ACADEMIC PRESS

Available online at www.sciencedirect.com

SCIENCE DIRECT

ADVANCES IN Mathematics

Advances in Mathematics 178 (2003) 177–243

http://www.elsevier.com/locate/aim

From racks to pointed Hopf algebras[☆]

Nicolás Andruskiewitsch[a,*] and Matías Graña[b,c]

[a] *Facultad de Matemática, Astronomía y Física, Universidad Nacional de Córdoba, CIEM-CONICET, Ciudad Universitaria, 5000 Córdoba, Argentina*
[b] *MIT, Mathematics Department, 77 Mass. Ave., 02139 Cambridge, MA, USA*
[c] *FCEyN-UBA, Pab. I-Ciudad Universitaria, 1428 Buenos Aires, Argentina*

Received 9 February 2002; accepted 22 May 2002

Communicated by Pavel Etingof

Abstract

A fundamental step in the classification of finite-dimensional complex pointed Hopf algebras is the determination of all finite-dimensional Nichols algebras of braided vector spaces arising from groups. The most important class of braided vector spaces arising from groups is the class of braided vector spaces $(\mathbb{C}X, c^q)$, where X is a rack and q is a 2-cocycle on X with values in $\mathbb{C}^\times$. Racks and cohomology of racks appeared also in the work of topologists. This leads us to the study of the structure of racks, their cohomology groups and the corresponding Nichols algebras. We will show advances in these three directions. We classify simple racks in group-theoretical terms; we describe projections of racks in terms of general cocycles; we introduce a general cohomology theory of racks containing properly the existing ones. We introduce a "Fourier transform" on racks of certain type; finally, we compute some new examples of finite-dimensional Nichols algebras.

MSC: Primary 16W30; Secondary 17B37; 52M27

Keywords: Pointed Hopf algebras; Racks; Quandles

☆This work was partially supported by ANPCyT, CONICET, Agencia Córdoba Ciencia, Fundación Antorchas, Secyt (UBA) and Secyt (UNC).
*Corresponding author.
E-mail address: andrus@mate.uncor.edu (N. Andruskiewitsch).

0001-8708/03/$ - see front matter © 2003 Elsevier Inc. All rights reserved.
doi:10.1016/S0001-8708(02)00071-3

0. Introduction

1. This paper is about braided vector spaces arising from pointed Hopf algebras, and their Nichols algebras. Our general reference for pointed Hopf algebras is [AS2]. wE SHALL work over the field $\mathbb{C}$ of complex numbers; many results below are valid over more general fields. We denote by $\mathbb{G}_\infty$ the group of roots of unity of $\mathbb{C}$.
2. The determination of all complex finite-dimensional pointed Hopf algebras H with group of group-likes $G(H)$ isomorphic to a fixed finite group Γ is still widely open. Even the existence of such Hopf algebras H (apart from the group algebra $\mathbb{C}\Gamma$) is unknown for many finite groups Γ. If Γ is abelian, substantial advances were done via the theory of quantum groups at roots of unit [AS1]. The results can be adapted to a non-necessarily abelian group Γ: if $(a_{ij})_{1 \leqslant i,j \leqslant \theta}$ is a finite Cartan matrix, $g_1, \dots, g_\theta$ are *central* elements in Γ, and $\chi_1, \dots, \chi_\theta$ are multiplicative characters of Γ, such that $\chi_i(g_j)\chi_j(g_i) = \chi_i(g_i)^{a_{ij}}$ (plus some technical hypotheses on the orders of $\chi_i(g_j)$), then a finite-dimensional pointed Hopf algebra H with group $G(H) \simeq \Gamma$ can be constructed from this datum. Besides these, only a small number of examples have appeared in print; in these examples, Γ is $\mathbb{S}_3$, $\mathbb{S}_4$, $\mathbb{D}_4$ (see [MS]), $\mathbb{S}_5$ (using [FK]), $\mathbb{A}_4 \times \mathbb{Z}/2$ (see [G1]).
3. An important invariant of a pointed Hopf algebra H is its *infinitesimal braiding*; this is a braided vector space, that is, a pair (V, c), where V is a vector space and $c \in \mathrm{Aut}(V \otimes V)$ is a solution of the braid equation: $(c \otimes \mathrm{id})(\mathrm{id} \otimes c)(c \otimes \mathrm{id}) = (\mathrm{id} \otimes c)(c \otimes \mathrm{id})(\mathrm{id} \otimes c)$. Let $\mathfrak{B}(V)$ be the Nichols algebra of (V, c), see [AS2]. If $\dim H$ is finite, then $\dim \mathfrak{B}(V)$ is finite and divides $\dim H$. Conversely, given a braided vector space (V, c), where V is a Yetter–Drinfeld module over the group algebra $\mathbb{C}\Gamma$, then the Radford's biproduct, or bosonization, $H = \mathfrak{B}(V) \# \mathbb{C}\Gamma$ is a pointed Hopf algebra with $G(H) \simeq \Gamma$. Thus, a fundamental problem is to determine the dimension of the Nichols algebra of a finite-dimensional braided vector space. We remark that the same braided vector space can arise as the infinitesimal braiding of pointed Hopf algebras H with very different $G(H)$, as in the examples with Cartan matrices above. Analogously, there are infinitely many finite-dimensional pointed Hopf algebras H, with non-isomorphic groups $G(H)$ and the same infinitesimal braiding as, respectively, the examples above related to the groups $\mathbb{S}_3$, $\mathbb{S}_4$, $\mathbb{D}_4$, $\mathbb{S}_5$, $\mathbb{A}_4 \times \mathbb{Z}/2$; and such that they are link-indecomposable in the sense of [MS,M].
4. It is then more convenient to study in a first stage Nichols algebras of braided vector spaces of group-type [G1, Definition 1.4.10]. However, there are strong constraints on a braided vector space of group-type to have a finite-dimensional Nichols algebra [G1, Lemma 3.1]. Briefly, we shall consider in this paper the class of braided vector spaces of the form $(\mathbb{C}X, c^q)$; where $(X, \triangleright)$ is a finite rack, q is a 2-cocycle with values on the multiplicative group of invertible elements of $\mathbb{C}$, and c^q is given by $c^q(i \otimes j) = q_{ij}\, i \triangleright j \otimes i$ (see the precise definitions in the main part of the text). See also the discussion in [A, Chapter 5].

We are faced with the following questions: to determine the general structure of finite racks; to compute their second cohomology groups; and to decide whether the dimensions of the corresponding Nichols algebras are finite.

5. We now describe the contents of this paper. The notions of "rack" and "quandle", sets provided with a binary operation like the conjugation of a group, have been considered in the literature, mainly as a way to produce knot invariants (cf. [B,CJKLS,De,FR,J1,K,Ma]). Section 1 is a short survey of the theory of racks and quandles, addressed to non-specialists on these structures, including a variety of examples relevant for this paper.

The determination of all finite racks is a very hard task. There are two successive approximations to this problem. First, any finite rack is a union of indecomposable components. However, indecomposable racks can be put together in many different ways, and the description of all possible ways is again very difficult. In other words, even the determination of all indecomposable finite racks would not solve the general question.

In Section 2, we describe epimorphisms of racks and quandles by general cocycles. We then introduce modules over a quandle, resp. a rack, X. We show that modules over X are in one-to-one correspondence with the abelian group objects in the category of arrows over X, if X is indecomposable. Our definition of modules over X generalizes those in [CES,CENS].

We say that a non-trivial rack is *simple* if it has no proper quotients. Then any indecomposable finite rack with cardinality >1 is an extension of a simple rack. We study simple racks in Section 3. One of our main results is the explicit classification of all finite simple racks, see Theorems 3.9 and 3.12. The proof is based on a group-theoretical result kindly communicated to us by Guralnick.

After acceptance of this paper, it became to our attention Joyce's article [J2], where results similar to those in Section 3.2 are obtained. However, notice that our classification in Theorem 3.9 includes more quandles than that of [J2, Theorem 7(2)]. This is one of the reasons why we decided to leave our results. The other reason is that, by using a result in [EGS] (which depends upon the classification of simple groups), we can split the simple quandles into two classes regarding their cardinality. These classes appear naturally in [J2] also, but the fact that they are split by cardinality was impossible to prove in 1982.

It is natural to define homology and cohomology theories of racks and quandles as standard homology and cohomology theories for abelian group objects in the category of arrows over X [Q]. We propose in Section 4 a complex that, conjecturally, would be suitable to compute these homology and cohomology theories. We show that the homology and cohomology theories known so far (see [CENS,CJKLS,FR,G1]) are special cases of ours. We discuss as well non-abelian cohomology theories.

A braided vector space of the form $(\mathbb{C}Y, c^q)$ *does not* determine the rack Y and the 2-cocycle q. We provide a general way of constructing two braided vector spaces $(\mathbb{C}Y, c^q)$ and $(\mathbb{C}\tilde{Y}, c^{\tilde{q}})$ where the racks Y and $\tilde{Y}$ are not isomorphic in general, but such that the corresponding Nichols algebras have the same dimension. In our construction, Y is an extension $X \times_\alpha A$, where A is an

X-module; $\tilde{Y}$ is an extension $X \times_\beta \hat{A}$, where $\hat{A}$, the group of characters of A, is also an X-module. The construction can be thought as a Fourier transform. We show how to use this construction to obtain new examples of pointed Hopf algebras with non-abelian group of group-like elements. This is the content of Section 5.

In Section 6, we present several new examples of finite-dimensional Nichols algebras $\mathfrak{B}(V)$ over finite groups. First, we show that some Nichols algebras can be computed by reduction to Nichols algebras of diagonal type, via Fourier transform. Next we use Fourier transform again to compute a Nichols algebra related to the faces of the cube, starting from a Nichols algebra related to the transpositions of $\mathbb{S}_4$ computed in [MS]. Finally, we establish some relations that hold in Nichols algebras related to affine racks, and use them to compute Nichols algebras related to the vertices of the tetrahedron (a result announced in [G1]) and the affine rack $(\mathbb{Z}/5, \triangleright^2)$. Support to our proofs is given by Theorem 6.4 which gives criteria to insure that a finite dimensional braided Hopf algebra is a Nichols algebra.

In most of the paper, we shall only consider finite racks, or quandles, or crossed sets, and omit the word "finite" when designing them, unless explicitly stated.

6. In conclusion, we remark that the next natural step in the classification of finite-dimensional pointed Hopf algebras is to deal with Nichols algebras of braided vector spaces arising from *simple* racks.

1. Preliminaries

1.1. Racks, quandles and crossed sets

Definition 1.1. A *rack* is a pair $(X, \triangleright)$ where X is a non-empty set and $\triangleright : X \times X \to X$ is a function, such that

$$\phi_i : X \to X, \quad \phi_i(j) = i \triangleright j, \quad \text{is a bijection for all } i \in X, \tag{1.1}$$

$$i \triangleright (j \triangleright k) = (i \triangleright j) \triangleright (i \triangleright k) \quad \forall i, j, k \in X. \tag{1.2}$$

A *quandle* is a rack $(X, \triangleright)$ which further satisfies

$$i \triangleright i = i, \quad \text{for all } i \in X. \tag{1.3}$$

A *crossed set* is a quandle $(X, \triangleright)$ which further satisfies

$$j \triangleright i = i \text{ whenever } i \triangleright j = j. \tag{1.4}$$

A morphism of racks is defined in the obvious way: $\psi : (X, \triangleright) \to (Y, \triangleright)$ is a morphism of racks if $\psi(i \triangleright j) = \psi(i) \triangleright \psi(j)$, for all $i, j \in X$. Morphisms of quandles (resp. crossed sets) are morphisms of racks between quandles (resp. crossed sets).

In particular, a subrack of a rack $(X, \triangleright)$ is a non-empty subset Y such that $Y \triangleright Y = Y$. If X is a crossed set and Y is a subrack, then, clearly, it is a crossed subset; same for quandles.

Definition 1.2. If Γ is a group, any non-empty subset $X \subseteq \Gamma$ stable under conjugation by Γ (i.e, a union of conjugacy classes) is a crossed set with the structure $i \triangleright j = iji^{-1}$. A crossed set isomorphic to one of these shall be called *standard*.

A primary goal is to compare arbitrary crossed sets with standard ones.

Definition 1.3. Let $(X, \triangleright)$ be a rack and let $\mathbb{S}_X$ denote the group of symmetries of X. By (1.1), we have a map $\phi : X \to \mathbb{S}_X$. Let $(X, \triangleright)$ be a rack. We set

$$\mathrm{Aut}_{\triangleright}(X) := \{g \in \mathbb{S}_X \colon g(i \triangleright j) = g(i) \triangleright g(j)\},$$

$$\mathrm{Inn}_{\triangleright}(X) := \text{the subgroup of } \mathbb{S}_X \text{ generated by } \phi(X).$$

By (1.2), $\mathrm{Inn}_{\triangleright}(X)$ is a subgroup of $\mathrm{Aut}_{\triangleright}(X)$. On the other hand, it is easy to see that

$$g\phi_x g^{-1} = \phi_{g(x)}, \quad \forall g \in \mathrm{Aut}_{\triangleright}(X),\ x \in X. \tag{1.5}$$

Therefore, $\phi(X) \subset \mathrm{Aut}_{\triangleright}(X)$ is a standard crossed subset, $\phi : X \to \mathrm{Aut}_{\triangleright}(X)$ is a morphism of racks, and $\mathrm{Inn}_{\triangleright}(X)$ is a normal subgroup of $\mathrm{Aut}_{\triangleright}(X)$. It is not true in general that $\mathrm{Inn}_{\triangleright}(X) = \mathrm{Aut}_{\triangleright}(X)$.

Example 1.4. Let $X = \{\pm i, \pm j\}$, a standard subset of the group of units of the quaternions. Then $\mathrm{Inn}_{\triangleright}(X) \neq \mathrm{Aut}_{\triangleright}(X)$.

Proof. It is easy to compute $\mathrm{Aut}_{\triangleright}(X)$ and $\mathrm{Inn}_{\triangleright}(X)$. One sees that $\mathrm{Inn}_{\triangleright}(X) = \langle \phi_i, \phi_j \rangle \simeq C_2 \times C_2$ and $\mathrm{Aut}_{\triangleright}(X) = \langle \phi_i, \phi_j, \sigma_0 \rangle$ has order 8, where $\sigma_0(\pm i) = \pm j$ and $\sigma_0(\pm j) = \pm i$. $\square$

Another basic group attached to X is the following one:

Definition 1.5 (Brieskorn [B], Fenn and Rourke [FR], Joyce [J1]). Let $(X, \triangleright)$ be a rack. We define the *enveloping group* of X as

$$G_X = F(X) / \langle xyx^{-1} = x \triangleright y,\ x, y \in X \rangle,$$

where $F(X)$ denotes the free group generated by X. The assignment $x \mapsto \phi_x$ extends to a group homomorphism $\pi_X : G_X \to \mathrm{Inn}_{\triangleright}(X)$; the kernel of π_X is called the *defect group* of X in the literature and coincides with the subgroup Γ considered in [So, Theorem 2.6].

The name "enveloping group" is justified by the following fact, contained essentially in [J1]:

Lemma 1.6. *The functor $X \mapsto G_X$ is left adjoint to the forgetful functor $H \mapsto \mathfrak{F}H$ from the category of groups to that of racks. That is,*

$$\mathrm{Hom}_{\mathrm{groups}}(G_X, H) \simeq \mathrm{Hom}_{\mathrm{racks}}(X, \mathfrak{F}H)$$

by natural isomorphisms.

Proof. Easy. $\square$

The definition of rack was proposed a long time ago by Conway and Wraith, see the historical account in [FR]. Quandles were introduced independently in [J1,Ma] and studied later in [B] and other articles. They are being extensively studied nowadays in relation with knot invariants, see [CS] and references therein. In [G1], it was proposed to consider crossed sets with the normalizing conditions (1.3) and (1.4); the conditions also appear in [So]. It is worth noting that in most of these articles the quandle structure is the opposite to the one here (i.e., $x * y$ for our $\phi_y^{-1}(x)$). Racks, quandles and crossed sets are related as follows.

1.1.1. From racks to quandles

We follow [B]. Let X be a rack and let $C_{\triangleright}(X)$ be the centralizer in $\mathrm{Aut}_{\triangleright}(X)$ of $\mathrm{Inn}_{\triangleright}(X)$. For $\psi \in C_{\triangleright}(X)$, define $\triangleright^{\psi}$ by

$$a \triangleright^{\psi} b = a \triangleright \psi(b) = \psi(a \triangleright b) = \psi(a) \triangleright \psi(b). \tag{1.6}$$

Then $(X, \triangleright^{\psi})$ is again a rack; we say that it is *conjugated to* $(X, \triangleright)$ *via* ψ.

Let now $\imath : X \to X$ be given by $a \triangleright \imath(a) = a$, which is well defined by (1.1). Then, by (1.2),

$$a \triangleright b = a \triangleright (b \triangleright \imath(b)) = (a \triangleright b) \triangleright (a \triangleright \imath(b));$$

hence $a \triangleright \imath(b) = \imath(a \triangleright b)$. In particular, $a = \imath(a \triangleright a)$, and $\imath$ is surjective. Also,

$$a \triangleright (\imath(a) \triangleright \imath(b)) = (a \triangleright \imath(a)) \triangleright (a \triangleright \imath(b)) = a \triangleright (a \triangleright \imath(b)),$$

so that, by (1.1), $\imath(a) \triangleright \imath(b) = a \triangleright \imath(b) = \imath(a \triangleright b)$. Suppose now that $\imath(a) = \imath(b)$. Then

$$a = a \triangleright \imath(a) = \imath(a) \triangleright \imath(a) = \imath(b) \triangleright \imath(b) = b.$$

That is, $\imath$ is injective, and belongs to $C_{\triangleright}(X)$. We can then consider $(X, \triangleright^{\imath})$, which is a quandle.

In conclusion, any rack $(X, \triangleright)$ is conjugated to a unique quandle, called *the quandle associated to* $(X, \triangleright)$. If $F : X \to Y$ is a morphism of racks, then $F\imath = \imath F$;

hence F is a morphism of the associated quandles. It follows that $\mathrm{Aut}_{\triangleright}(X) \simeq \mathrm{Aut}_{\triangleright'}(X)$. (But $\mathrm{Inn}_{\triangleright}(X)$ and $\mathrm{Inn}_{\triangleright'}(X)$ may be very different).

1.1.2. From quandles to crossed sets

We exhibit a functor Q from the category of finite quandles to that of crossed sets, which assigns to a quandle X a quotient crossed set $Q(X)$ with the expected universal property: any morphism of quandles $X \to Y$ is uniquely factorized through $Q(X)$ whenever Y is a crossed set. To see this, take on X $\sim$ as the equivalence relation generated by

$$x \sim x' \text{ if } \exists y \text{ s.t. } x \triangleright y = y \quad \text{and} \quad y \triangleright x = x'. \tag{1.7}$$

Then $\sim$ coincides with the identity relation if and only if X is a crossed set. Take $X_1 := X/\sim$. We must see that X_1 inherits the structure of a quandle. First, suppose x, x', y are as in (1.7). Then $x' \triangleright y = (y \triangleright x) \triangleright (y \triangleright y) = y \triangleright (x \triangleright y) = y$. Next, for $z \in X$, we have

$$\begin{aligned} y \triangleright (x' \triangleright z) &= (x' \triangleright y) \triangleright (x' \triangleright z) = x' \triangleright (y \triangleright z) \\ &= (y \triangleright x) \triangleright (y \triangleright z) = y \triangleright (x \triangleright z), \end{aligned}$$

whence we see that $\phi_x = \phi_{x'}$, and then $\phi_x = \phi_{x''}$ for any $x'' \sim x$. Thus, it makes sense to consider $\triangleright : (X/\sim) \times X \to X$. Finally, we have for $z \in X$,

$$(z \triangleright x) \triangleright (z \triangleright y) = z \triangleright (x \triangleright y) = (z \triangleright y)$$

and

$$(z \triangleright y) \triangleright (z \triangleright x) = z \triangleright (y \triangleright x) = (z \triangleright x').$$

Then $(z \triangleright x) \sim (z \triangleright x')$, and it makes sense to consider $\triangleright : (X/\sim) \times (X/\sim) \to (X/\sim)$. If X_1 is not a crossed set then take $X_2 = X_1/\sim$, and so on. Since X is finite, we must eventually arrive to a crossed set. The functoriality and universal property are clear.

1.2. Basic definitions

We collect now a number of definitions and results; many of them appear already in previous papers on racks or quandles, see [B,CJKLS,FR,J1].

We shall say that X is *trivial* if $i \triangleright j = j$ for all $i, j \in X$.

Lemma 1.7. *Let $(X, \triangleright)$ be a rack, H a group and $\varphi : X \to H$ an injective morphism of racks such that the image is invariant under conjugation in H (thus $(X, \triangleright)$ is actually a crossed set). Then the map $\tilde{\varphi} : H \to \mathbb{S}_X$, given by $\tilde{\varphi}_h(x) = \varphi^{-1}(h\varphi(x)h^{-1})$, is a group homomorphism and its image is contained in* $\mathrm{Aut}_{\triangleright}(X)$.

Proof. Left to the reader. □

The assignment $X \mapsto \mathrm{Inn}_{\triangleright}(X)$ is not functorial in general; just take $i \in X$ with $\phi_i \neq \mathrm{id}$; the inclusion $\{i\} \subset X$ does not extend to a morphism $\mathrm{Inn}_{\triangleright}(\{i\}) \to \mathrm{Inn}_{\triangleright}(X)$ commuting with ϕ. But we have:

Lemma 1.8. *If $\pi : X \to Y$ is a surjective morphism of racks, then it extends to a group homomorphism $\mathrm{Inn}_{\triangleright}(\pi) : \mathrm{Inn}_{\triangleright}(X) \to \mathrm{Inn}_{\triangleright}(Y)$.*

Proof. Let $\mathrm{Inn}_{\triangleright}(\pi)$ be defined on $\phi(X)$ by $\mathrm{Inn}_{\triangleright}(\pi)(\phi(x)) = \phi(\pi(x))$. It is well defined and it extends to a morphism of groups since π is surjective. $\square$

We determine now the structure of $\mathrm{Inn}_{\triangleright}(X)$ when X is standard.

Lemma 1.9. *Let H be a group and let $X \subset H$ be a standard subset.*

(1) $\mathrm{Inn}_{\triangleright}(X) \simeq C/Z(C)$, *where $C = \langle X \rangle$ is the subgroup of H generated by X, which is clearly normal.*
(2) *If X generates H then* $\mathrm{Inn}_{\triangleright}(X) \simeq H/Z(H)$.
(3) *If H is simple non-abelian and $X \neq \{1\}$, then $H = \mathrm{Inn}_{\triangleright}(X)$.*

Proof. We prove (2); (1) and (3) will follow. By Lemma 1.7, we have a morphism $\psi : H \to \mathrm{Aut}_{\triangleright}(X)$, whose image is $\mathrm{Inn}_{\triangleright}(X)$. Now, $h \in \ker(\psi) \Leftrightarrow hxh^{-1} = x \ \forall x \in X \Leftrightarrow h \in Z(H)$. $\square$

Corollary 1.10. *Let X be a rack, let H be a group and let $\psi : X \to H$ be a morphism. If $Z(\langle \psi(X) \rangle)$ is trivial, then ψ extends to a morphism $\Psi : \mathrm{Inn}_{\triangleright}(X) \to H$.*

Proof. If $Y = \psi(X)$, then $\Psi : \mathrm{Inn}_{\triangleright}(X) \xrightarrow{\mathrm{Inn}_{\triangleright}(\psi)} \mathrm{Inn}_{\triangleright}(Y) \simeq \langle Y \rangle \hookrightarrow H$. $\square$

The map $\phi : X \to \mathrm{Inn}_{\triangleright}(X)$ is not injective, in general.

Definition 1.11. We shall say that the rack $(X, \triangleright)$ is *faithful* when the corresponding ϕ is injective. Observe that in this case X is a crossed set, since it is standard.

Remark 1.12. If $(X, \triangleright)$ is faithful then the center of $\mathrm{Inn}_{\triangleright}(X)$ is trivial. More generally, if $z \in Z(\mathrm{Inn}_{\triangleright}(X))$, then $\phi_{z(i)} = \phi_i$, for all $i \in X$.

Definition 1.13. A *decomposition* of a rack $(X, \triangleright)$ is a disjoint union $X = Y \cup Z$ such that Y and Z are both subracks of X. (In particular, both Y and Z are non-empty). X is *decomposable* if it admits a decomposition, and *indecomposable* otherwise.

The image of an indecomposable rack under a morphism is again indecomposable.

We shall occasionally denote $i^n \triangleright j := \phi_i^n(j)$, $n \in \mathbb{Z}$. The *orbit* of an element $x \in X$ is the subset

$$\mathcal{O}_x := \{i_s^{\pm 1} \triangleright (i_{s-1}^{\pm 1} \triangleright (\dots (i_1^{\pm 1} \triangleright x) \dots)) \mid i_1, \dots, i_s \in X\}.$$

That is, $\mathcal{O}_x$ is the orbit of x under the natural action of the group $\mathrm{Inn}_{\triangleright}(X)$. (If X is finite, then $\mathcal{O}_x = \{i_s \triangleright (i_{s-1} \triangleright (\dots (i_1 \triangleright x) \dots)) \mid i_1, \dots, i_s \in X\}$).

