, pp. 1–40. 1, 2

[5] L. Babai, *Automorphism groups, isomorphism, reconstruction*, in: Handbook of Combinatorics, Vol. 2, Elsevier, Amsterdam, 1995, pp. 1447–1540. 2, 19

[6] R. Baer, *Situation der Untergruppen und Struktur der Gruppe*, S.-B. Heidelberg. Akad. Wiss. **2** (1933), 12–17. 9

[7] C. Bai, L. Guo, Y. Sheng and R. Tang, *Post-groups, (Lie-)Butcher groups and the Yang–Baxter equation*, Math. Ann. **388** (2024), 3127–3167. 6

[8] V.G. Bardakov, P. Dey and M. Singh, *Automorphism groups of quandles arising from groups*, Monatsh. Math. **184** (2017), 519–530. 3

[9] V.G. Bardakov, M. Elhamdadi and M. Singh, *Algebra of the Yang–Baxter equation. Skew braces, quandles, and cohomology*, Springer Monographs in Mathematics, Springer, to appear. 2, 3, 5, 12, 16, 17

[10] V.G. Bardakov, T.R. Nasybullov and M. Singh, *Automorphism groups of quandles and related groups*, Monatsh. Math. **189** (2019), 1–21. 3, 14, 15, 17

[11] V.G. Bardakov and B. Sangare, *Constructions and automorphisms of quandles*, arXiv:2610.18676. 3

[12] V.G. Bardakov and M. Singh, *Quandle cohomology, extensions and automorphisms*, J. Algebra **585** (2021), 558–591. 3

[13] G.M. Bergman and A.O. Hausknecht, *Co-groups and co-rings in categories of associative rings*, Mathematical Surveys and Monographs, American Mathematical Society, Providence, RI, 1996. 6

[14] A. Bishop, C. Cyr, J. Hutchens, C. May, N. Schwartz and B. Turner, *On involutions and generalized symmetric spaces of dicyclic groups*, arXiv:1310.0121. 7

[15] N. Bourbaki, *Algebra I. Chapters 1–3*, Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998. 4

[16] E. Brieskorn, *Automorphic sets and braids and singularities*, in: Braids (Santa Cruz, CA, 1986), Contemp. Math. **78**, Amer. Math. Soc., Providence, RI, 1988, pp. 45–115. 2, 5

[17] N. Cazet, *Quandles with one non-trivial column*, arXiv:2303.15815. 3, 10

[18] K. Conrad, *Generalized quaternions*, expository note, `https://kconrad.math.uconn.edu/blurbs/grouptheory/genquat.pdf`. 6

[19] J. de Groot, *Groups represented by homeomorphism groups I*, Math. Ann. **138** (1959), 80–102. 2

[20] R. Dedekind, *Ueber Gruppen, deren sämmtliche Theiler Normaltheiler sind*, Math. Ann. **48** (1897), 548–561. 9

[21] J.D. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics 163, Springer-Verlag, New York, 1996. 18

[22] M. Elhamdadi, J. Macquarrie and R. Restrepo, *Automorphism groups of quandles*, J. Algebra Appl. **11** (2012), 1250008, 9 pp. 3, 4, 14

[23] M. Elhamdadi and S. Nelson, *Quandles. An introduction to the algebra of knots*, Student Mathematical Library 74, American Mathematical Society, Providence, RI, 2015. 2, 5

[24] P. Etingof, T. Schedler and A. Soloviev, *Set-theoretical solutions to the quantum Yang–Baxter equation*, Duke Math. J. **100** (1999), 169–209. 5, 10

[25] R. Fenn and C. Rourke, *Racks and links in codimension two*, J. Knot Theory Ramifications **1** (1992), 343–406. 2, 6, 12

[26] A. Ferman, T. Nowik and M. Teicher, *On the structure and automorphism group of finite Alexander quandles*, J. Knot Theory Ramifications **20** (2011), 463–468. 3