Lemma 1.14. *Let $(X, \triangleright)$ be a rack, $Y \neq X$ a non-empty subset and $Z = X - Y$. Then the following are equivalent*:

(1) *$X = Y \cup Z$ is a decomposition of X.*
(2) *$Y \triangleright Z \subseteq Z$ and $Z \triangleright Y \subseteq Y$.*
(3) *$X \triangleright Y \subseteq Y$.*

Proof. Easy. □

Lemma 1.15. *Let $(X, \triangleright)$ be a rack. Then the following are equivalent*:

(1) *X is indecomposable.*
(2) *$X = \mathcal{O}_x$ for all* (*for some*) *$x \in X$.*

Proof. Easy. □

Note that a standard crossed set $X \subset H$ need not be indecomposable, even if it consists of only one H-orbit. However, it is so when H is simple by Lemma 1.9.

Example 1.16. If $X \subset H$ is a conjugacy class with two elements, then it is trivial as crossed set. As another example, take A an abelian group and G the group of automorphisms of A; let $H = A \rtimes G$, and let $X \subset A$ be any orbit for the action of G. Let $1_G \in G$ be the unit and consider $X \subset H$ as $X \rtimes 1_G$. Then X is trivial.

Proposition 1.17. *Any rack X is the disjoint union of maximal indecomposable subracks.*

Proof. Given $Y \subset X$ a subset, consider

$$Y' = Y \cup (Y \triangleright Y) \cup (Y^{-1} \triangleright Y) = Y \cup \{y \triangleright z \mid y, z \in Y\} \cup \{y^{-1} \triangleright z \mid y, z \in Y\}.$$

Then $Y' \supset Y$ and any subrack of X containing Y contains Y'. The *subrack generated* by Y is thus $\bigcup_{n \in \mathbb{N}} Y^n$, where $Y^{n+1} = (Y^n)'$ and $Y^1 = Y$. This is the smallest subrack of X containing Y.

For $Y \subset X$, we say that it is *connectable* if for any two elements $y_1, y_2 \in Y$ there exist $u_1^{\varepsilon_1}, \dots, u_n^{\varepsilon_n}$, where $u_i \in Y$ and $\varepsilon_i \in \{\pm 1\}$ $\forall i$, such that $y_2 = u_1^{\varepsilon_1} \triangleright (u_2^{\varepsilon_2} \triangleright \cdots (u_n^{\varepsilon_n} \triangleright y_1))$ (here the intermediate elements $u_i^{\varepsilon_i} \triangleright (u_{i+1}^{\varepsilon_{i+1}} \triangleright \cdots (u_n^{\varepsilon_n} \triangleright y_1))$ may not belong to Y). Then it is easy to see that if Y is connectable then so is Y'.

Hence, for Y connectable, the subrack generated by Y is connectable and, being a subrack, it is indecomposable. Also, since the union of intersecting indecomposable subracks is connectable, we see that they generate an indecomposable subrack. Hence the *indecomposable component* of $x \in X$, the union of all indecomposable subracks containing x, is an indecomposable subrack. Now, X is the disjoint union of such components. $\square$

Unlike the situation of Lemma 1.14, the indecomposable components may not be stable under the action of X. The case of two components is more satisfactory because we can describe how to glue two racks.

Lemma 1.18.

(1) *Let Y, Z be two racks and $X = Y \sqcup Z$ be their disjoint union. The following are equivalent*:
   (a) *Structures of rack on X such that $X = Y \cup Z$ is a decomposition.*
   (b) *Pairs (σ, τ) of morphisms of racks $\sigma: Y \to \mathrm{Aut}_{\triangleright}(Z)$, $\tau: Z \to \mathrm{Aut}_{\triangleright}(Y)$ such that*

$$y \triangleright \tau_z(u) = \tau_{\sigma_y(z)}(y \triangleright u), \quad \forall y, u \in Y, \ z \in Z, \quad i.e., \ \phi_y \tau_z = \tau_{\sigma_y(z)} \phi_y; \tag{1.8}$$

$$z \triangleright \sigma_y(w) = \sigma_{\tau_z(y)}(z \triangleright w), \quad \forall y \in Y, \ z, w \in Z, \quad i.e., \ \phi_z \sigma_y = \sigma_{\tau_z(y)} \phi_z. \tag{1.9}$$

(2) *Assume that Y and Z are crossed sets and* (1.8), (1.9) *hold. Then X is a crossed set exactly when*

$$\sigma_y(z) = z \ \textit{if and only if} \ \tau_z(y) = y, \quad \forall y \in Y, \ z \in Z. \tag{1.10}$$

Proof. Left to the reader. $\square$

If the conditions of the lemma are satisfied, we shall say that X is the *amalgamated sum* of Y and Z. If σ and τ are trivial, we say that X is the *disjoint sum* of Y and Z. Clearly, one can define the disjoint sum of any family of racks (resp. quandles, crossed sets).

For example, let X be a rack (resp. quandle, crossed set) and set $X \times 2 = 2X = X \times \{1, 2\}$; this is a rack (resp. quandle, crossed set) with $(x, i) \triangleright (y, j) = (x \triangleright y, j)$, and $2X = X_1 \cup X_2$ is a decomposition, where $X_i = X \times \{i\}$. Note that $\phi_{(x,i)} = \phi_{(x,j)}$; ϕ is not injective. In an analogous way, we define the crossed set nX, for any positive integer n. More generally, we have

Example 1.19. Let X, Y be two racks (resp. quandles, crossed sets). Then $X \times Y$ is a rack (resp. quandle, crossed set), with $(x, y) \triangleright (u, v) = (x \triangleright u, y \triangleright v)$; this is the direct product of X and Y in the category of racks (resp. quandles, crossed sets).

Lemma 1.20. *Let X, Y be two racks (resp. quandles, crossed sets). If $X \times Y$ is indecomposable then X and Y are indecomposable. The converse is true if X or Y is a quandle.*

Proof. Since the canonical projections $X \times Y \to X$ and $X \times Y \to Y$ are rack homomorphisms, the first statement is immediate. For the second one, let $(x_1, y_1), (x_2, y_2) \in X \times Y$. As X, Y are indecomposable, there exist $u_1^{\varepsilon_1}, \dots, u_n^{\varepsilon_n}$, $v_1^{\varepsilon'_1}, \dots, v_m^{\varepsilon'_m}$ where $u_i \in X$, $v_j \in Y$ and $\varepsilon_i, \varepsilon'_j \in \{\pm 1\}$ $\forall i,j$, such that $x_2 = u_1^{\varepsilon_1} \triangleright (u_2^{\varepsilon_2} \triangleright \cdots (u_n^{\varepsilon_n} \triangleright x_1))$ and $y_2 = v_1^{\varepsilon'_1} \triangleright (v_2^{\varepsilon'_2} \triangleright \cdots (v_m^{\varepsilon'_m} \triangleright y_1))$. Suppose X is a quandle. Adding if necessary at the end of the sequence in Y pairs y_1, y_1^{-1}, we may suppose that $m \geqslant n$. Adding if necessary at the end of the sequence in X elements x_1, we may suppose that $m = n$. Then,

$$(x_2, y_2) = (u_1^{\varepsilon_1}, v_1^{\varepsilon'_1}) \triangleright ((u_2^{\varepsilon_2}, v_2^{\varepsilon'_2}) \triangleright \cdots ((u_n^{\varepsilon_n}, v_n^{\varepsilon'_n}) \triangleright (x_1, y_1))). \qquad \square$$

Let X be a rack, take $\phi : X \to \mathrm{Inn}_{\triangleright}(X)$ as usual. Let us abbreviate $F_y \coloneqq \phi^{-1}(y)$, a fiber of ϕ. If X is a quandle, any fiber F_y is a trivial subquandle of X.

Lemma 1.21. (1) *For $x, y \in \phi(X)$ the fibers F_y and $F_{x \triangleright y}$ have the same cardinality.*

(2) *If X is an indecomposable crossed set, then the fibers of ϕ all have the same cardinality.*

Proof. We claim that $i \triangleright F_y \subseteq F_{\phi_i \triangleright y}$. Indeed, if $j \in F_y$, then $\phi_{i \triangleright j} = \phi_i \phi_j \phi_i^{-1} = \phi_i y \phi_i^{-1} = \phi_i \triangleright y$; the claim follows. Similarly, $i^{-1} \triangleright F_y \subseteq F_{\phi_i^{-1} \triangleright y}$, hence (1). Now (2) follows from (1). $\square$

We give finally some definitions of special classes of crossed sets, following [J1].

Definition 1.22. Let $(X, \triangleright)$ be a quandle. We shall say that X is *involutory* if $\phi_x^2 = \mathrm{id}$ for all $x \in X$. That is, if $x \triangleright (x \triangleright y) = y$ for all $x, y \in X$.

We shall say that X is *abelian* if $(x \triangleright w) \triangleright (y \triangleright z) = (x \triangleright y) \triangleright (w \triangleright z)$ for all $x, y, w, z \in X$.

1.3. Examples

1.3.1. A rack which is not a quandle

Take X any set and $f \in \mathbb{S}_X$ any function. Let $x \triangleright y = f(y)$. This is a rack, and it is not a quandle if $f \neq \mathrm{id}_X$. This rack is called *permutation rack*.

1.3.2. A quandle which is not a crossed set

Take $X = \{x, +, -\}$, $x \triangleright \pm = \mp$, $\phi_\pm = \mathrm{id}_X$.

1.3.3. Amalgamated sums

Let Z be a rack; we describe all the amalgamated sums $X = Y \cup Z$ for $Y = \{0, 1\}$ the trivial rack. Denote $\mathrm{Aut}(Y) = \{+ = \mathrm{id}, -\}$. Let σ, τ be as in Lemma 1.18. First, Z should decompose as a disjoint union of subracks $Z = Z_+ \cup Z_-$, where $\tau(Z_\pm) = \pm$. Second, (1.8) is equivalent to $Z_\pm$ being stable by σ_0 and σ_1; and condition (1.9) reads

$$\phi_z\sigma_0 = \sigma_0\phi_z, \quad \phi_z\sigma_1 = \sigma_1\phi_z, \quad \forall z \in Z_+,$$

$$\phi_z\sigma_0 = \sigma_1\phi_z, \quad \phi_z\sigma_1 = \sigma_0\phi_z, \quad \forall z \in Z_-.$$

Another way to describe the situation is: $Z = Z_+ \cup Z_-$ a disjoint union; let $C_+ = \langle \phi_x, \ x \in Z_+ \rangle$ be the group generated by ϕ_{Z_+}, $C_- = \langle \phi_x\phi_y, \ x, y \in Z_- \rangle$, and let $C = \langle C_+, C_- \rangle$. Then $[\sigma_0, C] = 1 \in \mathbb{S}_Z$, $\sigma_1 = \phi_x\sigma_0\phi_x^{-1}$ for any $x \in Z_-$. If Z is a quandle then X is a quandle. If Z is a crossed set then X is a crossed set iff $Z_+ = Z^{\sigma_0} = \{\text{fixed points of } \sigma_0\} = Z^{\sigma_1}$.

1.3.4. Polyhedral crossed sets

Let $P \subset \mathbb{R}^3$ be a regular polyhedron with vertices $X = \{x_1, \dots, x_n\}$ and center in 0. For $1 \leqslant i \leqslant n$, let T_i be the orthogonal linear map which fixes x_i and rotates the orthogonal plane by an angle of $2\pi/r$ with the right-hand rule (pointing the thumb to x_i), where r is the number of edges ending in each vertex. Then $(X, \triangleright)$ defined by $x_i \triangleright x_j = T_i(x_j)$ is a crossed set. To see this, simply take $\mathcal{G}$ as the group of orthogonal transformations of P with determinant 1 and notice that $\{T_1, \dots, T_n\}$ is a conjugacy class of $\mathcal{G}$, whose underlying (standard) crossed set is isomorphic to X. It is evident that $\mathrm{Inn}_\triangleright(X)$ is isomorphic to the group generated by $\{T_1, \dots, T_n\}$. It is clear that to each polyhedron also corresponds an analogous crossed set given by the faces; it is isomorphic to the crossed set given by the vertices of the dual polyhedron. It follows by inspection that the crossed sets of the vertices of the tetrahedron, the octahedron, the dodecahedron and the icosahedron are indecomposable, while that of the cube has two components, each of which is isomorphic to the crossed set of the vertices of the tetrahedron. It is easy to see that in the indecomposable cases the group $\mathrm{Inn}_\triangleright(X)$ coincides with $\mathcal{G}$. See Fig. 1.

1.3.5. Coxeter racks

Let $(V, \langle\,,\rangle)$ be a vector space over a field k, provided with an anisotropic symmetric bilinear form $\langle\,,\rangle$. Let $v \triangleright u = u - \frac{2\langle u,v\rangle}{\langle v,v\rangle} v$. Then $(V - \{0\}, \triangleright)$ is a rack, as well as any subset closed for this operation. Particular cases of this are the root systems of semisimple Lie algebras; the action ϕ_α coincides with the action of $w_\alpha \in W$, the Weyl group. To turn this into a quandle one can either quotient out by the relation $v \sim -v$, or take the conjugated quandle $(V - \{0\}, \triangleright^\iota)$ as in 1.1.1 (see (1.6)). It is easy to see that $v \triangleright^\iota u = \frac{2\langle u,v\rangle}{\langle v,v\rangle} v - u$, and then this also is a crossed set.

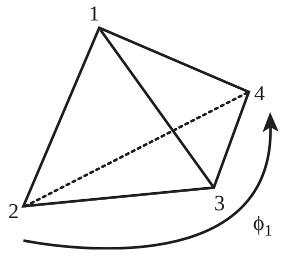


Fig. 1. Polyhedral crossed set of the tetrahedron.

1.3.6. Homogeneous crossed sets

Let G be a finite group and let $\phi : \mathbb{S}_G \to \mathrm{Fun}(G, \mathbb{S}_G)$ be the function given by

$$\phi^s_x(y) = s(yx^{-1})x, \quad s \in \mathbb{S}_G, \ x, y \in G.$$

Then $\phi^s_x \phi^t_x = \phi^{st}_x$, i.e., ϕ is a morphism of groups, with the pointwise multiplication in $\mathrm{Fun}(G, \mathbb{S}_G)$.

If, in addition, $s : G \to G$ is a group automorphism, then define $x \triangleright y = \phi^s_x(y) = s(yx^{-1})x$. It is easy to see that this makes $(G, \triangleright)$ into a crossed set. For instance, let us check (1.4):

$$x \triangleright y = y \ \Leftrightarrow \ y = s(yx^{-1})x \ \Leftrightarrow \ yx^{-1} = s(yx^{-1}) \ \Leftrightarrow \ xy^{-1} = s(xy^{-1}) \ \Leftrightarrow \ y \triangleright x = x.$$

We shall say that $(G, \triangleright)$ is a *principal homogeneous* crossed set, and we will denote it by (G, s).

Let $t : G \to G$, $t(x) = s(x^{-1})x$, so that $x \triangleright y = s(y)\, t(x)$. It is clear that

$$\phi_x = \phi_z \ \Leftrightarrow \ t(x) = t(z), \tag{1.11}$$

whence the fibers as a crossed set are the same as the fibers of t. Note that t is a group homomorphism if and only if $\mathrm{Im}(t) \subseteq Z(G)$, the center of G.

More generally, let $H \subset G^s$ be a subgroup, where G^s is the subgroup of elements of G fixed by s. Then $H \backslash G$ is a crossed set, with $Hx \triangleright Hy = Hs(yx^{-1})x$; it is called a *homogeneous* crossed set.

It can be shown that a crossed set X is homogeneous if and only if it is a single orbit under the action of $\mathrm{Aut}_{\triangleright}(X)$ [J1].

1.3.7. Twisted homogeneous crossed sets

In the same vein, let G be a group and $s \in \mathrm{Aut}(G)$. Take $x \triangleright y = xs(yx^{-1})$. This is a crossed set which is different, in general, to the previous one. Any orbit of this is called a *twisted homogeneous crossed set*.

1.3.8. Affine crossed sets

Let A be a finite abelian group and $g: A \to A$ an isomorphism of groups. The corresponding principal homogeneous crossed set is called an *affine* crossed set, and denoted by (A, g). (They are also called Alexander quandles, see e.g. [CJKLS]).

Let $f = \mathrm{id} - g$, then $x \triangleright y = x + g(y - x) = f(x) + g(y)$.

Let us compute the orbits of (A, g). Since $g = \mathrm{id} - f$, we have $x \triangleright y = f(x - y) + y$. It is clear then by induction that $x_1 \triangleright (x_2 \triangleright \cdots (x_n \triangleright y)) \in y + f(A)$, whence $\mathcal{O}_y = y + \mathrm{Im}(f)$. In this case, by (1.11), indecomposable is equivalent to being faithful (since A is finite).

We compute now when two indecomposable affine crossed sets are isomorphic.

Lemma 1.23. *Two indecomposable affine crossed sets (A, g) and (B, h) are isomorphic if and only if there exists a linear isomorphism $T: A \to B$ such that $Tg = hT$.*

If this happens, any isomorphism of crossed sets $U: (A, g) \to (B, h)$ can be uniquely written as $U = \tau_b T$, where $\tau_b: B \to B$ is the translation $\tau_b(x) = x + b$ and $T: A \to B$ is a linear isomorphism such that $Tg = hT$.

Proof. Let $U: (A, g) \to (B, h)$ be an isomorphism of crossed sets. Since the translations are isomorphisms of crossed sets, we decompose $U = \tau_b T$, where T is an isomorphism of crossed sets with $T(0) = 0$. Let $f = \mathrm{id} - g$, $k = \mathrm{id} - h$. We have

$$T(f(x) + g(y)) = k(T(x)) + h(T(y)).$$

Letting $x = 0$, we see that $Tg = hT$; letting $y = 0$, we see that $Tf = kT$. Hence $T(f(x) + g(y)) = T(f(x)) + T(g(y))$. But (A, g) is indecomposable, thus f is bijective; we conclude that T is linear. $\square$

Remark 1.24. After we finished (the first version of) the paper, Nelson gave in [Ne] a classification of non-indecomposable affine crossed sets.

Corollary 1.25. *If (A, g) is an indecomposable affine crossed set, then $\mathrm{Aut}_{\triangleright}(A, g)$ is the semidirect product $A \rtimes \mathrm{Aut}(A)^g$, where $\mathrm{Aut}(A)^g$ is the subgroup of all linear automorphisms of A such that $Tg = gT$.*

Proof. Easy. $\square$

Notice that when (A, g) is not indecomposable, the corollary does not hold. For instance, if $g = \mathrm{id}$, then $f = 0$ and (A, id) is trivial, whence $\mathrm{Aut}_{\triangleright}(A, g) = \mathbb{S}_A$.

The group $\mathrm{Inn}_{\triangleright}(A, g)$ is usually smaller: it can be easily shown that $\mathrm{Inn}_{\triangleright}(A, g) = \mathrm{Im} f \rtimes \langle g \rangle$. In fact, if $a \in A$ then $\phi_a = (f(a), g) \in A \rtimes \mathrm{Aut}(A)^g$. In particular, $\mathrm{Inn}_{\triangleright}(A, g)$ is solvable.

Remark 1.26. We conclude that a standard crossed set $\mathcal{O}$, where $\mathcal{O}$ is a single non-trivial orbit of a simple non-abelian group, cannot be affine; cf. Lemma 1.9.

Similarly, let us discuss when a polyhedral crossed set X is affine. The crossed set of vertices of the tetrahedron is affine, actually isomorphic to ($A = \mathbb{Z}_2 \times \mathbb{Z}_2$, $g = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$). It can be seen by hand that the crossed set of the vertices of the cube is not affine. Indeed, it is easy to see that the underlying group A should be either $\mathbb{Z}/2 \times \mathbb{Z}/4$ or $(\mathbb{Z}/2)^3$, but since $\mathrm{Aut}(\mathbb{Z}/2 \times \mathbb{Z}/4)$ has order 8 and $\mathrm{Inn}_{\triangleright}(X)$ has 3-torsion, the case $A = \mathbb{Z}/2 \times \mathbb{Z}/4$ is impossible. Furthermore, one can exclude the case $A = (\mathbb{Z}/2)^3$ by looking at automorphisms $g \in \mathrm{Aut}(A)$ s.t. $g^3 = \mathrm{id}$. For the other polyhedral crossed sets, we have that $\mathrm{Inn}_{\triangleright}(X)$ is $\mathbb{S}_4$ for the octahedron, and $\mathbb{A}_5$ for the icosahedron and the dodecahedron, so that X is not affine.

As a particular case, let $A = \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, and let $q \in \mathbb{Z}_n^{\times}$ such that $(1-q) \in \mathbb{Z}_n^{\times}$. Then we have a structure on $\mathbb{Z}_n$ given by

$$(\mathbb{Z}_n, \ \triangleright^q), \quad x \triangleright^q y = (1-q)x + qy.$$

This is an indecomposable crossed set, and it can be seen that $(\mathbb{Z}_n, \ \triangleright^q) \simeq (\mathbb{Z}_n, \ \triangleright^{q'}) \Leftrightarrow q = q'$ (by Lemma 1.23, since $\mathrm{Aut}(\mathbb{Z}_n)$ is abelian).

It is immediate to see that $(\mathbb{Z}_3, \ \triangleright^2)$ is the only indecomposable crossed set with three elements; and that any crossed set with three elements is either trivial or isomorphic to $(\mathbb{Z}_3, \ \triangleright^2)$.

It is proved in [EGS] that any indecomposable rack of prime order p is either isomorphic to $(\mathbb{Z}_p, \ \triangleright^q)$ for $q \in \mathbb{Z}_p^{\times}$ or it is isomorphic to $(\mathbb{Z}_p, \triangleright)$ with $x \triangleright y = y + 1$. Indecomposable racks of order p^2 are classified in [G3], in particular it is proved there that any indecomposable quandle of order p^2 is affine.

1.3.9. Affine racks

These are a generalization of affine quandles. Let A be an abelian group, $g \in \mathrm{Aut}(A), f \in \mathrm{End}(A)$ be such that $fg = gf$ and $f(\mathrm{id} - g - f) = 0$. We define then on A the structure of rack given by $x \triangleright y = f(x) + g(y)$. It is clear that A is a quandle iff $f = \mathrm{id} - g$. Notice that $(\mathrm{id} - f)(\mathrm{id} + g^{-1}f) = \mathrm{id}$; thus $\mathrm{id} - f$ is an automorphism of A. We can consider then the affine quandle $(A, \mathrm{id} - f)$. It is easy to see that this quandle is the associated quandle for the rack just defined (see (1.6)). As an example, one can take $A = \mathbb{Z}_{p^2}$, $g = \mathrm{id}$, $f(x) = px$.

1.3.10. Amalgamated unions of affine crossed sets

Let (A, g), (A, h) be two indecomposable affine crossed sets; let f, k be given by $f = \mathrm{id} - g$, $k = \mathrm{id} - h$, and let $\sigma : (A, g) \to \mathrm{Aut}_{\triangleright}(A, h)$, $\tau : (A, h) \to \mathrm{Aut}_{\triangleright}(A, g)$ have the form $\sigma_x = \alpha(x) + \beta$ (i.e., $\sigma_x(y) = \alpha(x) + \beta(y)$) and $\tau_y = \gamma + \delta(y)$ (i.e., $\tau_y(x) = \gamma(x) + \delta(y)$) for certain $\beta, \gamma \in \mathrm{Aut}(A)$, $\alpha, \delta \in \mathrm{End}(A)$. Then by Lemma 1.23 we must have $\beta \in (\mathrm{Aut}(A))^h$, $\gamma \in (\mathrm{Aut}(A))^g$ and one can verify that

$$(1.8) \quad \text{is equivalent to} \quad f - f\gamma - \delta\alpha = 0, \quad \delta\beta - g\delta = 0;$$

$$(1.9) \quad \text{is equivalent to} \quad k - k\beta - \alpha\delta = 0, \quad \alpha\gamma - h\alpha = 0;$$

$$(1.10) \quad \text{is equivalent to} \quad \alpha(x) + \beta(y) = y \Leftrightarrow \gamma(x) + \delta(y) = x.$$

Thus, the disjoint union $X = (A, g) \sqcup (A, h)$ is a decomposable crossed set. For instance, let $h = -gf^{-1} = \mathrm{id} - f^{-1}$. We define σ and τ by taking $\alpha = \mathrm{id}$, $\beta = g$, $\gamma = h$, $\delta = \mathrm{id}$.

If (A, g), (B, h) are non-isomorphic indecomposable affine crossed sets, then any amalgamated sum $A \cup B$ is not affine. This is a consequence of the following easy lemma:

Lemma 1.27. *If (A, g) is an affine crossed set, then its orbits are isomorphic as crossed sets.*

Proof. Let $\{x_0 = 0, \dots, x_n\}$ be a full set of representatives of coclasses in $A/\mathrm{Im}(f)$. The orbits are $\mathrm{Im}(f)$, $\mathrm{Im}(f) + x_1, \dots, \mathrm{Im}(f) + x_n$. Thus, $\tau_i : \mathrm{Im}(f) + x_i \to \mathrm{Im}(f)$, $\tau_i(y) = y - x_i$ are isomorphisms. $\square$

1.3.11. Involutory crossed sets

This is a discretization of symmetric spaces, which we shall roughly present (see [J1] for the full explanation). Let S be a set provided with a collection of functions $\gamma : \mathbb{Z} \to S$, called *geodesics*, such that any two points of S belong to the image of some of them. Consider the affine crossed set $(\mathbb{Z}, -1)$. Assume that the following condition holds: if $x, y \in S$ belong to two geodesics γ and γ', say $\gamma(n) = \gamma'(n') = x$, $\gamma(m) = \gamma'(m') = y$, then $\gamma(n \triangleright m) = \gamma'(n' \triangleright m')$. Then we can define on S a unique binary operation $\triangleright$ in such a way that the geodesics respect $\triangleright$, namely, $x \triangleright y = \gamma(n \triangleright m) = \gamma(2n - m)$ for any geodesic γ such that $\gamma(n) = x$ and $\gamma(m) = y$. This operation furnishes S with the structure of an involutory crossed set if it maps geodesics to geodesics; that is, if $x \triangleright \gamma$ is a geodesic for any x and any γ. It can be shown that any involutory crossed set arises in this way [J1].

1.3.12. Core crossed sets

Let G be a group. The *core* of G is the crossed set $(G, \triangleright)$, where $x \triangleright y = xy^{-1}x$. The core is an involutory crossed set. If G is abelian, its core is the affine crossed set with $g = -\mathrm{id}$. More generally, one can define the core of a Moufang loop.

1.3.13. The free quandle of a set

Let C be a set and let $F(C)$ be the free group generated by C; let $\mathcal{O}_c$ denote the orbit of $c \in C$ in $F(C)$. We claim that the standard crossed set $X_C \coloneqq \bigcup_{c \in C} \mathcal{O}_c$ is the free quandle on the set C.

For, let $\psi : C \to (X, \triangleright)$ be any function and let $\Psi : F(C) \to \mathrm{Inn}_{\triangleright}(X)$ be the unique group homomorphism extending $c \mapsto \phi_{\psi(c)}$. We define then $\hat{\psi} : X_C \to X$ by

$$\hat{\psi}(y) = \Psi(u)(c), \quad \text{if } y = ucu^{-1}, \ c \in C.$$

The well-definiteness of $\hat{\psi}$ is a consequence of the following facts about orbits in free groups:

(1) If $c, d \in C$ and $\mathcal{O}_c = \mathcal{O}_d$, then $c = d$.
(2) The centralizer of $c \in C$ is $\langle c \rangle$.

It is not difficult to see that $\hat{\psi}$ is indeed a morphism of quandles extending ψ, and the unique one. It is easy to see that X_C is also the free crossed set generated by C. It is not, however, a free rack.

2. Extensions

2.1. Extensions with dynamical cocycle

We now discuss another way of constructing racks (resp. quandles, crossed sets), generalizing Example 1.19. The proof of the following result is essentially straightforward.

Lemma 2.1. *Let X be a rack and let S be a non-empty set. Let $\alpha : X \times X \to \mathrm{Fun}(S \times S, S)$ be a function, so that for each $i, j \in X$ and $s, t \in S$ we have an element $\alpha_{ij}(s,t) \in S$. We will write $\alpha_{ij}(s) : S \to S$ the function $\alpha_{ij}(s)(t) = \alpha_{ij}(s,t)$. Then $X \times S$ is a rack with respect to*

$$(i,s) \triangleright (j,t) = (i \triangleright j, \alpha_{ij}(s,t))$$

if and only if the following conditions hold:

$$\alpha_{ij}(s) \text{ is a bijection}; \tag{2.1}$$

$$\alpha_{i,j\triangleright k}(s, \alpha_{jk}(t,u)) = \alpha_{i\triangleright j, i\triangleright k}(\alpha_{ij}(s,t), \alpha_{ik}(s,u)) \quad \forall i,j,k \in X, \;\; s,t,u \in S. \tag{2.2}$$

in other words, $\alpha_{i,j\triangleright k}(s)\alpha_{j,k}(t) = \alpha_{i\triangleright j, i\triangleright k}(\alpha_{i,j}(s,t))\alpha_{i,k}(s)$.

If X is a quandle, then $X \times S$ is a quandle iff further

$$\alpha_{ii}(s,s) = s \quad \text{for all } i \in X \text{ and } s \in S. \tag{2.3}$$

If X is a crossed set, then $X \times S$ is a crossed set iff further

$$\alpha_{ji}(t,s) = s \text{ whenever } i \triangleright j = j \text{ and } \alpha_{ij}(s,t) = t \quad \forall i,j \in X, \;\; s,t \in S. \tag{2.4}$$

Proof. Easy. $\square$

Definition 2.2. If these conditions hold we say that α is a *dynamical cocycle* and that $X \times S$ is an extension of X by S; we shall denote it by $X \times_\alpha S$. When necessary, we shall say that α is a *rack* (*resp. quandle*, *crossed set*) *dynamical cocycle* to specify that we require it to satisfy (2.1) + (2.2) (resp. (2.1) + (2.2) + (2.3), (2.1) + (2.2) + (2.3) + (2.4)). The presence of the parameter s justifies the name of "dynamical".

Assume that X is a quandle and let α be a quandle dynamical cocycle. For $i \in X$ consider $s \triangleright_i t := \alpha_{ii}(s,t)$. It is immediate to see that $(S, \triangleright_i)$ becomes a quandle $\forall i \in X$. Then (2.2), when $j = k$, says:

$$\alpha_{ij}(s, t \triangleright_j u) = \alpha_{ij}(s,t) \triangleright_{i \triangleright j} \alpha_{ij}(s,u), \quad \forall s,t,u \in S. \tag{2.5}$$

In other words, the map $\alpha_{ij}(s)$ is an isomorphism of quandles $\alpha_{ij}(s) : (S, \triangleright_j) \to (\mathrm{S}, \triangleright_{\mathrm{i} \triangleright \mathrm{j}})$.

The projection $X \times_\alpha S \to X$ is clearly a morphism. Conversely, it turns out that projections of indecomposable racks (resp. quandles, crossed sets) are always extensions. Before going over this, we state a technical lemma for further use.

Lemma 2.3. *Let $(X, \triangleright)$ be a quandle which is a disjoint union $X = \coprod_{i \in Y} X_i$ such that there exists $\bar{\triangleright} : Y \times Y \to Y$ with $X_i \triangleright X_j = X_{i \bar{\triangleright} j}$. Suppose that* $\mathrm{card}(X_i) = \mathrm{card}(X_j)$ $\forall i,j$ (*this holds for instance if X is indecomposable*). *Then $(Y, \bar{\triangleright})$ is a quandle.*

Furthermore, take S a set such that $\mathrm{card}(S) = \mathrm{card}(X_i)$ *and for each $i \in Y$ set $g_i : X_i \to S$ a bijection. Let $\alpha : Y \times Y \to \mathrm{Fun}(S \times S, S)$ be given by $\alpha_{ij}(s,t) := g_{i \bar{\triangleright} j}(g_i^{-1}(s) \triangleright g_j^{-1}(t))$. Then α is a dynamical cocycle and $X \simeq Y \times_\alpha S$.*

Proof. This follows without troubles from Lemma 2.1. □

Remark 2.4. (1) Within the hypotheses of the lemma, if X is indecomposable then so is Y.

(2) The whole lemma can be stated in terms of racks.

(3) In order to state the lemma in terms of crossed sets, it is necessary to further assume that $(Y, \bar{\triangleright})$ is a crossed set, i.e., that it satisfies (1.4).

Corollary 2.5. *Let $(X, \triangleright)$, $(Y, \bar{\triangleright})$ be quandles* (*resp. racks, crossed sets*). *Let $f : X \to Y$ be a surjective morphism such that the fibers $f^{-1}(y)$ all have the same cardinality* (*this happens for instance if X is indecomposable*). *Then X is an extension $X = Y \times_\alpha S$.*

Proof. Easy. □

Let X be a rack. Let $\alpha : X \times X \to \mathrm{Fun}(S \times S, S)$ be a dynamical cocycle and let $\gamma : X \to \mathbb{S}_S$ be a function. Define $\alpha' : X \times X \to \mathrm{Fun}(S \times S, S)$ by

$$\alpha_{ij}(s,t) = \gamma_{i \triangleright j}(\alpha_{ij}(\gamma_i^{-1}(s), \gamma_j^{-1}(t))), \quad \text{i.e.,} \ \alpha'_{ij}(s) = \gamma_{i \triangleright j} \alpha_{ij}(\gamma_i^{-1}(s)) \gamma_j^{-1}. \tag{2.6}$$

Then α' is a dynamical cocycle and we have an isomorphism of racks $T:(X\times_\alpha S)\to(X\times_{\alpha'} S)$ given by $T(i,s)=(i,\gamma_i(s))$. Conversely, if there is an isomorphism of racks $T:(X\times_\alpha S)\to(X\times_{\alpha'} S)$ which commutes with the canonical projection $X\times S\to X$ then there exists $\gamma:X\to\mathbb{S}_S$ such that α and α' are related as in (2.6).

Definition 2.6. We say that α and α' are *cohomologous* if and only if there exists $\gamma:X\to\mathbb{S}_S$ such that α and α' are related as in (2.6).

Example 2.7. Let Y be the crossed set given by the faces of the cube. Then Y is the disjoint union of the subsets made out of the pairs of opposite faces. This union satisfies the hypotheses of Lemma 2.3 and, being indecomposable, the quotient $(X,\bar{\triangleright})$ is isomorphic to the crossed set $(\mathbb{Z}_3,\ \triangleright^2)$.

Example 2.8. Let (A,g) be an affine crossed set. Suppose that there exists a subgroup $B\subseteq A$ invariant by g; let $\bar{g}$ be the induced automorphism of A/B. Consider the affine crossed set $(A/B,\bar{g})$; the projection $(A,g)\xrightarrow{\pi}(A/B,\bar{g})$ is a morphism of crossed sets. Corollary 2.5 applies and we see that A is an extension of A/B.

More examples appear in [CHNS] by means of group extensions. They are used to color twist-spun knots.

2.2. Extensions with constant cocycle

Let X be a rack. Let $\beta:X\times X\to\mathbb{S}_S$. We say that β is a *constant rack cocycle* if

$$\beta_{i,j\triangleright k}\beta_{j,k}=\beta_{i\triangleright j,i\triangleright k}\beta_{i,k}. \tag{2.7}$$

If X is a quandle, we say that β is a *constant quandle cocycle* if it further satisfies

$$\beta_{ii}=\mathrm{id},\quad \forall i\in X. \tag{2.8}$$

If X is a crossed set, we say that β is a *constant crossed set cocycle* if it further satisfies

$$\beta_{ji}=\mathrm{id}\text{ whenever } i\triangleright j=j \text{ and } \beta_{ij}(t)=t \text{ for some } t\in S. \tag{2.9}$$

We have then an extension $X\times_\beta S:=X\times_\alpha S$, taking $\alpha_{ij}(s,t)=\beta_{ij}(t)$. Note that $\triangleright_i$ is trivial for all i, and the fiber $F_{\phi_{(i,s)}}=F_{\phi_i}\times S$.

We shall say in this case that the extension is *non-abelian*. It is clear that an extension $X\times_\alpha S$ is non-abelian if and only if $\alpha_{ij}(s)=\alpha_{ij}(t)\ \forall s,t\in S,\ \forall i,j\in X$.

Definition 2.9. Let $\gamma:X\to\mathbb{S}_S$ be a function and let β be a constant cocycle. Define $\beta':X\times X\to\mathbb{S}_S$ by

$$\beta_{ij}=\gamma_{i\triangleright j}\,\beta_{ij}\,\gamma_j^{-1}.$$

Then we have an isomorphism $T:(X\times_\beta S)\to(X\times_{\beta'} S)$ given by $T(i,s)=(i,\gamma_i(s))$. In this case, we shall say that β and β' are *cohomologous*.

The use of the word "cocycle" is not only suggested by its analogy with group 2-cocycles, which describe extensions: there is a general definition of abelian cohomology (see Section 4) for which this is its natural non-abelian counterpart. The use of the word "cocycle" in the phrase "dynamical cocycle" stands on the same basis.

For $X\times_\beta S$ a non-abelian extension, let $\psi: X\to \mathrm{Inn}_\triangleright(X\times_\beta S)$ be given by $\psi_i=\phi_{(i,t)}$ for an arbitrary $t\in S$; that is, $\psi_i(j,s)=(i\triangleright j,\beta_{ij}(s))$. Then $\psi(X)$ generates $\mathrm{Inn}_\triangleright(X\times_\beta S)$. Let $H_i=\{h\in\mathrm{Inn}_\triangleright(X\times_\beta S)\mid h(i,s)\in i\times S\ \forall s\in S\}$.

Definition 2.10. Assume that X is indecomposable. A constant cocycle $\beta: X\times X\to\mathbb{S}_S$ is *transitive* if for some $i\in X$, the group H_i acts transitively on $i\times S$. Note that this definition does not depend on i.

We have seen that all the fibers of an indecomposable rack (resp. quandle, crossed set) have the same cardinality; we provide now a precise description of an indecomposable rack (resp. quandle, crossed set). Recall the map $\phi: Y\to\mathrm{Inn}_\triangleright(Y)$ from Definition 1.3.

Proposition 2.11. *Let Y be an indecomposable rack* (*resp. quandle*, *crossed set*), *let $X=\phi(Y)$ and let S be a set with the cardinality of the fibers of ϕ. Then we have an isomorphism $T: Y\to X\times_\beta S$ for some transitive constant cocycle β.*

Conversely, *a non-abelian extension $X\times_\beta S$ is indecomposable if and only if X is indecomposable and β is transitive.*

Proof. Choose, for each $x\in X$, a bijection $g_x: F_x=\phi^{-1}(x)\to S$. We have then a bijection $T: Y\to X\times S$, $T(i)=(\phi_i, g_{\phi_i}(i))$. We define, for $x,y\in X$ and $s\in S$, $\beta_{xy}(s)=g_{x\triangleright y}(T^{-1}(x,s)\triangleright T^{-1}(y,s))$. It is straightforward to see that β is a transitive constant cocycle and that T is an isomorphism.

The second part is clear. $\square$

Example 2.12. Let $X=\{1,2,3,4\}$ be the tetrahedral crossed set defined in Section 1.3 and let $S=\{a,b\}$. Then $\mathbb{S}_S=\{\mathrm{id},\sigma\}\simeq C_2=\{\pm1\}$. There is a non-trivial 2-cocycle $\beta: X\times X\to S$ given by

$$\begin{cases}\beta_{xy}=1 & \text{if } x=1 \text{ or } y=1 \text{ or } x=y,\\ \beta_{xy}=-1 & \text{otherwise.}\end{cases}$$

Let $\psi: X\to\mathrm{Inn}_\triangleright(X\times_\beta S)$ be as in the paragraph preceding Definition 2.10. It is clear that $\psi(1)\psi(2)\in H_4$, and $\psi(1)\psi(2)(4\times a)=\psi(1)(3\times b)=4\times b$, whence β is transitive and $X\times_\beta S$ is indecomposable.

A way to construct cocycles, which resembles the classification of Yetter–Drinfeld modules over group algebras, is the following one:

Example 2.13. Let X be an indecomposable (finite) rack, $x_0 \in X$ a fixed element, $G = \mathrm{Inn}_{\triangleright}(X)$, and let $H = G_{x_0}$ be the subgroup of the inner isomorphisms which fix x_0. Let Z be a (finite) set and $\rho : H \to \mathbb{S}_Z$ a group homomorphism. There is then a bijection $G/H \to X$ given by $g \mapsto g(x_0)$. Fix a (set theoretical) section $s : X \to G$; i.e., $s(x) \cdot x_0 = x \ \forall x \in X$. This determines, for each $x, y \in X$, an element $t_{x,y} \in H$ such that $\phi_x s(y) = s(x \triangleright y) t_{x,y}$. To see this, we compute

$$s(x \triangleright y)^{-1} \phi_x s(y) \cdot x_0 = s(x \triangleright y)^{-1} \phi_x \cdot y = s(x \triangleright y)^{-1} \cdot (x \triangleright y) = x_0.$$

Then it is straightforward to see that $\beta : X \times X \to \mathbb{S}_Z$, $\beta_{x,y} = \rho(t_{x,y})$ is a constant cocycle. Explicitly, this defines an extension $X \times_\beta Z$ as

$$(x, z) \triangleright (x', z') = (x \triangleright x', \rho(s(x \triangleright x')^{-1} \phi_x s(x'))(z')).$$

Even if X is a quandle, this is not a quandle in general, since it does not necessarily satisfy (2.8). Let us compute when (2.8) is satisfied (suppose that X is a quandle)

$$\beta_{x,x} = \rho(s(x \triangleright x)^{-1} \phi_x s(x)) = \rho(s(x)^{-1} \phi_x s(x)) = \rho(\phi_{s(x)^{-1} \cdot x}) = \rho(\phi_{x_0}).$$

Then $X \times_\beta Z$ is a quandle iff X is a quandle and $\rho(\phi_{x_0}) = 1 \in \mathbb{S}_Z$.

Remark 2.14. It is easy to see that for polyhedral quandles and affine quandles the group H is generated by ϕ_{x_0}, and then we cannot construct non-trivial quandle extensions in this way.

2.3. Modules over a rack

Throughout this subsection, $\mathfrak{R}$ will denote the category of racks. All the constructions below can be performed in the category $\mathfrak{Q}$ of quandles, or in the category $\mathfrak{CrS}$ of crossed sets.

It is clear that finite direct products exist in the category $\mathfrak{R}$, cf. Example 1.19. Then we can consider group objects in $\mathfrak{R}$; they are determined by the following Proposition.

Proposition 2.15. *A group object in $\mathfrak{R}$ is given by a triple (G, s, t), where G is a group, $s \in \mathrm{Aut}(G)$, $t : G \to Z(G)$ is a group homomorphism, and*

- $st = ts$,
- $s(x)x^{-1}t(x) \in \ker(t) \ \forall x \in G$.

The rack structure is given by $x \triangleright y = t(x)s(y)$.

A group object (G, s, t) *in* $\mathfrak{R}$ *is a quandle iff* $t(x) = s(x)^{-1}x\ \forall x \in G$, *iff it is an homogeneous quandle* (*hence crossed set*).

A group object (G, s, t) *in* $\mathfrak{R}$ *is abelian iff it is an affine rack.*

Proof. The second and third statements follow from the first without difficulties (notice that the image of t lies in the center).

A group object in $\mathfrak{R}$ is a triple $(G, \cdot, \triangleright)$ with $(G, \cdot)$ a group and $(G, \triangleright)$ a rack, such that the multiplication $\cdot$ is a morphism of racks. Let $s, t : G \to G$, $s(x) = 1 \triangleright x$, $t(x) = x \triangleright 1$. Then both s and t are group homomorphisms since $s(xy) = 1 \triangleright (xy) = (1 \cdot 1) \triangleright (x \cdot y) = (1 \triangleright x) \cdot (1 \triangleright y) = s(x)s(y)$, and analogously for t. Furthermore,

$$x \triangleright y = (1 \cdot x) \triangleright (y \cdot 1) = (1 \triangleright y) \cdot (x \triangleright 1) = s(y)t(x)$$

$$= (x \triangleright 1) \cdot (1 \triangleright y) = t(x)s(y).$$

Then, s must be an isomorphism, and then $t(x)$ is central $\forall x$. Last,

$$x \triangleright (y \triangleright z) = t(x) \cdot st(y) \cdot s^2(z),$$

$$(x \triangleright y) \triangleright (x \triangleright z) = t^2(x) \cdot ts(y) \cdot st(x) \cdot s^2(z),$$

whence $t(x) \cdot st(y) = t^2(x) \cdot ts(y) \cdot st(x)$. Taking $x = 1$ we see that $st = ts$. Taking $y = 1$ we see that $t(t(x)s(x)x^{-1}) = 1$. The converse is not difficult. $\square$

Let us now consider the "comma category" $\mathfrak{R}|_X$ over a fixed rack X; recall that the objects of $\mathfrak{R}|_X$ are the maps $f : Y \to X$ and the arrows between $f : Y \to X$ and $g : Z \to X$ are the commutative triangles, i.e., the maps $h : Y \to Z$ such that $gh = f$.

Since equalizers exist in $\mathfrak{R}$ (they are just the set-theoretical equalizers with the induced $\triangleright$), $\mathfrak{R}$ has finite limits. It follows that $\mathfrak{R}|_X$ also has finite limits. We are willing to determine all abelian group objects in $\mathfrak{R}|_X$.

Definition 2.16. Let X be a rack and let A be an abelian group. A *structure of* X*-module* on A consists of the following data:

- a family $(\eta_{ij})_{i,j \in X}$ of automorphisms of A, and
- a family $(\tau_{ij})_{i,j \in X}$ of endomorphisms of A,

such that the following axioms hold:

$$\eta_{i,j \triangleright k}\, \eta_{j,k} = \eta_{i \triangleright j, i \triangleright k}\, \eta_{i,k}, \tag{2.10}$$

$$\tau_{i,j \triangleright k} = \eta_{i \triangleright j, i \triangleright k}\, \tau_{i,k} + \tau_{i \triangleright j, i \triangleright k}\, \tau_{i,j}, \tag{2.11}$$

$$\eta_{i,j \triangleright k}\, \tau_{j,k} = \tau_{i \triangleright j, i \triangleright k}\, \eta_{i,j}. \tag{2.12}$$

If X is a quandle, a *quandle structure of* X*-module* on A is a structure of X-module which further satisfies

$$\eta_{ii} + \tau_{ii} = \mathrm{id}. \tag{2.13}$$

If X is a crossed set, a *crossed set structure of* X*-module* on A is a quandle structure of X-module which further satisfies

$$\text{if } i \triangleright j = j \text{ and } (\mathrm{id} - \eta_{ij})(t) = \tau_{ij}(s) \text{ for some } s, t \text{ then } (\mathrm{id} - \eta_{ji})(s) = \tau_{ji}(t). \tag{2.14}$$

An X*-module* is an abelian group A provided with a structure of X-module.

Remark 2.17. Taking $j = k$ in (2.10), one gets in presence of (1.3) the suggestive equality:

$$\eta_{i,j}\eta_{j,j} = \eta_{i \triangleright j, i \triangleright j}\eta_{i,j}. \tag{2.15}$$

Let A be an X-module. We define $\alpha_{ij} : A \times A \to A$ by

$$\alpha_{ij}(s,t) \coloneqq \eta_{ij}(t) + \tau_{ij}(s).$$

Theorem 2.18. (1) *α_{ij} is a dynamical cocycle, hence we can form the rack $Y = X \times_\alpha A$.*

(2) *The canonical projection $p : Y \to X$ is an abelian group in $\mathfrak{R}|_X$.*

(3) *If $p : Y \to X$ is an abelian group in $\mathfrak{R}|_X$ and X is indecomposable, then $Y \simeq X \times_\alpha A$ for some X-module A and p is the canonical projection.*

(4) *If X is a quandle and A is a quandle X-module, then the preceding statements are true in the category of quandles. Same for crossed sets.*

Proof.

(1) Condition (2.1) follows since η_{ij} is an automorphism. The left-hand side of (2.2) is

$$\eta_{i,j \triangleright k}\eta_{j,k}(u) + \eta_{i,j \triangleright k}\tau_{j,k}(t) + \tau_{i,j \triangleright k}(s)$$

and the right-hand side of (2.2) is

$$\eta_{i \triangleright j, i \triangleright k}\eta_{i,k}(u) + \tau_{i \triangleright j, i \triangleright k}\eta_{i,j}(t) + \eta_{i \triangleright j, i \triangleright k}\tau_{i,k}(s) + \tau_{i \triangleright j, i \triangleright k}\tau_{i,j}(s).$$

Thus, (2.2) follows from (2.10)–(2.12).

(2) Let $\sigma : X \to X \times_\alpha A$, $\sigma(i) = (i, 0)$, $i \in X$; it is clearly a morphism of racks. Let $+ : Y \times_X Y \to Y$, $(i,a) + (i,b) = (i, a+b)$; it is clearly a morphism in $\mathfrak{R}|_X$. It is not difficult to verify that $(Y, +)$ is an abelian group in $\mathfrak{R}|_X$ with identity element σ.

(3) Let $p : Y \to X$ be an abelian group in $\mathfrak{R}|_X$, X an arbitrary rack. We have morphisms in $\mathfrak{R}|_X$ $+ : Y \times_X Y \to Y$ and $\sigma : X \to Y$ satisfying the axioms of

abelian group. In particular, we have:

(a) The existence of σ implies that p is surjective; if $i \in X$, $A_i := p^{-1}(i)$ is an abelian group with identity $\sigma(i)$.
(b) $(a+b) \triangleright (c+d) = (a \triangleright c) + (b \triangleright d) \in A_{i \triangleright j}$, if $a, b \in A_i$, $c, d \in A_j$.
(c) The map $h_{ij} : A_j \to A_{i \triangleright j}$, h_{ij} the restriction of $\phi_{\sigma(i)}$, is an isomorphism of abelian groups, for all $i, j \in X$.

Assume now that X is indecomposable. Then all the abelian groups A_i are isomorphic, by (3c). Fix an abelian group A provided with group isomorphisms $\gamma_i : A_i \to A$. Define $\alpha_{ij} : A \times A \to A$, $i, j \in X$, by

$$\alpha_{ij}(s,t) := \gamma_{i \triangleright j}(\gamma_i^{-1}(s) \triangleright \gamma_j^{-1}(t)).$$

We claim that $\alpha_{ij}(s,t) = \eta_{ij}(t) + \tau_{ij}(s)$, where $\eta_{ij}(t) = \alpha_{ij}(0,t)$ and $\tau_{ij}(s) = \alpha_{ij}(s,0)$; this follows without difficulty from (3b), since the γ's are linear. Now, $\eta_{ij}(t) = \gamma_{i \triangleright j} h_{ij} \gamma_j^{-1}$ is a linear automorphism, whereas τ_{ij} is linear by (3b). We need finally to verify conditions (2.10)–(2.12); this is done reversing the arguments in part (1).