[27] T. Fritz, *Self-distributive structures in physics*, arXiv:2403.14458. 2

[28] R. Frucht, *Herstellung von Graphen mit vorgegebener abstrakter Gruppe*, Compositio Math. **6** (1939), 239–250. 2

[29] L. Guarnieri and L. Vendramin, *Skew braces and the Yang–Baxter equation*, Math. Comp. **86** (2017), 2519–2534. 6

[30] B. Ho and S. Nelson, *Matrices and finite quandles*, Homology Homotopy Appl. **7** (2005), 197–208. 3

[31] X.D. Hou, *Automorphism groups of Alexander quandles*, J. Algebra **344** (2011), 373–385. 3

[32] A. Hulpke, D. Stanovský and P. Vojtěchovský, *Connected quandles and transitive groups*, J. Pure Appl. Algebra **220** (2016), 735–758. 14

[33] D. Joyce, *A classifying invariant of knots, the knot quandle*, J. Pure Appl. Algebra **23** (1982), 37–65. 2, 3, 12

[34] D. Kőnig, *Theorie der endlichen und unendlichen Graphen*, Akademische Verlagsgesellschaft, Leipzig, 1936. 1

[35] V. Lebed and L. Vendramin, *On structure groups of set-theoretic solutions to the Yang–Baxter equation*, Proc. Edinb. Math. Soc. **62** (2019), 683–717. 10

[36] J.-H. Lu, M. Yan and Y.-C. Zhu, *On the set-theoretical Yang–Baxter equation*, Duke Math. J. **104** (2000), 1–18. 6

[37] J. Macquarrie, *Automorphism groups of quandles*, Master's thesis, University of South Florida, 2011. 3

[38] S.V. Matveev, *Distributive groupoids in knot theory*, Mat. Sb. (N.S.) **119(161)** (1982), 78–88 (in Russian); English transl. in Math. USSR-Sb. **47** (1984), 73–83. 2

[39] G. Militaru, *Every group is the automorphism group of a set-theoretic solution of the Yang–Baxter equation*, arXiv:2610.39228. 2, 3, 4, 5, 10, 12, 19, 20

[40] G. Militaru, *Bipartite solutions of the set-theoretic Yang–Baxter equation*, arXiv:2610.30845. 6

[41] G. Militaru, *Centralizers of maps as automorphism groups of Yang–Baxter solutions*, arXiv:2611.03380. 2, 4, 10

[42] E.A. Navas and S. Nelson, *On symplectic quandles*, Osaka J. Math. **45** (2008), 973–985. 16

[43] A. Pultr and V. Trnková, *Combinatorial, algebraic and topological representations of groups, semigroups and categories*, North-Holland Mathematical Library 22, North-Holland, Amsterdam–New York, 1980. 2

[44] S. Roman, *Fundamentals of group theory. An advanced approach*, Birkhäuser/Springer, New York, 2012. 6

[45] G. Sabidussi, *Graphs with given infinite group*, Monatsh. Math. **64** (1960), 64–67. 2

[46] Q.J.M. Salix and P.P. Wood, *More automorphism groups of quandles*, arXiv:2510.26673. 3

[47] B. Sangare, *Automorphisms and antiautomorphisms of quandles*, arXiv:2602.03080. 3

[48] A. Smoktunowicz and L. Vendramin, *On skew braces (with an appendix by N. Byott and L. Vendramin)*, J. Comb. Algebra **2** (2018), 47–86. 6

[49] A. Soloviev, *Non-unitary set-theoretical solutions to the quantum Yang–Baxter equation*, Math. Res. Lett. **7** (2000), 577–596. 10

[50] P. Vojtěchovský and S.Y. Yang, *Enumeration of racks and quandles up to isomorphism*, Math. Comp. **88** (2019), 2523–2540. 6

University of Bucharest, Faculty of Mathematics and Computer Science

Str. Academiei 14, RO-010014 Bucharest 1, Romania

E-mail address: gigel.militaru@gmail.com