(4) Condition (2.3) amounts in the present case to (2.13), whereas condition (2.4) amounts to (2.14). $\square$

Remark 2.19. Assume now that X is a *non-indecomposable* quandle and keep the notation of the proof. Then A_i is a subquandle of Y, indeed an abelian group in $\mathfrak{Q}$. By Proposition 2.15, A_i is affine, with respect to some $g_i \in \mathrm{Aut}(A_i)$.

Example 2.20. If (A, g) is an affine crossed set, then it is an X-module over any rack X with $\eta_{ij} = g$, $\tau_{ij} = f = \mathrm{id} - g$. We shall say that A is a *trivial* X-module if $g = \mathrm{id}$, that is when it is trivial as crossed set.

Example 2.21. Let X be a trivial quandle, let $(A_i)_{i \in X}$ be a family of affine quandles and let Y be the disjoint sum of the A_i's, with the evident projection $Y \to X$. Then $Y \to X$ is an abelian group in $\mathfrak{Q}|_X$ which is not an extension of X by any X-module, if the A_i's are not isomorphic.

We now show that the category of X-modules, X an indecomposable quandle or rack, is abelian with enough projectives. Actually, it is equivalent to the category of modules over a suitable algebra.

Definition 2.22. The *rack algebra* of a rack $(X, \triangleright)$ is the $\mathbb{Z}$-algebra $\mathbb{Z}\{X\}$ presented by generators $(\eta_{ij}^{\pm 1})_{i,j \in X}$ and $(\tau_{ij})_{i,j \in X}$, with relations $\eta_{ij}\eta_{ij}^{-1} = \eta_{ij}^{-1}\eta_{ij} = 1$, (2.10), (2.11) and (2.12).

The *quandle algebra* of a quandle $(X, \triangleright)$ is the $\mathbb{Z}$-algebra $\mathbb{Z}(X)$ presented by generators $(\eta_{ij}^{\pm 1})_{i,j \in X}$ and $(\tau_{ij})_{i,j \in X}$, with relations $\eta_{ij}\eta_{ij}^{-1} = \eta_{ij}^{-1}\eta_{ij} = 1$, (2.10), (2.11), (2.12) and (2.13).

It is evident that the category of X-modules, X a rack, is equivalent to the category of modules over $\mathbb{Z}\{X\}$; therefore, it is abelian with enough injective and projective objects. Same for quandle X-modules and $\mathbb{Z}(X)$.

The algebra $\mathbb{Z}(X)$ is augmented with augmentation $\varepsilon : \mathbb{Z}(X) \to \mathbb{Z}$, $\varepsilon(\eta_{ij}) = 1$, $\varepsilon(\tau_{ij}) = 0$. The algebra $\mathbb{Z}\{X\}$ is also augmented, composing ε with the projection $\mathbb{Z}\{X\} \to \mathbb{Z}(X)$.

There are various interesting quotients of the algebra $\mathbb{Z}(X)$.

First, the quotient of $\mathbb{Z}(X)$ by the ideal generated by the τ_{ij}'s is isomorphic to the group algebra of the group $\Lambda(X)$ presented by generators $(\eta_{ij})_{i,j \in X}$ with relations (2.10).

Next, consider the following elements of the group algebra $\mathbb{Z}G_X$ (see Definition 1.5):

$$\eta_{ij} := i, \quad \tau_{ij} := 1 - (i \triangleright j). \tag{2.16}$$

It is not difficult to see that this defines a surjective algebra homomorphism $\mathbb{Z}(X) \to \mathbb{Z}G_X$; in particular any G_X-module has a natural structure of X-module.

Definition 2.23. If X is a crossed set and M is any G_X-module then M also satisfies the extra condition (2.14). We shall say that M is a *restricted X-module*.

Definition 2.24. Let X be a rack and let A be an X-module. A 2-*cocycle on X with values in A* is a collection $(\kappa_{ij})_{i,j \in X}$ of elements in A such that

$$\eta_{i,j \triangleright k}(\kappa_{jk}) + \kappa_{i,j \triangleright k} = \eta_{i \triangleright j, i \triangleright k}(\kappa_{ik}) + \tau_{i \triangleright j, i \triangleright k}(\kappa_{ij}) + \kappa_{i \triangleright j, i \triangleright k} \quad \forall i,j,k \in X. \tag{2.17}$$

Two 2-cocycles κ and κ' are *cohomologous* iff $\exists f : X \to A$ such that

$$\kappa'_{ij} = \kappa_{ij} - \eta_{ij}(f(j)) + f(i \triangleright j) - \tau_{ij}(f(i)). \tag{2.18}$$

As remarked earlier, the reader can find in Section 4 a complex which justifies these names.

Proposition 2.25.

(1) *Let X be a rack and consider functions* $\eta : X \times X \to \mathrm{Aut}(A)$, $\tau : X \times X \to \mathrm{End}(A)$, $\kappa : X \times X \to A$. *Let us define a map* α *by*

$$\alpha_{ij}(a,b) = \eta_{ij}(b) + \tau_{ij}(a) + \kappa_{ij}, \quad a,b \in A. \tag{2.19}$$

Then the following conditions are equivalent:
   (a) α *is a dynamical cocycle*.
   (b) η, τ *define a structure of an X-module on A and* (κ_{ij}) *is a* 2-*cocycle*, *i.e.*, *it satisfies* (2.17).

(2) *Let* κ *and* κ' *be* 2-*cocycles and let* α, α' *be their respective dynamical cocycles. If* κ *and* κ' *are cohomologous then* α *and* α' *are cohomologous.*

Proof. Straightforward. For the second part, if f is as in (2.18), then take $\gamma : X \to \mathbb{S}_A$ by $\gamma_i(s) = f(i) + s$. It is easy to verify (2.6). $\square$

Definition 2.26. If X is a rack, A is an X-module and $(\kappa_{ij})_{i,j \in X}$ is a 2-cocycle on X with values in A, then the extension $X \times_\alpha A$, where α is given by (2.19), is called an *affine module over X*. By abuse of notation, this extension will be denoted $X \times_\kappa A$.

All the constructions and results in this section are valid more generally over a fixed commutative ring R.

3. Simple racks

3.1. Faithful indecomposable crossed sets

To classify indecomposable racks, we may first consider faithful indecomposable crossed sets (recall that a faithful rack is necessarily a crossed set), and next compute all possible extensions.

Proposition 3.1. *Let X be an indecomposable finite rack. Then X is isomorphic to an extension $Y \times_\alpha S$, where Y is a faithful indecomposable crossed set. Furthermore, Y can be chosen uniquely with the property that any surjection $X \to Z$ of racks, with Z faithful, factorizes through Y.*

Proof. Consider the sequence $X \to X_1 \coloneqq \phi(X) \to X_2 \coloneqq \phi(X_1) \dots$. Since X is finite the sequence stabilizes, say at $Y = X_n$, which is clearly faithful and indecomposable. By Corollary 2.5, $X \simeq Y \times_\alpha S$. Now let $\psi : X \to Z$ be a surjection, with Z faithful. By Lemma 1.8, it gives a surjection $\psi_1 : X_1 \to Z$, and so on. $\square$

Faithful indecomposable crossed sets can be characterized as follows.

Proposition 3.2.

(1) *If X is a faithful indecomposable crossed set, then there exists a group G and an injective morphism of crossed sets $\varphi : X \to G$, such that $Z(G)$ is trivial and $\varphi(X)$ is a single orbit generating G as a group. Furthermore, G is unique up to isomorphisms with these conditions.*
(2) *If X is a single orbit in a group G with $Z(G)$ trivial and X generates G, then X is a faithful indecomposable crossed set.*
(3) *There is an equivalence of categories between*
   (a) *The category of faithful indecomposable crossed sets, with surjective morphisms.*
   (b) *The category of pairs $(G, \mathcal{O})$, where G is a group with trivial center and $\mathcal{O}$ is an orbit generating G; a morphism $f : (G, \mathcal{O}) \to (K, \mathcal{U})$ is a group homomorphism $f : G \to K$ such that $f(\mathcal{O}) = \mathcal{U}$.*

Proof.

(1) Existence: take $G = \mathrm{Inn}_{\triangleright}(X)$; uniqueness: by Lemma 1.9.
(2) Immediate.
(3) Follows from (1), (2) and Lemma 1.8. $\square$

We shall say that a projection (=surjective homomorphism) $\pi : X \to Y$ of racks is *trivial* if card Y is either 1 or card X.

Definition 3.3. A rack X is *simple* if it is not trivial and any projection of racks $\pi : X \to Y$ is trivial.

A decomposable rack has a projection onto the trivial rack with two elements; it follows that a simple rack is indecomposable.

Let X be a simple rack with n elements; then $\phi(X)$ has only one point, or ϕ is a bijection. In the first case, X is a permutation rack defined by a cycle of length n; in the second case X is a crossed set (and necessarily card $X > 2$).

It is not difficult to see that a permutation rack with n elements defined by a cycle of length n is simple if and only if n is prime.

Proposition 3.4. *Let X be an indecomposable faithful crossed set, which corresponds to a pair $(G, \mathcal{O})$. Then X is simple if and only if any quotient of G different from G is cyclic.*

Proof. Assume X is simple. If $\pi : G \to K$ is an epimorphism of groups, then either $\pi(X)$ is a single point or $\pi|_X$ is bijective. If $\pi(X)$ is a point, this point generates K, and then K must be cyclic. If $\pi|_X$ is bijective, take $h \in \ker(\pi)$; then $hxh^{-1} = x \ \forall x \in X$, whence $h \in Z(G)$. This means that π is bijective.

Assume now that any non-trivial quotient of G is cyclic. Let $\pi : X \to Y$ be a surjective morphism of crossed sets, then $G \simeq \mathrm{Inn}_{\triangleright}(X) \to \mathrm{Inn}_{\triangleright}(Y)$ is an epimorphism, so that either it is a bijection (then $X \simeq Y$) or $\mathrm{Inn}_{\triangleright}(Y)$ is cyclic. In the last case, $\phi(Y)$, being indecomposable, is a point; hence Y, being also indecomposable, is a point. $\square$

Example 3.5. Let X be the crossed set of the faces of the cube. We can realize X as the orbit given by 4-cycles inside $\mathbb{S}_4$, since X is faithful and $\mathrm{Inn}_{\triangleright}(X) \simeq \mathbb{S}_4$. Considering the quotient $\mathbb{S}_4 \to \mathbb{S}_4/K \simeq \mathbb{S}_3$, where K is the Klein subgroup, we see that X is not simple. Indeed, this gives X as the same extension $\mathbb{Z}_3 \times_\alpha \mathbb{Z}_2$ as in Example 2.7. Also, if X' is the orbit given by the six transpositions in $\mathbb{S}_4$, we see taking the same quotient $\mathbb{S}_4/K$ that X' is an extension $\mathbb{Z}_3 \times_{\alpha'} \mathbb{Z}_2$.

Example 3.6. Since the only proper quotient of $\mathbb{S}_n$ $(n \geqslant 5)$ is cyclic, we see that if X is a non-trivial orbit of $\mathbb{S}_n$ then either

- X generates $\mathbb{S}_n$ and then it is simple, or
- $X \subset \mathbb{A}_n$.

If $X \subset \mathbb{A}_n$, then it might fail to be an orbit in $\mathbb{A}_n$. This would happen if and only if the centralizers of the elements of X lie inside $\mathbb{A}_n$ (because the order of the orbits is the ratio between the order of the group and the order of the centralizers). In this case, thus, X decomposes as a union of two orbits, which are isomorphic via conjugation by any element in $\mathbb{S}_n \backslash \mathbb{A}_n$ (an example of this case arises for $n = 5$ and X the 5-cycles). On the other hand, if the centralizers of the elements of X are not included in $\mathbb{A}_n$ then X is indecomposable, and hence simple by the proposition.

3.2. Classification of simple racks

We characterize now simple racks in group-theoretical terms. We first classify finite groups G such that $Z(G)$ is trivial and G/N is cyclic for any normal non-trivial subgroup of G. We are grateful to R. Guralnick for help in this question.

To fix notation, if G acts on H, we put $H \rtimes G$ the semidirect product with structure $(h, g)(h', g') = (h(g \cdot h'), gg')$.

Theorem 3.7 (Guralnick). *Let G be a non-trivial finite group such that $Z(G)$ is trivial and G/H is cyclic for any normal non-trivial subgroup H. Then there are a simple group L, a positive integer t and a finite cyclic group $C = \langle x \rangle$ in* $\mathrm{Aut}(N)$, *where $N := L^t = L \times \cdots \times L$ (t times), such that one of the following possibilities hold.*

(1) *L is abelian, so that N is elementary abelian of order p^t, x is not trivial and it acts irreducibly on N. Furthermore, $G \simeq N \rtimes C$.*

(2) *L is simple non-abelian, $G = NC \simeq (N \rtimes C)/Z(N \rtimes C)$ and x acts by*

$$x \cdot (l_1, \ldots, l_t) = (\theta(l_t), l_1, \ldots, l_{t-1}) \tag{3.1}$$

for some $\theta \in \mathrm{Aut}(L)$.

Conversely, all the groups in (1) *or* (2) *have the desired properties. Furthermore, two groups in either of the lists are isomorphic if and only if the corresponding groups L are isomorphic, the corresponding integers t are equal and the corresponding automorphisms x define, up to conjugation, the same element* $\mathrm{Out}(N) = \mathrm{Aut}(N)/\mathrm{Int}(N)$.

Before proving the Theorem, we observe that:

- If G is a group which is not abelian and such that G/H is abelian for any normal non-trivial subgroup H, then G has a unique minimal non-trivial normal subgroup, namely $[G, G]$.
- If G is a finite group such that G/N is cyclic for any normal non-trivial subgroup N, then "$Z(G)$ is trivial" is equivalent to "G is non-abelian".
- Case (2) covers the case where G is non-abelian simple ($t = 1$, C is trivial).
- In case (1), identify L with $\mathbb{F}_p$ and the automorphism x with $T \in \mathrm{GL}(t, \mathbb{F}_p)$. Then x acts irreducibly if and only if the characteristic polynomial of T is irreducible, hence equals the minimal polynomial of T. In this case, if $n = \mathrm{ord}\, x$ and if d divides n, $1 \neq d \neq n$, then $\ker(T^d - \mathrm{id}) = 0$; this implies that $N - 0$ is a union of

copies of C. Hence $|C|$ divides $p^t - 1$. Clearly, we may assume that x acts by the companion matrix of an irreducible polynomial in $\mathbb{F}_p[X]$ of degree t.

- Let N, C be two groups, C acting on N by group automorphisms. The center $Z(N \rtimes C)$ is given by $Z(N \rtimes C) = \{(n, c) \mid c \in Z(C),\ n \in N^C,\ c \cdot m = n^{-1}mn\ \forall m \in N\}$. In particular, if $p : (N \rtimes C) \to (N \rtimes C)/Z(N \rtimes C)$ is the projection then $p(N) \simeq N/Z(N)^C$.

Proof. *Step* I: We first show that the groups described in the Theorem have the desired properties.

Let $L,\ N,\ C,\ G$ be as in case (1). By the irreducibility of the action of C, being x non-trivial, we see that $Z(G)$ is trivial. We claim that any non-trivial normal subgroup M of G contains N. For, $M \cap N$ is either trivial or $M \cap N = N$. If $a \in G$ and $m \in M,\ m \neq e$; then $[a, m] \in M \cap [G, G] \subseteq M \cap N$. Thus $M \cap N$ is non-trivial, since otherwise $m \in Z(G)$, proving the claim. Hence any non-trivial quotient of G, being a quotient of C, is cyclic, and G satisfies the requirements of the theorem.

Let now $L,\ N,\ C,\ G$ be as in case (2). We identify N with its image in G. We claim next that $Z(G)$ is trivial. Let $(n, c) \in N \rtimes C$ be such that $p(n, c) = nc \in Z(G)$. It is easy to see that $n \in N^x$ and c acts on N by conjugation by n^{-1}. Thus $(n, c) \in Z(N \rtimes C)$ and $nc = 1$ in G.

Any normal subgroup P of N is of the form $\prod_{j \in J} L_j$, for some subset J of $\{1, \ldots, t\}$; if P is also x-stable then either P is trivial or equals N, because x permutes the copies of L. As in case (1), we conclude that any non-trivial normal subgroup M of G contains N; hence any non-trivial quotient of G is cyclic.

Step II: Let G be a finite group with a minimal normal non-trivial subgroup N, and assume that G/N is cyclic. Then there exists a simple subgroup L of N, and a subgroup $C = \langle x \rangle$ of G such that $N = L \times \cdots \times L$ (t copies) and $G = NC$.

Indeed, let $x \in G$ be such that its class generates G/N and let C be the subgroup generated by x; then $G = NC$. Let L be a minimal normal non-trivial subgroup of N. Then $L_i := x^{i-1}Lx^{-i+1}$ is also a minimal normal subgroup of N and $(L_1 \cdots L_j) \cap L_{j+1}$ is either trivial or L_{j+1}. Let t be the smallest positive integer such that $(L_1 \cdots L_t) \cap L_{t+1} = L_{t+1}$. Then $L_1 \cdots L_t \simeq L_1 \times \cdots \times L_t$ is a normal subgroup of N and is stable by conjugation by x; so it is normal in G and therefore equal to N. If S is a normal subgroup of L, then $S \simeq S \times 1 \times \cdots \times 1$ is normal in N, and by minimality of L, L is simple.

Step III: We now show that any group G satisfying the requirements of the theorem is either as in case (1) or (2). We may assume that G is not simple. We keep the notation of Step II and assume then that $Z(G)$ is trivial and that any proper quotient of G is cyclic.

If N is abelian then $N \cap C \subseteq Z(G)$ is trivial, whence $G = N \rtimes C$. Furthermore, x should act irreducibly since any subgroup $P \subset N$ which is x-stable is normal. Hence, G is as in case (1).

If L is not abelian and $t > 1$ we have, for $i > 1$, $[xL_tx^{-1}, L_i] = x[L_t, L_{i-1}]x^{-1} = 1$, from where x sends L_t isomorphically to L_1, and x acts as in case (2) of the statement. Consider the projection $p : N \rtimes C \to G$. Since $Z(G)$ is trivial,

$Z(N \rtimes C) \subset \ker(p)$. Let now $(n,c) \in \ker(p)$; then $c = n^{-1}$ in G, whence c acts by conjugation on N by n^{-1}. Thus $(n,c) \in Z(N \rtimes C)$, and we are done.

Step IV: We prove the uniqueness statement. N is unique since, as remarked, $N = [G,G]$. Now, L is unique by Jordan–Hölder, then t is unique. Since x was chosen modulo N, x and x' give rise to the same group if they coincide in $\mathrm{Out}(N)$. Furthermore, since any automorphism $G \to G$ must leave N invariant, x is unique up to conjugation in $\mathrm{Out}(N)$. $\square$

Remark 3.8. Let N, C be finite groups with C acting on N by group automorphisms, and let $G = N \rtimes C$. If $(m,z),(n,y) \in G$, then

$$(m,z)(n,y)(m,z)^{-1} = (m(z \cdot n)(zyz^{-1} \cdot m^{-1}), zyz^{-1}).$$

When C is abelian, it follows that

$$\mathscr{C}(n,y) = \bigcup_{z \in C} \mathcal{O}_y(z \cdot n) \times \{y\}, \tag{3.2}$$

where $\mathscr{C}$ stands for conjugacy class, and $\mathcal{O}_y$ for the orbit under the action of N on itself given by

$$m \rightharpoonup_y n := mn(y \cdot m^{-1}). \tag{3.3}$$

Note that $\bigcup_{z \in \langle y \rangle} \mathcal{O}_y(z \cdot n) = \mathcal{O}_y(n)$. For, $n^{-1} \rightharpoonup_y n = y \cdot n$, and the claim follows. Note also that $m \rightharpoonup_y n$ is *not* the same as $m \triangleright n$.

We can now state the classification of simple racks. We begin by the following important theorem. The proof uses [EGS, Lemma 8], which is in turn based on the classification of simple finite groups.

Theorem 3.9. *Let $(X, \triangleright)$ be a simple crossed set and let p be a prime number. Then the following are equivalent.*

(1) *X has p^t elements, for some $t \in \mathbb{N}$.*
(2) *$\mathrm{Inn}_{\triangleright}(X)$ is solvable.*
(3) *$\mathrm{Inn}_{\triangleright}(X)$ is as in case* (1) *of Theorem* 3.7.
(4) *X is an affine crossed set $(\mathbb{F}_p^t, T)$ where $T \in \mathrm{GL}(t, \mathbb{F}_p)$ acts irreducibly.*

Proof.

- $(1 \Rightarrow 2)$ This is [EGS, Lemma 8].
- $(2 \Rightarrow 3)$ This is Proposition 3.4 plus Theorem 3.7.
- $(3 \Rightarrow 4)$ This follows from the preceding discussion. Since $\phi(X) \subset \mathrm{Inn}_{\triangleright}(X)$ is a conjugacy class, by (3.2) we have $\phi(X) = N \times \{x^r\}$ for some r. Since $\phi(X)$ generates $\mathrm{Inn}_{\triangleright}(X)$, r must be coprime to the order of x. Take $y = x^r$ and call $T \in \mathrm{GL}(t, \mathbb{F}_p)$ the action of y (which is also irreducible).

We have

$$(m,y) \triangleright (n,y) = (m,y)(n,y)(m,y)^{-1} = (Tn + (\mathrm{id} - T)m, y).$$

$(4 \Rightarrow 1)$ Clear. $\square$

Corollary 3.10. *The classification of simple racks with p^t elements, for some prime number p and $t \in \mathbb{N}$, is the following*:

1. *Affine crossed sets $(\mathbb{F}_p^t, T)$, where T is the companion matrix of an irreducible monic polynomial in $\mathbb{F}_p[X]$ different from $X - 1$ and X.*
2. *The permutation rack corresponding to the cycle $(1, 2, \ldots, p)$ if $t = 1$.*

Proof. Easy. $\square$

Remark 3.11. Keep the notation of Step III in Theorem 3.7. If L is abelian, then x does not necessarily send L_t to L_1, as wrongly stated in [J2, Lemma 4(ii)]. This explains why in [J2, Lemma 6], only irreducible polynomials of the form $X^t - a$ appear; while, as we have seen, this restriction is not necessary.

Theorem 3.12. *Let $(X, \triangleright)$ be a crossed set whose cardinality is divisible by at least two different primes. Then the following are equivalent.*

1. *X is simple.*
2. *There exist a non-abelian simple group L, a positive integer t and $x \in \mathrm{Aut}(L^t)$, where x acts by* (3.1) *for some $\theta \in \mathrm{Aut}(L)$, such that $X = \mathcal{O}_x(n)$ is an orbit of the action $\rightharpoonup_x$ of $N = L^t$ on itself as in* (3.3) *($n \neq m^{-1}$ if $t = 1$ and x is inner, $x(p) = mpm^{-1}$). Furthermore, L and t are unique, and x only depends on its conjugacy class in $\mathrm{Out}(L^t)$. If $m, p \in X$ then*

$$m \triangleright p = mx(pm^{-1}). \tag{3.4}$$

Proof.

$(1 \Rightarrow 2)$ By Theorem 3.9, $\mathrm{Inn}_{\triangleright}(X)$ is as in case (2) of Theorem 3.7. Therefore, we have L, t and $x \in \mathrm{Aut}(L^t)$. Let $G = (N \rtimes C)/Z(N \rtimes C) \simeq \mathrm{Inn}_{\triangleright}(X)$, and $\tilde{G} = N \rtimes C$ and let $p : \tilde{G} \to G$ be the projection. If $\mathscr{C}(n, y)$ is a conjugacy class in $\tilde{G}$ then $p(\mathscr{C}(n, y))$ is a conjugacy class in G, and it is not difficult to see that $p : \mathscr{C}(n, y) \to p(\mathscr{C}(n, y))$ is an isomorphism of crossed sets. Then X has the structure of $\mathscr{C}(n, y)$ given by (3.3). Now, $ny \in G$ must be such that $p(\mathscr{C}(n, y))$ generates G. Since the subgroup generated by $p(\mathscr{C}(n, y))$ is invariant, we know by the proof of Theorem 3.7 that it is either trivial or it contains N. It is trivial if $(n, y) \in Z(N \rtimes C)$, i.e., if $t = 1$ and y acts on N by conjugation by n^{-1}; thus we must exclude this case. This case excluded, y must generate C, and then we can take $x = y$ in the proof of Theorem 3.7, whence X is as in (3.4).

$(2 \Rightarrow 1)$ Similar. $\square$

We restate the previous results as: if X is a simple rack then either

(1) $|X| = p$ a prime, $X \simeq \mathbb{F}_p$ a permutation rack, $x \triangleright y = y + 1$.
(2) $|X| = p^t$, $X \simeq (\mathbb{F}_p^t, T)$ is affine, as in Corollary 3.10(1).
(3) $|X|$ is divisible by at least two different primes, and X is twisted homogeneous, as in Theorem 3.12.

Compare this with [J2, Theorem 7].

The simple crossed sets in (2) can be alternatively described as $(X, \triangleright^a)$ where $X \simeq \mathbb{F}_q$, $q = p^t$; $a \in \mathbb{F}_q$ generates $\mathbb{F}_q$ over $\mathbb{F}_p$ and $x \triangleright^a y = (1-a)x + ay$. It follows easily that $\mathrm{Aut}(X, \triangleright^a)$ is the semidirect product $\mathbb{F}_q \rtimes \mathbb{F}_q^\times$.

It is natural to ask how many different simple crossed sets with $q = p^t$ elements there are. This is a well-known elementary result. For, if $I(n)$ denotes the number of monic irreducible polynomials in $\mathbb{F}_p[X]$ with degree n, then $\sum_{d|n} dI(d) = p^n$. Thus

$$I(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d,$$

where μ is the Möbius function.

4. Cohomology

4.1. Abelian cohomology

Let $(X, \triangleright)$ be a rack. We define now a cohomology theory which contains all cohomology theories of racks known so far. We think that this cohomology can be computed by some cohomology theory in the category of modules over X.

For a sequence of elements $(x_1, x_2, \dots x_n) \in X^n$ we will denote

$$[x_1 \cdots x_n] = x_1 \triangleright (x_2 \triangleright (\cdots (x_{n-1} \triangleright x_n) \cdots)).$$

Notice that if $i < n$ then

$$[x_1 \cdots x_i] \triangleright [x_1 \cdots \hat{x}_i \cdots x_n] = [x_1 \cdots x_n].$$

Definition 4.1. Let $* \in X$ be a fixed element (which is important only in degrees 0 and 1). Let $\mathbb{Z}\{X\}$ be the rack algebra of X (see Definition 2.22) and let, for $n \geqslant 0$, $C_n(X) = \mathbb{Z}\{X\}X^n$, i.e., the free left $\mathbb{Z}\{X\}$-module with basis X^n $(X^0 = \{*\}$

is a singleton). Let $\partial = \partial_n : C_{n+1}(X) \to C_n(X)$ be the $\mathbb{Z}\{X\}$-linear map defined on the basis by

For $n \geqslant 1$:

$$\begin{aligned}
&\partial(x_1, \ldots, x_{n+1}) \\
&\quad = \sum_{i=1}^{n} (-1)^i \eta_{[x_1 \cdots x_i],[x_1 \cdots \hat{x}_i \cdots x_{n+1}]}(x_1, \ldots, \hat{x}_i, \ldots, x_{n+1}) \\
&\qquad - \sum_{i=1}^{n} (-1)^i (x_1, \ldots, x_{i-1}, x_i \triangleright x_{i+1}, \ldots, x_i \triangleright x_{n+1}) \\
&\qquad - (-1)^{n+1} \tau_{[x_1 \cdots x_n],[x_1 \cdots x_{n-1} x_{n+1}]}(x_1, \ldots, x_n).
\end{aligned}$$

For $n = 0$:

$$\partial(x) = -\tau_{*,*^{-1} \triangleright x} *. \tag{4.1}$$

Lemma 4.2. *$(C_\bullet(X), \partial)$ is a complex.*

Proof. We decompose $\partial_n = \sum_{i=1}^{n+1} (-1)^i \partial_n^i$, where

$$\begin{aligned}
\partial_n^i(x_1, \ldots, x_{n+1}) = {} & \eta_{[x_1 \cdots x_i],[x_1 \cdots \hat{x}_i \cdots x_{n+1}]}(x_1, \ldots, \hat{x}_i, \ldots, x_{n+1}) \\
& - (x_1, \ldots, x_{i-1}, x_i \triangleright x_{i+1}, \ldots, x_i \triangleright x_{n+1}) \quad \text{for } i \leqslant n
\end{aligned}$$

$$\partial_n^{n+1}(x_1, \ldots, x_{n+1}) = -\tau_{[x_1 \cdots x_n],[x_1 \cdots x_{n-1} x_{n+1}]}(x_1, \ldots, x_n) \quad \text{for } i = n+1 > 1,$$

$$\partial_0^1(x) = -\tau_{*,*^{-1} \triangleright x} * \quad \text{for } n = 0.$$

Then, it is straightforward to verify that

$$\partial_{n-1}^i \partial_n^j = \partial_{n-1}^{j-1} \partial_n^i \quad \text{for } 1 \leqslant i < j \leqslant n+1,$$

and thus

$$\begin{aligned}
\partial_{n-1}\partial_n &= \sum_{1 \leqslant i < j \leqslant n+1} (-1)^{i+j} \partial^i \partial^j + \sum_{1 \leqslant j \leqslant i \leqslant n} (-1)^{i+j} \partial^i \partial^j \\
&= \sum_{1 \leqslant i < j \leqslant n+1} (-1)^{i+j} \partial^{j-1} \partial^i + \sum_{1 \leqslant j \leqslant i \leqslant n} (-1)^{i+j} \partial^i \partial^j = 0. \qquad \square
\end{aligned}$$

We are now in position to define rack (co)homology.

Definition 4.3. Let X be a rack. Let $A = (A, \eta, \tau)$ be a left X-module and take $C^n(X, A) = \mathrm{Hom}_{\mathbb{Z}\{X\}}(C_n(X), A)$, and the differential $d = \partial^*$. By the lemma, this is a cochain complex. We define then

$$H^n(X,A) = H^n(C^\bullet(X,A)).$$

If A is a right X-module (i.e., a right $\mathbb{Z}\{X\}$-module), we define

$$C_n(X,A) = A \otimes_{\mathbb{Z}\{X\}} C_n(X) \quad \text{and} \quad H_n(X,A) = H_n(C_\bullet(X,A)).$$

Remark 4.4. Low degree cohomology can be interpreted in terms of extensions: a 2-cocycle is the same as a function $\kappa : X \times X \to A$ which satisfies (2.17); and two 2-cocycles are cohomologous if and only if they satisfy (2.18).

Remark 4.5. Let X be a quandle; replacing the rack algebra $\mathbb{Z}\{X\}$ by the quandle algebra $\mathbb{Z}(X)$ in Definition 4.1 one can define quandle cohomology theory that has as a particular case the *quandle cohomology* $H_Q^\bullet(X,A)$ in [CJKLS].

We consider now particular cases of this definition.

4.2. Cohomology with coefficients in an abelian group

Recall that $\mathbb{Z}\{X\}$ has an augmentation $\mathbb{Z}\{X\} \to \mathbb{Z}$ given by $\eta_{i,j} \mapsto 1$, $\tau_{i,j} \mapsto 0$. Then, any abelian group A becomes an X-module. The complexes $C_\bullet(X,A)$, $C^\bullet(X,A)$ coincide thus with previous complexes found in the literature (see for instance [CJKLS,FR,G1]). We recall them for later use:

$$C_n(X,A) = A \otimes_{\mathbb{Z}} \mathbb{Z}X^n, \quad C^n(X,A) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}X^n, A) \simeq \mathrm{Fun}(X^n, A)$$

$$\begin{aligned}\partial(a \otimes (x_1, \dots, x_{n+1})) = \sum_{i=1}^{n} (-1)^i (&a \otimes (x_1, \dots, \hat{x}_i, \dots, x_{n+1}) \\ &- a \otimes (x_1, \dots, x_{i-1}, x_i \triangleright x_{i+1}, \dots, x_i \triangleright x_{n+1}))\end{aligned}$$

$$\begin{aligned}df(x_1, \dots, x_{n+1}) = \sum_{i=1}^{n} (-1)^i (&f(x_1, \dots, \hat{x}_i, \dots, x_{n+1}) \\ &- f(x_1, \dots, x_{i-1}, x_i \triangleright x_{i+1}, \dots, x_i \triangleright x_{n+1})).\end{aligned} \tag{4.2}$$

Here, $\partial_0 : C_1(X,A) \to C_0(X,A)$ vanishes. Notice that $H^1(X,A) = A^{\pi_0(X)}$, where $\pi_0(X)$ is the set of $\mathrm{Inn}_\triangleright(X)$-orbits in X.

Example 4.6. Let $(X, \triangleright)$ be a crossed set, let A be an abelian group (denoted additively), and let f be a 2-cocycle with values in A. Let $B : X \times X \to \mathbb{S}_A$ be given by

$$B_{ij}(a) = a + f_{ij}, \quad i,j \in X, \ a \in A.$$

Then B is a constant rack cocycle (i.e., it satisfies (2.7)). It is a constant quandle cocycle (i.e., it satisfies (2.8)) iff $f_{ii} = 0\ \forall i \in X$. The definition of "quandle cocycle" is thus seen to be the same for these kind of extensions as that in [CJKLS]. The cocycle B_{ij} satisfies (2.9) iff $f_{ji} = 0$ whenever $i \triangleright j = j$ and $f_{ij} = 0$.

Lemma 4.7. *$H^2(X, G) \simeq \mathrm{Hom}(H_2(X, \mathbb{Z}), G)$ for any abelian group G.*

Proof. This follows from the "Universal Coefficient Theorem" since $H_1(X, \mathbb{Z})$ is free (cf. [CJKS, Proposition 3.4]). $\square$

Remark 4.8. Some second and third cohomology groups are computed in [LN]; some others in [Mo]. See [O] for tables of the computations done so far. In particular, we excerpt from [Mo] that $H^2(X, \mathbb{Z}) = \mathbb{Z}$ if $X = (\mathbb{Z}/p,\ \triangleright^q)$ where p is a prime and $1 \neq q \in (\mathbb{Z}/p)^\times$.

Lemma 4.9. *Let X be the disjoint sum of the indecomposable crossed sets Y and Z. Then $H^2(X, \mathbb{Z}) \simeq H^2(Y, \mathbb{Z}) \oplus H^2(Z, \mathbb{Z}) \oplus \mathbb{Z}^2$.*

Proof. Let $f \in Z^2(X, \mathbb{Z})$, i.e., $f_{j,k} + f_{i,j \triangleright k} = f_{i \triangleright j, i \triangleright k} + f_{i,k}\ \forall i,j,k \in X$. Then one has $f_{i,j \triangleright k} = f_{i,k} = f_{t \triangleright i,k}$ for all $i,t \in Y$, $j,k \in Z$, since the actions of Z on Y and viceversa are trivial. Therefore, $f_{i,k} = f_{t,j}$ for all $i,t \in Y$, $j,k \in Z$, being both Y and Z indecomposable. We conclude that $Z^2(X, \mathbb{Z}) \simeq Z^2(Y, \mathbb{Z}) \oplus Z^2(Z, \mathbb{Z}) \oplus \mathbb{Z}^2$. Now, if $g: X \to \mathbb{Z}$ then δg is really only a function on $(Y \times Y) \cup (Z \times Z)$, and the claim follows. $\square$

4.3. Restricted modules

Consider a restricted X-module A, see Definition 2.23. This is the same as a G_X-module, G_X the enveloping group of X. We get then the complex $(C^\bullet(X, A), d) \simeq (\mathrm{Fun}(X^\bullet, A), d)$, with

$$\begin{aligned} df(x_1, \dots, x_{n+1}) = &\sum_{i=1}^{n} (-1)^i [x_1 \cdots x_i] f(x_1, \dots, \hat{x}_i, \dots, x_{n+1}) \\ &- \sum_{i=1}^{n} (-1)^i f(x_1, \dots, x_{i-1}, x_i \triangleright x_{i+1}, \dots, x_i \triangleright x_{n+1}) \\ &- (-1)^{n+1} (1 - [x_1 \cdots x_{n+1}]) f(x_1, \dots, x_n). \end{aligned}$$

As a particular case, suppose that X is any quandle and (A, g) is an affine crossed set. Take $\Lambda = \mathbb{Z}[T, T^{-1}]$ the ring of Laurent polynomials. Then A becomes a Λ-module, and a fortiori a G_X module by $x \cdot a = Ta = g(a)\ \forall x \in X,\ a \in A$ (since for any quandle there is a unique algebra map $\mathbb{Z}G_X \to \Lambda$, $x \mapsto T$). Then $\eta_{i,j}$ acts by g and $\tau_{i,j}$ acts by $f = 1 - g$ on A. We get in this way the complex considered in [CES].

Lemma 4.10. *If X is a rack and A is an abelian group with trivial action then*

$$H^2(X,A) = H^1(G_X, \mathrm{Fun}(X,A)).$$

Here the space $\mathrm{Fun}(X,A)$ *of all functions from X to A is a trivial left G_X-module; the right action is given by* $(f \cdot x)(z) = f(x \triangleright z)$.

Proof (Sketch, see [EG]). Consider the map $\Phi : X \to G_X$, $x \mapsto x$. Let $f : G_X \to \mathrm{Fun}(X,A)$ and take $r(f) : X \times X \to A$, where $r(f)(x,y) = f(\Phi(x))(y)$. It is easy to see that this map gives a morphism $H^1(G_X, \mathrm{Fun}(X,A)) \to H^2(X,A)$. On the other hand, let $g \in Z^2(X,A)$. This gives a map $g' : X \to \mathrm{Fun}(X,A)$, $g'(x)(y) = g(x,y)$. Recall that for a right G_X-module M, a map $\pi : G_X \to M$ is a 1-cocycle iff the map $\hat{\pi} : G_X \to G_X \ltimes M$ given by $z \mapsto (z, \pi(z))$ is a homomorphism of groups. Denote $M = \mathrm{Fun}(X,A)$. We have a map $\xi_g : X \to G_X \ltimes M$ given by $\xi_g(x) = (x, g'(x))$. So we need to show that ξ_g extends to a homomorphism $G_X \to G_X \ltimes M$. But the group G_X is generated by X with relations $xy = (x \triangleright y)x$. Thus, we only need to check that the $\xi_g(x)$'s satisfy the same relations, and it is straightforward to see that this is equivalent to $dg = 0$. Now, it is easy to see that this map is the inverse of r. $\square$

4.4. Non-principal cohomology

Let $X = \bigsqcup_{i \in I} X_i$ be a decomposition of the rack X. It is possible then to decompose the complex $C_\bullet(X, \mathbb{Z})$ of (4.2) into a direct sum

$$C_n(X) = \bigoplus_{i \in I} C_n^i(X), \quad C_n^i(X) = \mathbb{Z}(X^{n-1} \times X_i) \simeq \mathbb{Z}X^{n-1} \otimes \mathbb{Z}X_i.$$

For each $i \in I$, let A_i be an abelian group. We denote by A_I this collection. Then we take $C^\bullet(X, A_I)$ the complex

$$C^\bullet(X, A_I) = \bigoplus_{i \in I} \mathrm{Hom}_{\mathbb{Z}}(C_n^i(X), A_i)$$

Notice that if $A = A_i$ $\forall i \in I$, then this complex is the same as $C^\bullet(X,A)$ in (4.2).

4.5. Non-abelian cohomology

Let $(X, \triangleright)$ be a rack and let Γ be a group. We define:

$$H^1(X, \Gamma) = Z^1(X, \Gamma) = \{\gamma : X \to \Gamma \mid \gamma_{i \triangleright j} = \gamma_j, \ \forall i,j \in X\}, \tag{4.3}$$

$$Z^2(X, \Gamma) = \{\beta : X \times X \to \Gamma \mid \beta_{i, j \triangleright k} \beta_{j,k} = \beta_{i \triangleright j, i \triangleright k} \beta_{i,k} \ \forall i,j,k \in X\}. \tag{4.4}$$

The elements of $Z^2(X, \Gamma)$ shall be called non-abelian 2-cocycles with coefficients in Γ. If $\beta, \tilde{\beta} : X \times X \to \Gamma$ we set $\beta \sim \tilde{\beta}$ if and only if there exists $\gamma : X \to \Gamma$

such that

$$\tilde{\beta}_{ij} = (\gamma_{i \triangleright j})^{-1} \beta_{ij} \gamma_j. \tag{4.5}$$

It is easy to see that $\sim$ is an equivalence relation, and that $Z^2(X, \Gamma)$ is stable under $\sim$. We define

$$H^2(X, \Gamma) = Z^2(X, \Gamma)/\sim. \tag{4.6}$$

Example 4.11. Let S be a non-empty set; then $H^2(X, \mathbb{S}_S)$ parameterizes isomorphism classes of constant extensions of X by S, as in Section 2.2.

Remark 4.12. Though obvious, we point out that $H^2(X, \mathbb{S}_S) = H^2(X, \mathbb{Z}_2)$ when S has only two elements.

4.6. Non-abelian non-principal cohomology

We combine the theory of non-principal cohomology in Section 4.4 with that of non-abelian cohomology: let $X = \bigsqcup_{i \in I} X_i$ be a decomposition of the rack X and for each $i \in I$ let Γ_i be a group. Let us denote Γ_I this collection. We consider

$$Z^2(X, \Gamma_I) = \Big\{ f = \bigsqcup_i f_i : X \times X_i \to \Gamma_i \,| \\ f_i(x, y \triangleright z) f_i(y, z) = f_i(x \triangleright y, x \triangleright z) f_i(x, z) \ \forall x, y \in X, \ z \in X_i \Big\}.$$

As usual, if $f, \tilde{f} \in Z^2(X, \Gamma_I)$, we say that $f \sim \tilde{f}$ iff $\exists g = \bigsqcup_i g_i : X_i \to \Gamma_i$ such that

$$\tilde{f}_i(x, y) = g_i(x \triangleright y)^{-1} f_i(x, y) g_i(y) \quad \forall x \in X, \ y \in X_i.$$

The importance of such a theory becomes apparent in Theorem 4.14.

Definition 4.13. For $i \in I$, let be given a positive integer n_i and a subgroup $\Gamma_i \subset \mathrm{GL}(\mathbb{C}, n_i)$. Let $f = \bigsqcup_i f_i : X \times X_i \to \Gamma_i$. Take $V = \bigoplus_{i \in I} X_i \times \mathbb{C}^{n_i}$ a vector space and consider the linear isomorphism

$$c^f : V \otimes V \to V \otimes V, \quad c^f((x, a) \otimes (y, b)) = (x \triangleright y, f_i(x, y)(b)) \otimes (x, a),$$

$x \in X_j$, $y \in X_i$, $a \in \mathbb{C}^{n_j}$, $b \in \mathbb{C}^{n_i}$.

Theorem 4.14. (1) *Let X, Γ_I, V, c^f be as in the definition. Then c^f satisfies the Braid Equation if and only if $f \in Z^2(X, \Gamma_I)$.*

(2) *Furthermore, if* $f \in Z^2(X, \Gamma_I)$, *then there exists a group* G *such that* V *is a Yetter–Drinfeld module over* G. *In particular, the braiding of* V *as an object in* ${}^G_G\mathcal{YD}$ *coincides with* c^f. *If* Γ_i *is finite* $\forall i \in I$ *and* X *is finite, then* G *can be chosen to be finite.*

(3) *Conversely, if* G *is a finite group and* $V \in {}^G_G\mathcal{YD}$, *then there exist* $X = \bigsqcup X_i$, *finite groups* Γ_I, $f \in Z^2(X, \Gamma_I)$ *such that* V *is given as in the definition and the braiding* $c \in \mathrm{Aut}(V \otimes V)$ *in the category* ${}^G_G\mathcal{YD}$ *coincides with* c^f. *Here,* X *can be chosen to be a crossed set.*

(4) *If* $f \sim \tilde{f}$ *and* (V, c^f), $(\tilde{V}, c^{\tilde{f}})$ *are the spaces associated to* $f, \tilde{f}$, *then they are isomorphic as braided vector spaces, i.e., there exists a linear isomorphism* $\gamma : \tilde{V} \to V$ *such that* $(\gamma \otimes \gamma)c^{\tilde{f}} = c^f(\gamma \otimes \gamma) : \tilde{V} \otimes \tilde{V} \to V \otimes V$.

Proof.

(1) Straightforward.
(2) It follows from [G2, 2.14]. The finiteness of G follows from the fact that the group $G \subset \mathrm{GL}(V)$ can be chosen to be the group generated by the maps $(y, b) \mapsto (x \triangleright y, f(x, y)b)$, which is contained in the product $\prod_{i \in I} G_i$, where $G_i = \mathbb{S}_{X_i} \times \Gamma_i$.
(3) It follows from the structure of the modules in ${}^G_G\mathcal{YD}$. Indeed, if $V = \oplus_i M(g_i, \rho_i)$ (see [G1] for the notation), $g_i \in G$, $G_i = \{xg_i = g_i x\}$ the centralizer of g_i, $\{h^i_1, \dots, h^i_{s_i}\}$ a set of representatives of left coclasses G/G_i, and $t^{iu}_{jv} \in G_u$ defined by $h^i_j g_i (h^i_j)^{-1} h^u_v = h^u_{v'} t^{iu}_{jv}$; then take $X = \bigsqcup_i X_i$, $X_i = \{h^i_1, \dots, h^i_{s_i}\}$, and $f(h^i_j, h^u_v) = \rho_u(t^{iu}_{jv})$.
(4) It is straightforward to verify that if $\tilde{f}_i(x, y) = g_i(x \triangleright y)^{-1} f_i(x, y) g_i(y)$ $\forall x \in X$, $y \in X_i$, then the map $(x, a) \mapsto (x, g_i(x)(a))$ $(x \in X_i)$ is an isomorphism of braided vector spaces. $\square$

Notice that any Yetter–Drinfeld module over a group algebra can be constructed by means of a crossed set, and one does not need the more general setting of quandles, nor racks for it. However, racks may give easier presentations than crossed sets for some braided vector spaces.

5. Braided vector spaces

We have seen that it is possible to build a braided vector space $(\mathbb{C}X, c^{\mathfrak{q}})$ from a rack $(X, \triangleright)$ and a 2-cocycle $\mathfrak{q}$, cf. Theorem 4.14 and [G1]. It turns out that the braided vector space does *not* determine the rack. We now present a systematic way of constructing examples of different racks, with suitable cocycles, giving rise to equivalent braided vector spaces. We consider affine modules over a rack X, that is extensions of the form $X \times_\kappa A$, where A is an abelian X-module; see Definition 2.26. If the cocycle $\mathfrak{q}$ is chosen in a convenient way, we can change the basis "à la Fourier" and obtain a braided vector space arising from a set-theoretical solution of the QYBE. This solution is in turn related to the braided vector space arising from the derived rack of the set-theoretical solution of the QYBE.

Section 5.1 is an exposition of the relevant facts about set-theoretical solutions needed in this paper. In Section 5.2 we discuss braided vector spaces arising from set-theoretical solutions. In Section 5.3 we present the general method and discuss several examples.

5.1. Set-theoretical solutions of the QYBE

There is a close relation between racks and set-theoretical solutions of the Yang–Baxter equation, or, equivalently, of the braid equation. It was already observed by Brieskorn [B] that racks provide solutions of the braid equation. On the other hand, certain set-theoretical solutions of the braid equation produce racks. This is proved in [LYZ1,So], which belong to a series of papers (see [EGS,ESS,LYZ2,LYZ3]) devoted to set-theoretical solutions of the braid equation and originated in a question by Drinfeld [Dr]. We give here the definitions necessary to us.

Let X be a non-empty set and let $S : X \times X \to X \times X$ be a bijection. We say that S is a *set-theoretical solution of the braid equation* if $(S \times \mathrm{id})(\mathrm{id} \times S)(S \times \mathrm{id}) = (\mathrm{id} \times S)(S \times \mathrm{id})(\mathrm{id} \times S)$. We shall briefly say that S is "a solution" or that (X, S) is a *braided set*. A trivial example of a solution is the transposition $\tau : X \times X \to X \times X$, $(x, y) \mapsto (y, x)$. It is well-known that S is a solution if and only if $R = \tau S : X \times X \to X \times X$ is a solution of the set-theoretical quantum Yang–Baxter equation. If (X, S) is a braided set, there is an action of the braid group $\mathbb{B}_n$ on X^n, the standard generators σ_i acting by $S_{i,i+1}$, which means, as usual, that S acts on the $i, i+1$ entries.

In particular, a finite braided set gives rise to a finite quotient of $\mathbb{B}_n$ for any n, namely the image of the group homomorphism $\rho^n : \mathbb{B}_n \to \mathbb{S}_{X^n}$ induced by the action.

Lemma 5.1. [B]. *Let X be a set and let $\triangleright : X \times X \to X$ be a function. Let*

$$c : X \times X \to X \times X, \quad c(i,j) = (i \triangleright j, i). \tag{5.1}$$

Then c is a solution if and only if $(X, \triangleright)$ is a rack.

Proof. It is easy to check that c is a bijection if and only if (1.1) holds, and that it satisfies the braid equation if and only if (1.2) holds. $\square$

Definition 5.2. Let X, $\tilde{X}$ be two non-empty sets and let $S : X \times X \to X \times X$, $\tilde{S} : \tilde{X} \times \tilde{X} \to \tilde{X} \times \tilde{X}$ be two bijections. We say that (X, S) and $(\tilde{X}, \tilde{S})$ are *equivalent* if there exists a family of bijections $T^n : X^n \to \tilde{X}^n$ such that $T^n S_{i,i+1} = \tilde{S}_{i,i+1} T^n$, for all $n \geqslant 2$, $1 \leqslant i \leqslant n-1$.

If (X,S) and $(\tilde{X},\tilde{S})$ are equivalent and (X,S) is a solution, then $(\tilde{X},\tilde{S})$ is also a solution and the T^n's intertwine the corresponding actions of the braid group $\mathbb{B}_n$.

Definition 5.3 ([ESS,LYZ1]). Let (X,S) be a solution and let $f,g : X \to \mathrm{Fun}(X,X)$ be given by

$$S(i,j) = (g_i(j), f_j(i)). \tag{5.2}$$

The solution (or the braided set) is *non-degenerate* if the images of f and g lie inside $\mathbb{S}_X$.

Proposition 5.4 ([So,LYZ1]). *Let S be a non-degenerate solution with the notation in* (5.2) *and define $\triangleright$ by*

$$i \triangleright j = f_i(g_{f_j^{-1}(i)}(j)). \tag{5.3}$$

(1) *One has*

$$f \text{ preserves } \triangleright, \text{ i.e. } f_i(j \triangleright k) = f_i(j) \triangleright f_i(k); \tag{5.4}$$

$$f_i f_j = f_{f_i(j)} f_{g_j(i)}, \quad \forall i,j \in X. \tag{5.5}$$

(2) *If c is given by* (5.1), *then c is a solution*; *we call it the* derived solution of S. *The solutions S and c are equivalent*, *and $(X, \triangleright)$ is a rack.*

(3) *Let $(X, \triangleright)$ be a rack and let $f : X \to \mathbb{S}_X$. We define $g : X \to \mathbb{S}_X$ by*

$$g_i(j) = f^{-1}_{f_j(i)}(f_j(i) \triangleright j). \tag{5.6}$$

Let $S : X \times X \to X \times X$ be given by (5.2). *Then S is a solution if and only if* (5.4), (5.5) *hold. If this happens*, *the solutions S and c are equivalent*, *and S is non-degenerate.*

Proof.

(1) It is not difficult.
(2) It is enough to show that S and c are equivalent; automatically, c is a solution and *a fortiori* $(X, \triangleright)$ is a rack. Let $T^n : X^n \to X^n$ be defined inductively by

$$T^2(i,j) = (f_j(i), j), \quad T^{n+1} = Q_n(T^n \times \mathrm{id}),$$

where $Q_n(i_1, \dots, i_{n+1}) = (f_{i_{n+1}}(i_1), \dots, f_{i_{n+1}}(i_n), i_{n+1})$. One verifies using (5.4) and (5.5) that $T^n S_{i,i+1} = c_{i,i+1} T^n$, as needed.
(3) Straightforward. $\square$

Note that (5.6) is equivalent to

$$g_{f_j^{-1}(h)}(j) = f_h^{-1}(h \triangleright j). \tag{5.7}$$

Remark 5.5. Let (X, S) be a non-degenerate solution and let $\triangleright$ be defined by (5.3). Then $(X, \triangleright)$ is a quandle if and only if

$$f_i^{-1}(i) = (g_{f_i^{-1}(i)}(i)), \quad \forall i \in X; \tag{5.8}$$

if this holds, it is a crossed set if and only if

$$f_i^{-1}(j) = (g_{f_j^{-1}(i)}(j)) \;\Rightarrow\; f_j^{-1}(i) = (g_{f_i^{-1}(j)}(i)) \quad \forall i,j \in X. \tag{5.9}$$

Let (X, S), $(\tilde{X}, \tilde{S})$ be two non-degenerate braided sets, with corresponding maps f, g, resp. $\tilde{f}$, $\tilde{g}$. A function $\varphi : X \to \tilde{X}$ is a morphism of braided sets if and only if

$$\tilde{g}_{\varphi(i)}\varphi(j) = \varphi g_i(j), \tag{5.10}$$

$$\tilde{f}_{\varphi(i)}\varphi(j) = \varphi f_i(j), \quad \forall i,j \in X. \tag{5.11}$$

It can be shown that φ is a morphism of braided sets if and only φ is a morphism of the associated racks and (5.11) holds. One may say that a non-degenerate braided set is *simple* if it admits no non-trivial projections. It follows that any solution associated to a simple crossed set is simple, but the converse is not true as the following example shows: take a set X with p elements, p a prime, and a cycle μ of length p. Then $S(i,j) = (\mu(j), \mu^{-1}(i))$ is simple but the associated rack is trivial.

Definition 5.6 ([ESS,SO]). Let (X, S) be a solution and let $S^2(i,j) = (G_i(j), F_j(i))$. The group G_X, resp. A_X, is the quotient of the free group generated by X by the relations $ij = g_i(j)f_j(i)$, resp. $f_j(i)j = F_j(i)f_j(i)$, for all $i,j \in X$.

If $(X, \triangleright)$ is a rack and c is the corresponding solution, then G_X is the group already defined in Definition 1.5, and coincides with A_X.

5.2. Braided vector spaces of set-theoretical type

We now describe how set-theoretical solutions of the QYBE plus a 2-cocycle give rise to braided vector spaces. We begin by the case of solutions arising from a rack.

Let $(X, \triangleright)$ be a rack and let $q \in Z^2(X, \mathbb{C}^\times)$; so that

$$q_{i,j\triangleright k}\, q_{j,k} = q_{i\triangleright j, i\triangleright k}\, q_{i,k} \quad \forall i,j,k \in X. \tag{5.12}$$

Then, by Theorem 4.14, the space $V = \mathbb{C}X$ has a structure of a Yetter–Drinfeld module over a group whose braiding is given by $c^q : \mathbb{C}X \otimes \mathbb{C}X \to \mathbb{C}X \otimes \mathbb{C}X$,

$$c^q(i \otimes j) = q_{i,j}\, i \triangleright j \otimes i, \quad i,j \in X.$$

Let $X = \{x_1, \dots, x_n\}$ be a set, let $S : X \times X \to X \times X$ be a bijection and let $F : X \times X \to \mathbb{C}^\times$ be a function. Let $\mathbb{C}X$ denote the vector space with basis X and define

$S^F : \mathbb{C}X \otimes \mathbb{C}X \to \mathbb{C}X \otimes \mathbb{C}X$ by

$$S^F(i \otimes j) = F_{i,j} S(i,j) = F_{i,j} g_i j \otimes f_j i, \quad i,j \in X, \tag{5.13}$$

where we use the notation in (5.2).

Lemma 5.7. (1) *S^F is a solution of the braid equation if and only if (X,S) a solution and*

$$F_{i,j} F_{f_j i,k} F_{g_i j, g_{f_j i} k} = F_{j,k} F_{i,g_j k} F_{f_{g_j k} i, f_k j}, \quad i,j,k \in X. \tag{5.14}$$

(2) *Assume that* (5.14) *holds. Then S^F is* rigid *if and only if S is non-degenerate.*

Proof.

(1) Straightforward.
(2) Rigidity is equivalent to $c^\flat : V^* \otimes V \to V \otimes V^*$ being an isomorphism, where

$$c^\flat = (\mathrm{ev}_V \otimes \mathrm{id}_{V \otimes V^*})(\mathrm{id}_{V^*} \otimes c \otimes \mathrm{id}_{V^*})(\mathrm{id}_{V^* \otimes V} \otimes \mathrm{ev}_V^*).$$

Assume for simplicity that $F = 1$. Let $(\delta_i)_{i \in X}$ be the basis of V^* dual to X. Then $c^\flat(\delta_i \otimes j) = \sum_{h : g_j(h) = i} f_h(j) \otimes h$. Hence, if $c^\flat$ is an isomorphism then g_j is bijective for all j, for $c^\flat(\delta_i \otimes j) = 0$ if i is not in the image of g_j. Now, if $f_h(j) = f_h(k)$ then $c^\flat(\delta_{g_j(h)} \otimes j) = c^\flat(\delta_{g_j(k)} \otimes j)$, which implies $j = k$.

Conversely, if S is non-degenerate then $c^\flat$ is an isomorphism with inverse $(c^\flat)^{-1}(r \otimes \delta_s) = \delta_{g_{f_s^{-1}(r)}(s)} \otimes f_s^{-1}(r)$. □

Definition 5.8. Let (X,S) be a non-degenerate solution and let $F : X \times X \to \mathbb{C}^\times$ be a function such that (5.14) holds. We say that the braided vector space $(\mathbb{C}X, S^F)$ is *of set-theoretical type*.

By results of Lyubashenko and others, a braided vector space $(\mathbb{C}X, c^F)$ of set-theoretical type can be realized as a Yetter–Drinfeld module over some Hopf algebra H. See for example [Tk].

Example 5.9. Let Γ be a finite group. Let $x \in \Gamma$, let $\mathcal{O}$ be the conjugacy class containing x and let $\rho : \Gamma_x \to \mathrm{Aut}\, W$ be a finite dimensional representation of Γ_x the centralizer of x. We choose a numeration $\{p_1 = x, p_2, \dots, p_r\}$ of $\mathcal{O}$ and fix elements $g_1, g_2, \dots, g_r$ in Γ such that $g_i x g_i^{-1} = p_i$. Then

$$M(x,\rho) := \mathrm{Ind}_{\Gamma_x}^{\Gamma} W \simeq \mathbb{C}\mathcal{O} \otimes W \simeq \bigoplus_{1 \leqslant i \leqslant r} g_i \otimes W$$

is a Yetter–Drinfeld module over $\mathbb{C}\Gamma$ with the coaction $\delta(g_i \otimes w) = p_i \otimes g_i \otimes w$, and the induced action; that is $h \cdot (g_i \otimes w) = g_j \otimes t \cdot w$, where j and $t \in \Gamma_x$ are uniquely determined by $hp_ih^{-1} = p_j$, $hg_i = g_jt$. In particular, given $i, k \in \{1, \dots, r\}$, let us denote by $j_{ik} \in \{1, \dots, r\}$, $t_{ik} \in \Gamma_x$ the elements uniquely determined by

$$p_kp_ip_k^{-1} = p_{j_{ik}}, \quad p_kg_i = g_{j_{ik}}t_{ik}. \tag{5.15}$$

We can then express the braiding in a compact way; write for simplicity $g_iw = g_i \otimes w$. If $u, w \in W$ and $i, k \in \{1, \dots, r\}$ then

$$c(g_kw \otimes g_iu) = g_{j_{ik}}t_{ik} \cdot u \otimes g_kw. \tag{5.16}$$

We know from Theorem 4.14 that this braided vector space can be presented with the crossed set $\{p_1, \dots, p_r\}$ and a non-abelian 2-cocycle with values in $\mathrm{GL}(W)$. We now show that under a suitable assumption we can present it with a (larger) rack and an abelian 2-cocycle with values in $\mathbb{C}^\times$: assume that there exists a basis $w_1, w_2, \dots, w_r$ of W such that

$$h \cdot w_s = \chi_s(h)w_{\sigma_h(s)}. \tag{5.17}$$

for some group homomorphism $\sigma : \Gamma_x \to \mathbb{S}_r$ and some map $\chi : \{1, \dots, r\} \times \Gamma_x \to \mathbb{C}^\times$ satisfying

$$\chi_s(th) = \chi_s(h)\chi_{\sigma_h(s)}(t), \quad 1 \leqslant s \leqslant r, \ t, h \in \Gamma_x.$$

Then

$$c(p_kw_q \otimes p_iw_s) = \chi_s(t_{ik})p_{j_{ik}}w_{\sigma_{p_k}(s)} \otimes p_kw_q. \tag{5.18}$$

That is, the braided vector space $(M(x, \rho), c)$ is of rack type.

We now introduce a relation between braided vector spaces weaker than isomorphism but useful enough to deal with Nichols algebras; for example braided vector spaces related by a twisting are t-equivalent as below.

Definition 5.10. We say that two braided vector spaces (V, c) and (W, d) are *t-equivalent* if there is a collection of linear isomorphisms $U^n : V^{\otimes n} \to W^{\otimes n}$ intertwining the corresponding representations of the braid group $\mathbb{B}_n$, for all $n \geqslant 2$. The collection $(U^n)_{n \geqslant 2}$ is called a *t-equivalence*.

Example 5.11. Let $(\mathbb{C}X, S^F)$ be a braided vector space of set-theoretical type (see (5.13)). Let (X, c) be the derived solution; define $q_{ij} = F_{f_j^{-1}(i),j}$. If

$$q_{f_ki, f_kj} = q_{ij} \quad \forall i, j, k \in X. \tag{5.19}$$

then the collection of maps $T^n : X^n \to X^n$ defined in the proof of Proposition 5.4 induce a t-equivalence between $(\mathbb{C}X, S^F)$ and $(\mathbb{C}X, c^q)$. Indeed, computing only the coefficients, we have

$$\operatorname{coeff}(T^n S^F_{h,h+1}(i_1 \otimes \cdots \otimes i_n)) = F_{i_h,i_{h+1}}$$

$$\operatorname{coeff}(c^q_{h,h+1} T^n(i_1 \otimes \cdots \otimes i_n)) = q_{f_{i_n} f_{i_{n-1}} \cdots f_{i_{h+1}} i_h, f_{i_n} f_{i_{n-1}} \cdots f_{i_{h+2}} i_{h+1}}$$

and the equality holds by (5.19).

5.3. Fourier transform

We consider a rack $(X, \triangleright)$, a finite abelian X-module A, a dynamical cocycle $\alpha : X \times X \to \mathrm{Fun}(A \times A, A)$, and a 2-cocycle $\mathfrak{q}$ on the rack $X \times_\alpha A$. Let $\hat{A}$ be the group of characters of A. We define a family of elements

$$(i, \psi) := \sum_{a \in A} \psi(a)(i, a) \in \mathbb{C}(X \times_\alpha A), \quad i \in X, \ \psi \in \hat{A}. \tag{5.20}$$

We want to know under which conditions there exists a family of scalars $F^{\psi,\phi}_{ij}$ such that

$$c^{\mathfrak{q}}((i, \psi) \otimes (j, \phi)) = F^{\psi,\phi}_{ij}(i \triangleright j, \vartheta) \otimes (i, \nu), \quad i, j \in X, \ \psi, \phi \in \hat{A}, \tag{5.21}$$

for some $\vartheta, \nu \in \hat{A}$. Our main result in this direction, and one of the main results in this paper, is Theorem 5.13 below.

In what follows, we shall assume that the extension $X \times_\alpha A$ is an affine module over X, cf. Definition 2.26. That is, α is given by

$$\alpha_{i,j}(a, b) = \eta_{i,j}(b) + \tau_{i,j}(a) + \kappa_{ij}, \tag{5.22}$$

where $\eta_{i,j} \in \mathrm{Aut}(A)$, $\tau_{i,j} \in \mathrm{End}(A)$ define the X-module structure on A, and $\kappa_{ij} \in A$. We denote $Y_\kappa := X \times_\kappa A$. We shall also write $\mathfrak{q}^{a,b}_{i,j} = \mathfrak{q}_{(i,a),(j,b)}$. We begin by the following result.

Lemma 5.12. *Let $\mathfrak{q}$ be given by*

$$\mathfrak{q}^{a,b}_{i,j} = \chi_{i,j}(b)\mu_{i,j}(a)q_{ij}, \tag{5.23}$$

where $\chi_{i,j}, \mu_{i,j} \in \hat{A}$, $q_{ij} \in \mathbb{C}^\times$. Then $\mathfrak{q}$ is a 2-cocycle if and only if

$$\chi_{i,j \triangleright k}(\kappa_{j,k}) q_{i,j \triangleright k} q_{j,k} = \chi_{i \triangleright j, i \triangleright k}(\kappa_{i,k}) \mu_{i \triangleright j, i \triangleright k}(\kappa_{i,j}) q_{i \triangleright j, i \triangleright k} q_{i,k}, \tag{5.24}$$

$$\chi_{i,j \triangleright k}(\eta_{j,k}(a)) \chi_{j,k}(a) = \chi_{i \triangleright j, i \triangleright k}(\eta_{i,k}(a)) \chi_{i,k}(a), \tag{5.25}$$

$$\mu_{i,j\triangleright k}(a) = \chi_{i\triangleright j,i\triangleright k}(\tau_{i,k}(a))\mu_{i\triangleright j,i\triangleright k}(\tau_{i,j}(a))\mu_{i,k}(a), \tag{5.26}$$

$$\mu_{i\triangleright j,i\triangleright k}(\eta_{i,j}(a)) = \chi_{i,j\triangleright k}(\tau_{j,k}(a))\mu_{j,k}(a). \tag{5.27}$$

for all $i,j,k\in X$, $a\in A$.

Proof. Writing explicitly down the cocycle condition on $\mathfrak{q}$, one gets an equality of functions from $A\times A\times A$ to $\mathbb{C}$. Specialization at $(0,0,0)$ implies (5.24); then, specialization at $(a,0,0)$, $(0,a,0)$, $(0,0,a)$ implies the other conditions. The converse is similar. $\square$

Theorem 5.13. *If the* 2*-cocycle* $\mathfrak{q}$ *is given by* (5.23) *with* $\chi_{i,j},\mu_{i,j}\in\hat{A}$, $q_{ij}\in\mathbb{C}^\times$, *then*

$$c^{\mathfrak{q}}((i,\psi)\otimes(j,\phi)) = F_{ij}^{\psi,\phi}(i\triangleright j,\vartheta)\otimes(i,v), \tag{5.28}$$

for all $i,j\in X$, $\psi,\phi\in\hat{A}$, *where*

$$F_{ij}^{\psi,\phi} = q_{ij}\phi(\tilde{\kappa}_{ij})^{-1}\chi_{i,j}(\tilde{\kappa}_{ij})^{-1}, \tag{5.29}$$

$$\vartheta = (\phi\chi_{i,j})\circ\eta_{i,j}^{-1}, \tag{5.30}$$

$$v = \psi\mu_{i,j}((\phi\chi_{i,j})\circ\tilde{\tau}_{i,j})^{-1}. \tag{5.31}$$

Here $\tilde{\tau}_{i,j}(a) = \eta_{i,j}^{-1}(\tau_{i,j}(a))$, $\tilde{\kappa}_{ij} = \eta_{i,j}^{-1}(\kappa_{ij})$.

Proof. We compute

$$\begin{aligned}
&c^{\mathfrak{q}}((i,\psi)\otimes(j,\phi))\\
&\quad=\sum_{a,b\in A}\psi(a)\phi(b)\mathfrak{q}_{i,j}^{a,b}(i\triangleright j,\eta_{i,j}(b)+\tau_{i,j}(a)+\kappa_{ij})\otimes(i,a)\\
&\quad=\sum_{a,c\in A}\psi(a)\phi(\eta_{i,j}^{-1}(c)-\tilde{\tau}_{i,j}(a)-\tilde{\kappa}_{ij})\mathfrak{q}_{i,j}^{a,\eta_{i,j}^{-1}(c)-\tilde{\tau}_{i,j}(a)-\tilde{\kappa}_{ij}}(i\triangleright j,c)\otimes(i,a)\\
&\quad=\sum_{a,c\in A}q_{ij}\phi(\tilde{\kappa}_{ij})^{-1}\chi_{i,j}(\tilde{\kappa}_{ij})^{-1}\quad\psi(a)\phi(\tilde{\tau}_{i,j}(a))^{-1}\mu_{i,j}(a)\chi_{i,j}(\tilde{\tau}_{i,j}(a))^{-1}\\
&\qquad\times\phi(\eta_{i,j}^{-1}(c))\chi_{i,j}(\eta_{i,j}^{-1}(c))(i\triangleright j,c)\otimes(i,a);
\end{aligned}$$

where in the first equality we use (5.22); in the second, we perform the change of variables $c=\eta_{i,j}(b)+\tau_{i,j}(a)+\kappa_{ij}$ which gives

$$b=\eta_{i,j}^{-1}(c-\tau_{i,j}(a)-\kappa_{ij})=\eta_{i,j}^{-1}(c)-\tilde{\tau}_{i,j}(a)-\tilde{\kappa}_{ij};$$

in the third equality we use (5.23) and that ϕ and χ_{ij} are multiplicative. The claim follows. $\square$

Remark 5.14. The derived rack of the braided set underlying (5.28) is given by

$$(i,\psi) \triangleright (j,\phi) = (i \triangleright j, [(\phi\chi_{ij}) \circ \eta_{ij}^{-1}][(\psi\chi_{i\triangleright j,i}) \circ \tilde{\tau}_{i\triangleright j,i}]^{-1}\mu_{i\triangleright j,i}).$$

Note that it *does not* depend on (κ_{ij}) but only on the cocycle $\mathfrak{q}$.

Example 5.15. Assume that X is trivial.

(1) $\mathfrak{q}$ given by (5.23) is a cocycle if and only if:

$$\chi_{i,k}(\kappa_{j,k}) = \chi_{j,k}(\kappa_{i,k})\mu_{j,k}(\kappa_{i,j}), \tag{5.32}$$

$$\chi_{i,k}(\eta_{j,k}(s))\chi_{j,k}(s) = \chi_{j,k}(\eta_{i,k}(s))\chi_{i,k}(s), \tag{5.33}$$

$$1 = \chi_{j,k}(\tau_{i,k}(s))\mu_{j,k}(\tau_{i,j}(s)), \tag{5.34}$$

$$\mu_{j,k}(\eta_{i,j}(s)) = \chi_{i,k}(\tau_{j,k}(s))\mu_{j,k}(s), \tag{5.35}$$

for any $i,j,k \in X$, $s \in A$.

(2) Let $\sigma : X \to A$ be any function; define $\kappa_{ij} := \sigma_i - \sigma_j$, and

$$\alpha_{i,j}(a,b) = b + \kappa_{ij}, \tag{5.36}$$

that is $\eta_{ij} = \mathrm{id}$, $\tau_{ij} = 0$ in (5.22). Then α is a non-trivial cocycle, provided that σ is not constant; we shall assume this in the rest of the example and in Lemma 5.16 below.

(3) Furthermore, let $q_{ij} \in \mathbb{C}^\times$ and let $\omega : X \to \hat{A}$ be any function; define $\chi_{i,j} := \omega_j =: \mu_{i,j}^{-1}$, and define $\mathfrak{q}$ by (5.23). We claim that $\mathfrak{q}$ is a cocycle. Conditions (5.33), (5.34) and (5.35) follow because $\eta_{ij} = \mathrm{id}$ and $\tau_{ij} = 0$; condition (5.32) follows from the special definition of κ_{ij}.

Then we can apply Theorem 5.13. We have

$$c^{\mathfrak{q}}((i,\psi) \otimes (j,\phi)) = q_{ij}(\phi\omega_j)(\sigma_j)(\phi\omega_j)(\sigma_i)^{-1}(j,\phi\omega_j) \otimes (i,\psi\omega_j^{-1}), \tag{5.37}$$

for all $i,j \in X$, $\psi,\phi \in \hat{A}$. In other words, we consider the solution $(X \times \hat{A}, S)$ where

$$S((i,\psi),(j,\phi)) = ((j,\phi\omega_j),(i,\psi\omega_j^{-1})), \tag{5.38}$$

the cocycle $F_{ij}^{\psi,\phi} = q_{ij}(\phi\omega_j)(\sigma_j)(\phi\omega_j)(\sigma_i)^{-1}$, and the corresponding braided vector space $(\mathbb{C}(X \times \hat{A}), S^F)$. The associated rack is

$$(i,\psi) \triangleright (j,\phi) = (j, \phi\omega_j\omega_i^{-1}).$$

(4) Assume now that $\omega_i = \omega \in \hat{A}$, for all i. Hence the associated rack is trivial. Let

$$Q_{ij}^{\psi,\phi} = q_{ij}\phi(\sigma_j)\phi(\sigma_i)^{-1}$$

and let $(\mathbb{C}(X \times \hat{A}), c^Q)$ be the associated braided vector space. Let $T^n : (X \times \hat{A})^n \to (X \times \hat{A})^n$ be as in the proof of Proposition 5.4. In our case, we have

$$T^n((i_1, \psi_1), \dots, (i_j, \psi_j), \dots, (i_n, \psi_n)) = ((i_1, \psi_1\omega^{1-n}), \dots, (i_j, \psi_j\omega^{j-n}), \dots, (i_n, \psi_n)).$$

Lemma 5.16. *The braided vector spaces $(\mathbb{C}(X \times \hat{A}), S^F)$ and $(\mathbb{C}(X \times \hat{A}), c^Q)$ are t-equivalent.*

Proof. Let p_h be defined inductively by $p_1 = 1$, $p_{h+1} = p_h + n - h$, and let

$$\lambda_{i_1,\dots,i_n} = \prod_{1 \leqslant h \leqslant n} \omega^{p_h}(\sigma_{i_h}).$$

We shall show that the map $U^n : \mathbb{C}(X \times \hat{A})^{\otimes n} \to \mathbb{C}(X \times \hat{A})^{\otimes n}$, $U^n((i_1, \psi_1) \otimes \cdots \otimes (i_n, \psi_n)) = \lambda_{i_1,\dots,i_n} T^n((i_1, \psi_1) \otimes \cdots \otimes (i_n, \psi_n))$, satisfies $U^n S^F_{j,j+1} = c^Q_{j,j+1} U^n$; that is, U^n intertwines the corresponding representations of the braid group.

On one hand,

$$\begin{aligned}
&U^n S^F_{j,j+1}((i_1, \psi_1) \otimes \cdots \otimes (i_n, \psi_n)) \\
&\quad = q_{i_j i_{j+1}} (\psi_{j+1}\omega)(\sigma_{i_{j+1}})(\psi_{j+1}\omega)(\sigma_{i_j})^{-1} \\
&\qquad \times U^n((i_1, \psi_1\omega^{1-n}) \otimes \cdots \otimes (i_{j+1}, \psi_{j+1}\omega) \otimes (i_j, \psi_j\omega^{-1}) \otimes \cdots \otimes (i_n, \psi_n)) \\
&\quad = q_{i_j i_{j+1}} (\psi_{j+1}\omega)(\sigma_{i_{j+1}})(\psi_{j+1}\omega)(\sigma_{i_j})^{-1} \lambda_{i_1,\dots,i_{j+1},i_j,\dots,i_n} \\
&\qquad \times ((i_1, \psi_1\omega^{1-n}) \otimes \cdots \otimes (i_{j+1}, \psi_{j+1}\omega^{j+1-n}) \otimes (i_j, \psi_j\omega^{j-n}) \otimes \cdots \otimes (i_n, \psi_n));
\end{aligned}$$

whereas, on the other hand,

$$\begin{aligned}
&c^Q_{j,j+1} U^n((i_1, \psi_1) \otimes \cdots \otimes (i_n, \psi_n)) \\
&\quad = \lambda_{i_1,\dots,i_n} c^Q_{j,j+1}((i_1, \psi_1\omega^{1-n}) \otimes \cdots \otimes (i_j, \psi_j\omega^{j-n}) \otimes (i_{j+1}, \psi_{j+1}\omega^{j+1-n}) \otimes \cdots \otimes (i_n, \psi_n)) \\
&\quad = \lambda_{i_1,\dots,i_n} q_{i_j i_{j+1}} \psi_{j+1}\omega^{j+1-n}(\sigma_{i_{j+1}}) \psi_{j+1}\omega^{j+1-n}(\sigma_{i_j})^{-1} \\
&\quad \times ((i_1, \psi_1\omega^{1-n}) \otimes \cdots \otimes (i_{j+1}, \psi_{j+1}\omega^{j+1-n}) \otimes (i_j, \psi_j\omega^{j-n}) \otimes \cdots \otimes (i_n, \psi_n)).
\end{aligned}$$

The equality holds since

$$\omega(\sigma_{i_{j+1}})\omega(\sigma_{i_j})^{-1}\omega^{p_j}(\sigma_{i_{j+1}})\omega^{p_{j+1}}(\sigma_{i_j}) = \omega^{p_j}(\sigma_{i_j})\omega^{p_{j+1}}(\sigma_{i_{j+1}})\omega^{j+1-n}(\sigma_{i_{j+1}})\omega^{-j-1+n}(\sigma_{i_j}),$$

by definition of the p_h's. □

Example 5.17. Assume that $\eta_{ij} = \mathrm{id}$ for all $i, j \in X$.

(1) A family (τ_{ij}) defines a quandle structure of X-module on A if and only if $\tau_{ii} = 0$, $\tau_{j,k} = \tau_{i \triangleright j, i \triangleright k}$ and

$$\tau_{i, j \triangleright k} = \tau_{i,k} + \tau_{i,j}\tau_{j,k}, \tag{5.39}$$

for all $i, j, k \in X$. Given such a family, (κ_{ij}) is a 2-cocycle if and only if

$$\kappa_{j,k} + \kappa_{i, j \triangleright k} = \kappa_{i,k} + \tau_{j,k}(\kappa_{i,j}) + \kappa_{i \triangleright j, i \triangleright k}, \tag{5.40}$$

(2) We shall consider the following family of examples: $X = (\mathbb{Z}/3, \triangleright^2)$ is the unique simple crossed set with three elements; A is a finite abelian group of exponent 2; $\tau_{ij} = \mathrm{id} - \delta_{ij}$, $i, j \in X$. It is not difficult to verify that (τ_{ij}) satisfies the conditions in (1). We fix $a \in A$, and set

$$\kappa_{ij} = (1 - \delta_{ij})a, \quad \tilde{\kappa}_{ij} = \delta_{i,j+1}a,$$

$i, j \in X$. Both families (κ_{ij}) and $(\tilde{\kappa}_{ij})$ satisfy (5.40); we denote the corresponding extensions by $Y = X \times_\kappa A$, $\tilde{Y} = X \times_{\tilde{\kappa}} A$. We shall assume that $a \neq 0$. Indeed, $Y = X \times_\kappa A$ (for $a \neq 0$) is isomorphic to $Y = X \times_0 A$ (case $a = 0$); just consider the function $f : X \to A, f(i) = a$ for all i, and check that κ is cohomologous to 0, cf. (2.18).

Analogously, we denote $\hat{Y} = X \times_0 \hat{A}$.

(3) If $A = \mathbb{Z}/2$, $a = 1$, Y is isomorphic to the crossed set of transpositions in $\mathbb{S}_4$, via the identification

$$(12) = (0,0), \quad (34) = (0,1), \quad (13) = (1,0),$$

$$(24) = (1,1), \quad (14) = (2,0), \quad (23) = (2,1).$$

Furthermore, $\tilde{Y}$ is isomorphic to the crossed set of 4-cycles in $\mathbb{S}_4$ (that is, the faces of the cube), via the identification

$$(1234) = (0,0), \quad (1324) = (1,0), \quad (1243) = (2,0),$$

$$(1432) = (0,1), \quad (1423) = (1,1), \quad (1342) = (2,1).$$

The crossed sets Y and $\tilde{Y}$ are not isomorphic.

(4) We consider now the cocycle $\mathfrak{q}_{ij}^{ab} = q_{ij} \in \mathbb{C}^\times$; that is $\chi_{i,j} = \mu_{i,j} = \varepsilon$, for all i,j, in (5.23). By Theorem 5.13, we have in the braided vector spaces $(\mathbb{C}Y, c^{\mathfrak{q}})$ and $(\mathbb{C}\tilde{Y}, \tilde{c}^{\mathfrak{q}})$ the equalities

$$c^{\mathfrak{q}}((i,\psi)\otimes(j,\phi)) = q_{ij}\phi((1-\delta_{ij})a)(i\triangleright j,\phi)\otimes(i,\psi\phi^{1-\delta_{ij}}),$$

$$\tilde{c}^{\mathfrak{q}}((i,\psi)\otimes(j,\phi)) = q_{ij}\phi((\delta_{i,j+1})a)(i\triangleright j,\phi)\otimes(i,\psi\phi^{1-\delta_{ij}}),$$

for all $i,j\in X$, $\psi,\phi\in\hat{A}$. That is, we have isomorphisms with braided vector spaces $(\mathbb{C}(X\times\hat{A}), S^F)$, respectively $(\mathbb{C}(X\times\hat{A}), \tilde{S}^F)$. In both cases, the associated rack is given by $(i,\psi)\triangleright(j,\phi) = (i\triangleright j, \phi\psi^{1-\delta_{ij}})$; this is the crossed set $\hat{Y}$. Let $Q_{ij}^{\psi\phi} = q_{ij}$.

Lemma 5.18. (1) *The braided vector spaces* $(\mathbb{C}Y, c^{\mathfrak{q}})$ *and* $(\mathbb{C}\hat{Y}, c^Q)$ *are t-equivalent.*

(2) *The braided vector spaces* $(\mathbb{C}\tilde{Y}, \tilde{c}^{\mathfrak{q}})$ *and* $(\mathbb{C}\hat{Y}, c^Q)$ *are t-equivalent.*

(3) *The braided vector spaces* $(\mathbb{C}Y, c^{\mathfrak{q}})$ *and* $(\mathbb{C}\tilde{Y}, \tilde{c}^{\mathfrak{q}})$ *are t-equivalent.*

Proof

(1) By Theorem 5.13, it is enough to show that the map

$$U^n : \mathbb{C}(X\times\hat{A})^{\otimes n} \to \mathbb{C}(X\times\hat{A})^{\otimes n},$$

$$U^n((i_1,\psi_1)\otimes\cdots\otimes(i_n,\psi_n)) = (\psi_1\cdots\psi_n)(a)\, T^n((i_1,\psi_1)\otimes\cdots\otimes(i_n,\psi_n)),$$

satisfies $U^n S_{j,j+1}^F = c_{j,j+1}^Q U^n$. This is a straightforward computation.

(2) Let Γ_n be the image of the group homomorphism $\rho^n : \mathbb{B}_n \to \mathbb{S}_{X^n}$ induced by the rack structure on X. Let $\Lambda_n \coloneqq \sum_{g\in\Gamma_n} g$ be a non-normalized integral of the Hopf algebra $\mathbb{C}\Gamma_n$. The group Γ_n acts on the vector space $\mathrm{Fun}(X^n, \mathbb{C}X)$ in the usual way; let $\eta^n = \Lambda_n \cdot \delta_1$ where δ_1 is the function $\delta_1(i_1,\dots,i_n) = i_1$. We write

$$\eta^n = \sum_{k\in K^n} \eta_k^n,$$

where η_k^n is actually a function from X^n to X and K^n is an index set. Let

$$R_1^n(i_1,\dots,i_n) = \left(\sum_{k\in K^{n-1}} \delta_{i_1\triangleright\eta_k^n(i_2,\dots,i_n),\, i_1+1}\right)a,$$

$$R_t^n(i_1,\dots,i_n) = R_1^n(i_t, i_t\triangleright i_1, i_t\triangleright i_2,\dots,i_t\triangleright i_{t-1}, i_{t+1},\dots,i_n),\quad t\geqslant 2.$$

We consider the map $U^n : \mathbb{C}(X\times\hat{A})^{\otimes n} \to \mathbb{C}(X\times\hat{A})^{\otimes n}$,

$$U^n((i_1,\psi_1)\otimes\cdots\otimes(i_n,\psi_n)) = \psi_1(R_1^n)\cdots\psi_n(R_n^n)T^n((i_1,\psi_1)\otimes\cdots\otimes(i_n,\psi_n)).$$

By Theorem 5.13, it is enough to show that U_n satisfies $U^n S^F_{j,j+1} = c^Q_{j,j+1} U^n$. A straightforward computation shows that this is equivalent to the following set of identities:

$$R^n_t(i_1, \dots, i_n) = R^n_t(i_1, \dots, i_h \triangleright i_{h+1}, i_h, \dots, i_n), \quad h \neq t, t+1; \tag{5.41}$$

$$R^n_t(i_1, \dots, i_n) = R^n_{t+1}(i_1, \dots, i_t \triangleright i_{t+1}, i_t, \dots, i_n); \tag{5.42}$$

$$\begin{aligned} R^n_t(i_1, \dots, i_n) = {} & \delta_{i_t, i_{t+1}+1} a + R^n_{t-1}(i_1, \dots, i_{t-1} \triangleright i_t, i_{t-1}, \dots, i_n) \\ & + (1 - \delta_{i_t, i_{t-1}}) R^n_t(i_1, \dots, i_{t-1} \triangleright i_t, i_{t-1}, \dots, i_n). \end{aligned} \tag{5.43}$$

Now, Eq. (5.41) for $t = 1$ follows from the invariance of the integral, whereas for $t > 1$ follows from the definition and the case $t = 1$. Clearly, (5.42) follows from the definition also. Finally, (5.43) can be shown by induction on n and t.

(3) follows from (1) and (2). □

6. Nichols algebras and pointed Hopf algebras

6.1. *Definitions and tools*

The Nichols algebra of a rigid braided vector space (V, c) can be defined in various different ways, see for example [AG,AS2]. We retain the following one. If we consider the symmetric group $\mathbb{S}_n$ and the braid group $\mathbb{B}_n$ with standard generators $\{\tau_1, \dots, \tau_{n-1}\}$ and $\{\sigma_1, \dots, \sigma_{n-1}\}$, respectively, then the so-called Matsumoto section for the canonical projection $\mathbb{B}_n \to \mathbb{S}_n$, $\sigma_i \mapsto \tau_i$, is the set-theoretical function defined on $x \in \mathbb{S}_n$ by the recipe (i) write $x = \tau_{i_1} \cdots \tau_{i_l}$ in a shortest possible way, and (ii) replace the τ_i's by σ_i's, i.e., $M(x) = \sigma_{i_1} \cdots \sigma_{i_l}$. Then,

$$\mathfrak{B}(V) = \bigoplus_{n \geqslant 0} \mathfrak{B}^n(V) = \mathbb{C} \oplus V \oplus \left(\bigoplus_{n \geqslant 2} T^n(V) / \ker Q_n \right),$$

where $Q_n = \sum_{x \in \mathbb{S}_n} M(x)$ is the so-called "quantum symmetrizer". This presentation of the Nichols algebra immediately implies:

Lemma 6.1. *If* (V, c) *and* $(\tilde{V}, \tilde{c})$ *are t-equivalent braided vector spaces* (*cf. Definition* 5.10) *then the corresponding Nichols algebras* $\mathfrak{B}(V)$ *and* $\mathfrak{B}(\tilde{V})$ *are isomorphic as graded vector spaces. In particular, one has finite dimension, resp. finite GK-dimension, if and only if the other one has.*

Proof. Easy. □

For a subspace $J \subseteq T(V)$ we say that it is *compatible with the braiding* if $c(V \otimes J) = J \otimes V$ and $c(J \otimes V) = V \otimes J$.

Lemma 6.2. *Let $(X, \triangleright)$ be a rack, let $q \in \mathbb{C}^\times$ and let $\mathfrak{q} \equiv q$ be the cocycle $\mathfrak{q}_{ij} = q$ $\forall i, j \in X$. Let $(V = \mathbb{C}X, c^{\mathfrak{q}})$ be the associated braided space and let $J \subseteq T(V)$ be a subspace. Notice that $T(V)$ is an $\mathrm{Inn}_\triangleright(X)$-comodule algebra with the structure induced by $V \to \mathbb{C}\mathrm{Inn}_\triangleright(X) \otimes V$, $x \mapsto \phi_x \otimes x$ for $x \in X$. Furthermore, $T(V)$ is an $\mathrm{Inn}_\triangleright(X)$-module algebra via $\triangleright$. If J is $\mathrm{Inn}_\triangleright(X)$-homogeneous and $\mathrm{Inn}_\triangleright(X)$-stable, then it is compatible with the braiding.*

Proof. It is sufficient to prove that for $x \in X$ we have $c(J \otimes \mathbb{C}x) \subseteq V \otimes J$ and $c(\mathbb{C}x \otimes J) \subseteq J \otimes \mathbb{C}x$. The first inclusion is a consequence of the homogeneity of J, the second one is a consequence of the stability of J. $\square$

Finite-dimensional Nichols algebras (as well as any finite-dimensional graded rigid braided Hopf algebra) satisfy a Poincaré duality: let n be the degree of the space of integrals (it is easy to see that the space of integrals is homogeneous with respect to the $\mathbb{Z}$-grading), then $\dim \mathfrak{B}^r(V) = \dim \mathfrak{B}^{n-r}(V)$ for all $r \in \mathbb{Z}$. Furthermore, since $\mathfrak{B}(V)$ is concentrated in positive degrees, we have that $\mathfrak{B}^m(V) = 0$ for $m > n$; since $\dim \mathfrak{B}^0(V) = 1$ we have that $\dim \mathfrak{B}^n(V) = 1$; since $\mathfrak{B}(V)$ is generated by $\mathfrak{B}^1(V)$, we have that $\dim \mathfrak{B}^r(V) \neq 0$ for $0 \leqslant r \leqslant n$. We call n the *top degree of* $\mathfrak{B}(V)$. Choose then a non-zero integral $\int$. There is a non-degenerate bilinear pairing (which is the same as that in the proof of the Poincaré duality) given by $(x|y) = \lambda$ if $xy = \lambda \int +$ terms of degree $< n$. These facts, first encountered by Nichols [N], give a powerful strategy for computing Nichols algebras. We state this strategy after the following definition.

Definition 6.3. For $r \geqslant 2$, let J_r be the ideal generated by $\oplus_{i=2}^r \ker(Q_i)$. Let $\hat{\mathfrak{B}}_r(V) = T(V)/J_r$, which has a projection $\hat{\mathfrak{B}}_r \to \mathfrak{B}(V)$. It is not difficult to see that $\oplus_{i=2}^r \ker(Q_i)$ is a coideal which is compatible with the braiding, whence $\hat{\mathfrak{B}}_r(V)$ is a braided Hopf algebra. Moreover, it is graded, it is generated by its elements in degree 1, and in degree 0 it is 1-dimensional. Then it fulfills the same properties above about Poincaré duality as $\mathfrak{B}(V)$.

Theorem 6.4. (1) *Suppose that $\hat{\mathfrak{B}}_r(V)$ vanishes in degree $2r+1$. Then $\hat{\mathfrak{B}}_r(V) = \mathfrak{B}(V)$.*

(2) *Let $J \subseteq \ker(T(V) \to \mathfrak{B}(V))$ be an ideal which is also a coideal and is compatible with the braiding. Suppose that $T(V)/J$ is finite dimensional, it has top degree n and* $\dim \mathfrak{B}^n(V) \neq 0$. *Then $T(V)/J = \mathfrak{B}(V)$.*

(3) *Suppose that $\hat{\mathfrak{B}}_r(V)$ is finite dimensional, it has top degree n and* $\dim \mathfrak{B}^n(V) \neq 0$. *Then $\hat{\mathfrak{B}}_r(V) = \mathfrak{B}(V)$.*

Proof.

(1) Follows from Poincaré duality: $\dim \hat{\mathfrak{B}}_r^i(V) = \dim \mathfrak{B}^i(V)$ for $0 \leqslant i \leqslant r$ and the top degree of $\mathfrak{B}(V)$ is $\leqslant 2r$.
(2) This is so thanks to the non-degenerate bilinear form of $T(V)/J$: let $\int$ be an integral in $T(V)/J$. If $0 \neq x \in \ker(T(V)/J \to \mathfrak{B}(V))$, then there exists $y \in T(V)/J$

such that $xy = \int$. But then $\int \in \ker(T(V)/J \to \mathfrak{B}(V))$, which implies that $\operatorname{Im}(T^n(V)/J \to \mathfrak{B}(V)) = 0$, a contradiction.

(3) follows from (2). $\square$

In the examples we present in Sections 6.3 and 6.5, we have computed the quotients $T(V)/J$ finding Gröbner bases, with the help of [Opal]. We also used a program in Maple with subroutines in C to find the dimensions of the ideals J_r in degree r for small r's. Generators of J_r have been found by hand, using differential operators (see below). Thus, we have used part (1) of the Theorem. However, we shall use part (2) in the proofs.

The best way to prove that certain elements vanish (or not) in a Nichols algebra is given by the differential operators $\partial_{x^*} : \mathfrak{B}^n(V) \to \mathfrak{B}^{n-1}(V)$ ($x^* \in V^*$). These are skew derivations. When $V = \mathbb{C}X$ is given by a rack, we consider the basis $\{x \in X\}$ of V and $\{x^*\}$ its dual basis; we extend x^* to $\mathfrak{B}(V)$ by $x^*(\alpha) = 0$ if $\alpha \in \mathfrak{B}^n(V)$, $n \neq 1$. We put then $\partial_x = \partial_{x^*} = (\mathrm{id} \otimes x^*) \circ \Delta$ (here Δ is the comultiplication in $\mathfrak{B}(V)$). It can be proved that for $\alpha \in \mathfrak{B}^n(V)$ $(n \geqslant 2)$ we have $\alpha = 0$ if and only if $\partial_{x^*}(\alpha) = 0$ $\forall x^* \in V^*$ (cf. [N,G2]). We consider analogously defined derivations ∂_x in the algebras $T(V)$, $\hat{\mathfrak{B}}_r(V)$, $T(V)/J$ for J an ideal as above.

6.2. *Some calculations of Nichols algebras related to braided vector spaces of diagonal group type*

In this subsection we compute examples of Nichols algebras of braided vector spaces arising from Example 5.15. We first recall some results on Nichols algebras of braided spaces of diagonal group type, i.e., $(V, c) = (\mathbb{C}X, c^{\mathfrak{q}})$, where X is a trivial rack.

Proposition 6.5. *Let (V, c) be a braided vector space with $V = \mathbb{C}x_1 \oplus \cdots \oplus \mathbb{C}x_\theta$ and*

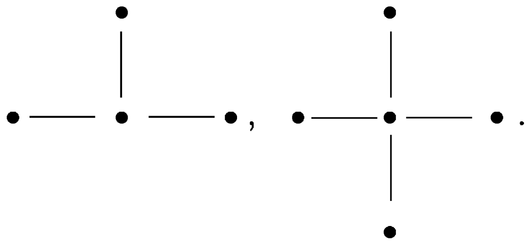
$$c(x_i \otimes x_j) = q_{ij} x_j \otimes x_i, \quad 1 \leqslant i, j \leqslant \theta.$$

(1) *Assume that $q_{ij} = q$ for all i, j. Thus*
   - (*Nichols*) *If $q = -1$, then* $\mathfrak{B}(V) \simeq \Lambda(V)$, *hence* $\dim \mathfrak{B}(V) = 2^\theta$.
   - (*Lusztig*; *see* [AS2]) *If q is a primitive third root of* 1, *then* $\dim \mathfrak{B}(V) = 27$ *when $\theta = 2$; and* $\dim \mathfrak{B}(V) = \infty$ *when $\theta > 2$.*
   - (*Lusztig*; see [AS2]) *If* $\operatorname{ord} q > 3$ *and $\theta \geqslant 2$, then* $\dim \mathfrak{B}(V) = \infty$.

(2) [AD] *Assume that $q_{ii} = -1$ $\forall i$, $q_{ij} \in \{\pm 1\}$ $\forall i, j$. For $i \neq j$, set $A_{ij} \in \{0, -1\}$ such that $q_{ij} q_{ji} = (-1)^{A_{ij}}$. Set also $A_{ii} = 2$. Then $(A_{ij})_{1 \leqslant i,j \leqslant \theta}$ is a simply laced generalized Cartan matrix. Thus*
   - *If the components of the Dynkin diagram corresponding to (A_{ij}) are of type A_m (not necessarily the same m), then* $\dim \mathfrak{B}(V) = 2^{|\Phi^+|}$, *where Φ^+ is the set of positive roots corresponding to (A_{ij}).*
   - *If the Dynkin diagram corresponding to (A_{ij}) contains a cycle, then* $\dim \mathfrak{B}(V) = \infty$. $\square$

Conjecture 6.6 (Andruskiewitsch and Dăscălescu [AD]). *Same notation as in* (2) *above. Then* $\dim \mathfrak{B}(V) = 2^{|\Phi^+|}$ *if* (A_{ij}) *is of finite type, and* $\dim \mathfrak{B}(V) = \infty$ *otherwise.*

Let us consider the Dynkin diagrams:



D_4 $\qquad\qquad$ $D_4^{(1)}$

We shall need to assume only the following weaker form of the previous conjecture:

Conjecture 6.7. *Same notation as in* (2) *above. Then* $\dim \mathfrak{B}(V) = 2^{12}$ *if* (A_{ij}) *is of type* D_4, *and* $\dim \mathfrak{B}(V) = \infty$ *if* (A_{ij}) *is of type* $D_4^{(1)}$.

We next consider a trivial rack X, a finite, non-trivial, abelian group A, denoted multiplicatively; and a non-constant function $\sigma : X \to A$. We set $\kappa_{ij} := \sigma_i \sigma_j^{-1}$, $\eta_{ij} = \mathrm{id}$, $\tau_{ij} = 0$ $\forall i, j \in X$ (cf. Example 5.15). Let $Y = X \times A$, let $(q_{ij})_{i,j \in X}$ be a collection of scalars, let $\omega \in \hat{A}$, let $\chi_{i,j} := \omega =: \mu_{i,j}^{-1}$, for all i, j; define q by (5.23).

Proposition 6.8. *Let* (V, c) *be the braided vector space* $(\mathbb{C}Y, c^{\mathrm{q}})$.

(1) *If* $\operatorname{ord} q_{ii} > 3$ *for some* i, *then* $\dim \mathfrak{B}(V) = \infty$.
(2) *If* $\operatorname{ord} q_{ii} = 3$ *for some* i, *then either* $A \simeq C_2$, *the group of order* 2 (*hence* 27 *divides* $\dim \mathfrak{B}(V)$ *if this is finite*), *or else* $\dim \mathfrak{B}(V) = \infty$.
(3) *Assume that* $q_{ii} = -1$ *for all* $i \in X$. *Furthermore, assume that* $q_{ij} q_{ji} = (-1)^{A_{ij}}$ *for all* $i \neq j \in X$, *where* $A_{ij} \in \{0, -1\}$; *and that* $\operatorname{ord} \kappa_{ij} \leqslant 2$. *Then, if* $A \not\simeq C_2$, *we have* $\dim \mathfrak{B}(V) = \infty$.
(4) *Same hypotheses as in* (3); *assume that the group* $A \simeq \{\pm 1\} \simeq C_2$. *Let* $X_\pm = \{i \in X \colon \sigma_i = \pm 1\}$. *Assume that Conjecture* 6.7 *is true. Then*
   - *If* $\operatorname{card} X_+ = 1$, $\operatorname{card} X_- \leqslant 3$ *and* $q_{ij} q_{ji} = 1$ *for all* $i \neq j \in X_-$, *then* $\dim \mathfrak{B}(V)$ *is finite.*
   - *If* $\operatorname{card} X_- = 1$, $\operatorname{card} X_+ \leqslant 3$ *and* $q_{ij} q_{ji} = 1$ *for all* $i \neq j \in X_+$, *then* $\dim \mathfrak{B}(V)$ *is finite.*
   - *In all other cases*, $\dim \mathfrak{B}(V) = \infty$.

Proof. Let $\hat{Y} = X \times \hat{A}$ and let $Q_{ij}^{\psi,\phi} = q_{ij} \phi(\kappa_{ij}^{-1})$. By Theorem 5.13 and Lemma 5.16, it is enough to consider the braided vector space $(W, c) = (\mathbb{C}\hat{Y}, c^{Q})$.

Then (1) and (2) follow from Proposition 6.5, applied to the subspace $\mathbb{C}\hat{Y}_i$, where $Y_i = \{(i,\psi)\colon \psi \in \hat{A}\}$. The divisibility claim in (2) follows from Proposition 6.17 below.

We prove (3). There exists $i \neq j$ such that κ_{ij} has order 2 (recall that σ is not constant). Let $E = \{\phi \in \hat{A}\colon \phi(\kappa_{ij}) = 1\}$ and $F = \{\phi \in \hat{A}\colon \phi(\kappa_{ij}) = -1\}$; clearly, $\operatorname{card} E = \operatorname{card} F$. Assume that $\operatorname{card} E > 1$, and let $\phi_1 \neq \phi_2 \in E$, $\psi_1 \neq \psi_2 \in F$. There are two possibilities:

- If $q_{ij}q_{ji} = 1$, then (i,ϕ_1), (i,ϕ_2), (j,ψ_1), (j,ψ_2) span a subspace U of W with $c(U \otimes U) = U \otimes U$; the associated Cartan matrix is of type $A_3^{(1)}$, hence $\dim \mathfrak{B}(V) = \infty$.
- If $q_{ij}q_{ji} = -1$, then (i,ϕ_1), (i,ϕ_2), (j,ϕ_1), (j,ϕ_2) span a subspace U of W with $c(U \otimes U) = U \otimes U$; the associated Cartan matrix is of type $A_3^{(1)}$, hence $\dim \mathfrak{B}(V) = \infty$.

We prove (4). Let $i \neq j \in X_+$; then $\kappa_{ij} = 1$. Let us denote $\hat{A} = \{\varepsilon, \operatorname{sgn}\}$. If $q_{ij}q_{ji} = -1$, then (i,ε), (i,sgn), (j,ε), (j,sgn) span a braided vector subspace of Cartan type with matrix $A_3^{(1)}$; by Proposition 6.5 (2), $\dim \mathfrak{B}(V) = \infty$.

We assume then that $q_{ij}q_{ji} = 1$ for all $i \neq j \in X_+$, and also for all $i \neq j \in X_-$. Since κ is non-trivial, both X_+ and X_- are non-empty. Let $i \in X_+$ and consider the vector subspace U spanned by $(\{i\} \cup X_-) \times \hat{A}$. If $\operatorname{card} X_- > 3$, then the Cartan matrix of the braiding of U contains a principal submatrix of type $D_4^{(1)}$. If Conjecture 6.7 is true, then $\dim \mathfrak{B}(V) = \infty$. Hence, we can assume that $\operatorname{card} X_\pm \leqslant 3$. Also, if $\operatorname{card} X_\pm = 2$ then the Cartan matrix of W contains a cycle; by Proposition 6.5 (2), $\dim \mathfrak{B}(V) = \infty$. The only cases left are $\operatorname{card} X_+ = 1$, $\operatorname{card} X_- \leqslant 3$, or $\operatorname{card} X_- = 1$, $\operatorname{card} X_+ \leqslant 3$. In these cases, the Cartan matrices of W are of finite type; either $A_2 \times A_2$, or $A_3 \times A_3$, or $D_4 \times D_4$. This concludes the proof of (4). $\square$

Remark 6.9. (1) In part (2) of the proposition, if $\operatorname{ord} q_{ii} = 3$, for some $i \in X$, and $\operatorname{card} A = 2$, then our present knowledge of Nichols algebras of diagonal type does not allow to obtain any general conclusion on $\dim \mathfrak{B}(V)$.

(2) In part (3) of the proposition, if $\operatorname{ord} q_{ij}q_{ji} > 2$, or $\operatorname{ord} \kappa_{ij} > 2$ for some $i,j \in X$, then our present knowledge of Nichols algebras of diagonal type does not allow to obtain any conclusion on $\dim \mathfrak{B}(V)$.

6.3. Concrete realizations of pointed Hopf algebras computed with Fourier transform

Here we give examples of groups with Yetter–Drinfeld modules as in Proposition 6.8. This in turn produces new examples of pointed Hopf algebras with non-abelian group of grouplikes. We also give a new pointed Hopf algebra using Example 5.17.

For $n, m \in \mathbb{N}$, let $F = C_{4n}$, $G = C_{4m}$ be cyclic groups. Denote by x a generator of F and by y a generator of G. Let F act on G by $y \prec x = y^{2m+1}$, and G act on F by

$y \succ x = x^{2n+1}$. We can consider then the group $F \bowtie G$, which coincides with $F \times G$ as a set and whose multiplication is defined by

$$(x^i y^j)(x^k y^l) = x^i (y^j \succ x^k)(y^j \prec x^k) y^l = x^{i+k+jk(2n)} y^{j+l+jk(2m)}.$$

Notice that the center $Z(F \bowtie G)$ is generated by x^2, y^2. The conjugacy classes of $F \bowtie G$ have then cardinality 1 and 2, and they are $\{x^{2i}y^{2j}\}$, $\{x^{2i+1}y^{2j}, x^{2i+2n+1}y^{2j+2m}\}$, $\{x^{2i}y^{2j+1}, x^{2i+2n}y^{2j+2m+1}\}$, $\{x^{2i+1}y^{2j+1}, x^{2i+2n+1}y^{2j+2m+1}\}$. Take χ defined by $\chi(x) = \chi(y) = -1$, and the Yetter–Drinfeld modules $V_i = M(x^{2i+1}, \chi)$, $W_j = M(y^{2j+1}, \chi)$. We have then the following examples:

(1) $V = V_0 \oplus W_0$. By Proposition 6.8, V is t-equivalent to a space of type $A_2 \times A_2$, and then $\dim \mathfrak{B}(V) = 2^6$. We have a family of link-indecomposable pointed Hopf algebras $\mathfrak{B}(V)\#\mathbb{C}(F \bowtie G)$ of dimension $2^6 \times 16mn = 2^{10}mn$. The smallest example of this family is $n = m = 1$ with dimension 2^{10}. Another way to realize this example is over the dihedral group $\mathbb{D}_4$ of order 8, as described in [MS, 6.5; G1, 5.2].

(2) $V = V_0 \oplus V_1 \oplus W_0$. By Proposition 6.8, V is t-equivalent to a space of type $A_3 \times A_3$, and then $\dim \mathfrak{B}(V) = 2^{12}$. We have a family of link-indecomposable pointed Hopf algebras $\mathfrak{B}(V)\#\mathbb{C}(F \bowtie G)$ of dimension $2^{12} \times 16mn = 2^{16}mn$, for $n \geqslant 2$. The smallest example of this family is $n = 2$, $m = 1$, and then $\dim \mathfrak{B}(V)\#\mathbb{C}(F \bowtie G) = 2^{12} \cdot 32 = 2^{17}$.

(3) $V = V_0 \oplus V_1 \oplus V_2 \oplus W_0$. By Proposition 6.8, V is t-equivalent to a space of type $D_4 \times D_4$. Assuming Conjecture 6.7, we have $\dim \mathfrak{B}(V) = 2^{24}$. We have a family of link-indecomposable pointed Hopf algebras $\mathfrak{B}(V)\#\mathbb{C}(F \bowtie G)$ of dimension $2^{24} \times 16mn = 2^{28}mn$, for $n \geqslant 3$. The smallest example of this family is $n = 3$, $m = 1$, and then $\dim \mathfrak{B}(V)\#\mathbb{C}(F \bowtie G) = 2^{24} \cdot 48 = 2^{28}3$.

Remark 6.10. Actually, in the examples above we have $\dim \mathscr{P}_{g,h} \leqslant 2$ for any g, h grouplikes. If we allow bigger dimensions, then we can take always $\mathbb{D}_4$ as group.

We give now the algebras obtained from Example 5.17. One of them appears in [MS], and then by Lemma 5.18 the other one has the same dimension. We give a full presentation by generators and relations of both of them.

6.3.1. Nichols algebra related to the transpositions in $\mathbb{S}_4$ [MS]

Let $X = \{a, b, c, d, e, f\}$ be the standard crossed set of the transpositions in $\mathbb{S}_4$ and consider the braided vector space $(V, c) = (\mathbb{C}X, c^{\mathfrak{q}})$ associated to the cocycle $\mathfrak{q} \equiv -1$. Here

$$a = (12), \quad b = (13), \quad c = (14), \quad d = (23), \quad e = (24), \quad f = (34).$$

Theorem 6.11 (Milinski and Schneider [MS, 6.4]). *The Nichols algebra $\mathfrak{B}(V)$ can be presented by generators $\{a, b, c, d, e, f\}$ with defining relations*

$$\begin{aligned}
&a^2,\ b^2,\ c^2,\ d^2,\ e^2,\ f^2,\\
&dc + cd,\ eb + be,\ fa + af,\\
&da + bd + ab,\ db + ad + ba,\ ea + ce + ac,\ ec + ae + ca,\\
&fb + cf + bc,\ fc + bf + cb,\ fd + ef + de,\ fe + df + ed.
\end{aligned}\tag{6.1}$$

To obtain a basis, choose one element per row below, juxtaposing them from top to bottom:

$$\begin{aligned}
&(1, a),\\
&(1, b, ba),\\
&(1, c, cb, cba, ca, cab, caba, cabac),\\
&(1, d),\\
&(1, e, ed),\\
&(1, f).
\end{aligned}$$

Its Hilbert polynomial is then

$$\begin{aligned}
P(t) &= (1+t)(1+t+t^2)(1+t+2t^2+2t^3+t^4+t^5)(1+t)(1+t+t^2)(1+t)\\
&= (1+t)^4(1+t+t^2)^2(1+t^2)^2\\
&= t^{12} + 6t^{11} + 19t^{10} + 42t^9 + 71t^8 + 96t^7 + 106t^6 + 96t^5 + 71t^4 + 42t^3\\
&\quad + 19t^2 + 6t + 1.
\end{aligned}$$

Its dimension is $2^6 3^2 = 576$. Its top degree is 12. An integral is given by abacabacdedf.

We give an alternative proof to that in [MS, 6.4] using Theorem 6.4.

Proof. It is straightforward to see that the elements in (6.1) vanish in $\mathfrak{B}(V)$. One can either use differential operators or either compute $Q_2 = 1 + c$ on them. Using Gröbner bases it can be seen that if J is the ideal generated by these relations, then $T(V)/J$ has the stated basis. Since J is generated by primitive elements, it is a coideal. Furthermore, J is generated by homogeneous elements with respect to the $\mathrm{Inn}_{\triangleright}(X)$-grading, and it is invariant under the $\mathrm{Inn}_{\triangleright}(X)$-action. By Lemma 6.2, it is compatible with the braiding and then $T(V)/J$ is a braided Hopf algebra. Last, we show that *abacabacdedf* does not vanish in $\mathfrak{B}(V)$: it is straightforward to see that

$$\partial_a\partial_b\partial_a\partial_c\partial_a\partial_b\partial_a\partial_c\partial_d\partial_e\partial_d\partial_f(abacabacdedf) = 1.$$

Now, we conclude by Theorem 6.4, part (2). $\square$

To realize this example, one can take $G = \mathbb{S}_4$, $g = (1\,2)$, $\chi = \mathrm{sgn}$. Then $V = M(g,\chi) \in {}^G_G\mathcal{YD}$ is isomorphic to $(\mathbb{C}X, c^{\mathfrak{q}})$. We get a pointed Hopf algebra $\mathfrak{B}(V)\#\mathbb{C}G$ whose dimension is $576 \times 24 = 2^9 3^3$. One can construct also a family of link-indecomposable pointed Hopf algebras taking as group $\mathbb{S}_4 \times C_m$, where C_m is the cyclic group of m elements and m is odd. Let $g = (1\,2) \times t$ (t is a generator of C_m) and let the character χ be the product $\mathrm{sgn} \times \varepsilon$ (ε is the trivial character). Then $V = M(g,\chi)$ is again isomorphic to $(\mathbb{C}X, c^{\mathfrak{q}})$ and we get a pointed Hopf algebra of dimension $2^9 3^3 m$.

6.3.2. Nichols algebra related to the faces of the cube

Let $X = \{a,b,c,d,e,f\}$ be the polyhedral crossed set of the faces of the cube (that is, the 4-cycles in $\mathbb{S}_4$), where $\{a,f\}$, $\{b,e\}$, $\{c,d\}$ are the pairs of opposite faces and $a \triangleright b = c$. Consider the braided vector space $(V,c) = (\mathbb{C}X, c^{\mathfrak{q}})$ associated to the cocycle $\mathfrak{q} \equiv -1$.

By Lemmas 6.1 and 5.18, the Nichols algebra of V has the same Hilbert series as that of the preceding example. We can indeed give the precise description of $\mathfrak{B}(V)$:

Theorem 6.12. *The Nichols algebra $\mathfrak{B}(V)$ can be presented by generators $\{a,b,c,d,e,f\}$ with defining relations*

$$\begin{gathered} a^2,\ b^2,\ c^2,\ d^2,\ e^2,\ f^2, \\ ec+ce,\ db+bd,\ fa+af, \\ ca+bc+ab,\ da+cd+ac,\ eb+ba+ae,\ fb+ef+be, \\ fc+cb+bf,\ fd+dc+cf,\ fe+ed+df,\ ea+de+ad. \end{gathered} \tag{6.2}$$

To obtain a basis, choose one element per row below, juxtaposing them from top to bottom:

$$\begin{gathered} (1,a), \\ (1,b,ba), \\ (1,c,cb,cba), \end{gathered}$$

$$(1, d, dc, dcb),$$

$$(1, e, ed),$$

$$(1, f).$$

Its Hilbert polynomial is then

$$\begin{aligned}P(t) &= (1+t)(1+t+t^2)(1+t+t^2+t^3)(1+t+t^2+t^3)(1+t+t^2)(1+t)\\ &= (1+t)^4(1+t+t^2)^2(1+t^2)^2\\ &= t^{12}+6t^{11}+19t^{10}+42t^9+71t^8+96t^7+106t^6+96t^5+71t^4+42t^3\\ &\quad + 19t^2+6t+1.\end{aligned}$$

Its dimension is $2^6 3^2 = 576$. *Its top degree is* 12. *An integral is given by abacbadcbedf.*

Proof. Again, the elements in (6.2) are easily seen to be relations in $\mathfrak{B}(V)$. Using Gröbner bases, it can be seen that if J is the ideal generated by these elements, then $T(V)/J$ is as stated. We conclude now using Lemmas 6.1 and 5.18. □

To realize this example, one can take the $G = \mathbb{S}_4$, $g = (1\,2\,3\,4)$, $\chi = \mathrm{sgn}$. Then $V = M(g,\chi) \in {}^G_G\mathcal{YD}$ is isomorphic to $(\mathbb{C}X, c^{\mathfrak{q}})$. We get a pointed Hopf algebra $\mathfrak{B}(V)\#\mathbb{C}G$ whose dimension is $576 \times 24 = 2^9 3^3$. Also here we get a family of link-indecomposable pointed Hopf algebras taking the group $\mathbb{S}_4 \times C_m$ (m odd), $g = (1\,2\,3\,4) \times t$ (t a generator of C_m) and $\chi = \mathrm{sgn} \times \varepsilon$.

6.4. Some relations of Nichols algebras of affine racks

We first present relations in Nichols algebras related to affine racks. The relation in part (1) of the following lemma is related to [MS, 5.7]; here the rack is more general than there, there the cocycle is more general than here. Although the relation in part (3) below has the same appearance than [MS, (5.24)], the racks and the elements x, y are different.

Lemma 6.13. *Let* (A, g) *be an affine crossed set. Let* $\mathfrak{q} \equiv q$ *and* $(V = \mathbb{C}A, c^{\mathfrak{q}})$ *the corresponding braided vector space.*

(1) *Let* $x_1, x_2 \in A$ *and* $q = -1$. *Define inductively the elements* $x_i \in A$ $(i \geqslant 3)$ *by* $x_i = x_{i-1} \triangleright x_{i-2}$. *Let* n *be the minimum positive integer such that* $x_2 - x_1 \in \ker \sum_{i=0}^{n-1} (-g)^i$. *Then in* $\mathfrak{B}(V)$ *we have the relation*

$$x_2x_1 + x_3x_2 + \cdots + x_nx_{n-1} + x_1x_n = 0.$$

Furthermore, taking different pairs (x_2, x_1), *this is a basis of the relations in degree* 2. *In other words, consider in* $A \times A$ *the relation* $(x_2, x_1) \sim (a, b)$ *if* *there exists* $m \in \mathbb{N}$ *such that* $(a, b) = (x_m, x_{m-1})$, *where the* x_i*'s are defined as above. Then* $\sim$ *is an equivalence relation, and the dimension of the space of relations of* $\mathfrak{B}(V)$ *in degree* 2 (*i.e.*, *the kernel of the multiplication* $V \otimes V \to \mathfrak{B}(V)$) *coincides with the number of equivalence classes* $|A \times A/\sim|$.

(2) *If* $-q$ *is a primitive* ℓ*th root of unity*, *then the relations in degree* 2 *are the chains*

$$x_2x_1 + (-q)x_3x_2 + (-q)^2x_4x_3 + \cdots + (-q)^{n-1}x_1x_n$$

such that $\ell | n$. *The elements* $x_i \in A$ *and* $n \in \mathbb{N}$ *are defined as in part* (1).

(3) *If* $(1 - g + g^2 - g^3)(x - y) = 0$ *and* $q = -1$, *then in the Nichols algebra* $\mathfrak{B}(V)$ *we have the relation*

$$xyxy + yxyx = 0.$$

The element $xyxy + yxyx$ *is homogeneous with respect to the* $\mathrm{Inn}_{\triangleright}(A)$-*grading*. *Furthermore*, *in the algebra* $\hat{\mathfrak{B}}_2(V)$ (*see Theorem* 6.4) *the element* $xyxy + yxyx$ *is primitive. In other words*, *if* $Q \supseteq Q_2$ *is an* $\mathrm{Inn}_{\triangleright}(A)$-*homogeneous coideal*, *then the ideal generated by* $Q + \mathbb{C}(xyxy + yxyx)$ *is also an* $\mathrm{Inn}_{\triangleright}(A)$-*homogeneous coideal*.

(4) *If* $(1 - g + g^2)(x - z) = (1 - g + g^2)(y - z) = 0$ *and* $q = -1$, *then in the Nichols algebra* $\mathfrak{B}(V)$ *we have the relation*

$$xyzxyz + yzxyzx + zxyzxy = 0.$$

The element $xyzxyz + yzxyzx + zxyzxy$ *is homogeneous with respect to the* $\mathrm{Inn}_{\triangleright}(A)$-*grading*. *Furthermore*, *in the algebra* $\hat{\mathfrak{B}}_2(V)$ (*see Theorem* 6.4) *the element* $xyzxyz + yzxyzx + zxyzxy$ *is primitive. In other words*, *if* $Q \supseteq Q_2$ *is an* $\mathrm{Inn}_{\triangleright}(A)$-*homogeneous coideal*, *then the ideal generated by* $Q + \mathbb{C}(xyzxyz + yzxyzx + zxyzxy)$ *is also an* $\mathrm{Inn}_{\triangleright}(A)$-*homogeneous coideal*.

Proof

(1) It is easy to see by induction that

$$x_t = \sum_{i=0}^{t-2} (-g)^i (x_2 - x_1) + x_1.$$

Then $x_n \triangleright x_{n-1} = x_{n+1} = x_1$ and $x_1 \triangleright x_n = x_{n+2} = x_2$. It is easy to see that, g being invertible, the chain corresponding to $x'_1 = x_t$, $x'_2 = x_{t+1}$ is exactly the same. This is because $x_{t+1} - x_t = (-g)^{t-1}(x_2 - x_1)$. This proves that the relation $\sim$ is an equivalence relation. On the other hand, the relations in degree 2 are exactly the kernel of $1 + c$. Thus, we compute

$$\begin{aligned}
&(1 + c)(x_2x_1 + x_3x_2 + \cdots + x_1x_n) \\
&\quad = x_2x_1 - x_3x_2 + x_3x_2 - x_4x_3 + \cdots + x_1x_n - x_2x_1 \\
&\quad = 0.
\end{aligned}$$

Observe that for $x_1 = x_2 = x$ the minimum n is 1 and we get the relation $x^2 = 0$. To see that these relations generate all the relations in degree 2, let us take, for a (not necessarily primitive) nth root of unit ζ, the vector

$$x_2x_1 + \zeta x_3x_2 + \zeta^2 x_4x_3 + \cdots + \zeta^{n-1}x_1x_n.$$

It is clear that this vector is an eigenvector of c with eigenvalue $\frac{-1}{\zeta}$. Thus, each of the strings $(x_1, x_2, \dots, x_n)$ occurs n times, one for each nth root of unity, and each of these times with a different eigenvalue. By a dimension argument, we have diagonalized c and we have picked up the eigenspace associated to -1.

(2) The same eigenvectors found in the previous part are eigenvectors here, though their eigenvalues are q/ζ. Thus, for a chain of length n to be a relation, one must have $q/\zeta = -1$, i.e., $-q$ must be an nth root of unity.

(3) Let $z = y \triangleright x$, $w = z \triangleright y$. By the previous part, we have in $\mathfrak{B}(V)$

$$x^2 = y^2 = z^2 = w^2 = 0, \quad yx + zy + wz + xw = 0.$$

Let us apply now ∂_y to the alleged relation. We get

$$\begin{aligned}\partial_y(xyxy + yxyx) &= xzy + xyx - zyz - yxz = x(zy + yx) - (zy + yx)z \\ &= -x(wz + xw) + (wz + xw)z = -xwz + xwz = 0.\end{aligned}$$

Analogously, $\partial_x(xyxy + yxyx) = 0$. If $a \neq x, a \neq y$, then $\partial_a(xyxy + yxyx) = 0$ as well. This shows that $xyxy + yxyx = 0$ in $\mathfrak{B}(V)$, but we have claimed a stronger fact. To see that $xyxy + yxyx$ is primitive modulo J_2, we must prove that in $T(V)$ we have

$$\Delta(xyxy + yxyx) \in (xyxy + yxyx) \otimes 1 + 1 \otimes (xyxy + yxyx) + T(V) \otimes J_2 + J_2 \otimes T(V).$$

Now, Δ is a graded map: $\Delta = \oplus_{n,m}\Delta_{n,m}$, where $\Delta_{n,m} : T^{n+m}(V) \to T^n(V) \otimes T^m(V)$. We must prove then that the images of $xyxy + yxyx$ by $\Delta_{1,3}$, $\Delta_{2,2}$ and $\Delta_{3,1}$ lie in $T(V) \otimes J_2 + J_2 \otimes T(V)$. The previous argument, with derivations, shows that $\Delta_{3,1}(xyxy + yxyx) \in J_2 \otimes V$. For the others, let us introduce the following notation: if $m \in \mathbb{N}$, we take the basis $\{x_1 \cdots x_m \mid x_i \in A \ \forall i\}$ of $T^m(V)$. Let $\{(x_1 \cdots x_m)^* \mid x_i \in A \ \forall i\}$ be the dual basis, and let $\partial_{x_1 \cdots x_m} = (\mathrm{id} \otimes (x_1 \cdots x_m)^*) \circ \Delta$. These maps are skew differential operators of degree m and for $m = 1$ they coincide with the derivations. We have then for $W \in T^n(V)$,

$$\Delta_{n-m,m}(W) = \sum_{x_1 \in A, \dots, x_m \in A} \partial_{x_1 \cdots x_m}(W) \otimes (x_1 \cdots x_m).$$

We prove now that $\Delta_{2,2}(xyxy + yxyx) \in T(V) \otimes J_2 + J_2 \otimes T(V)$. Clearly, $\Delta_{ab}(xyxy + yxyx) = 0$ unless $\{a, b\} \subseteq \{x, y\}$. Since xx and yy are in J_2, it is sufficient to see that the image of $xyxy + yxyx$ by ∂_{xy} and ∂_{yx} lies in J_2. Let $t = x \triangleright y$ and $s = t \triangleright x$. Then $st + tx + xy + ys \in Q_2$. Furthermore, $x \triangleright z = x \triangleright (y \triangleright x) = (x \triangleright y) \triangleright (x \triangleright x) = t \triangleright x = s$. Now, it is straightforward to check that $\partial_{xy}(xyxy + yxyx) = st + tx + xy + ys \in J_2$. The computation for ∂_{yx} is analogous. Finally, it is easy to see that

$\partial_{xyx}(xyxy+yxyx)=\partial_{yxy}(xyxy+yxyx)=0$, which proves that $\Delta_{1,3}(xyxy+yxyx)\in T(V)\otimes J_2+J_2\otimes T(V)$.

It remains to be proved that $xyxy+yxyx$ is $\mathrm{Inn}_{\triangleright}(A)$-homogeneous. This is equivalent to prove that $\phi_x\phi_y\phi_x\phi_y=\phi_y\phi_x\phi_y\phi_x$. Take $a\in A$. We have $\phi_x\phi_y(a)=(1-g)x+g(1-g)y+g^2a$, and then

$$\begin{aligned}\phi_x\phi_y\phi_x\phi_y(a)&=(1+g^2)(1-g)x+g(1-g)(1+g^2)y+g^4a\\&=x-g^4y+g(1-g+g^2)(y-x)+g^4a=x-g^4y+(y-x)+g^4a\\&=y-g^4y+g^4a\end{aligned}$$

Analogously, $\phi_y\phi_x\phi_y\phi_x(a)=x-g^4x+g^4a$. Then

$$\phi_x\phi_y\phi_x\phi_y(a)-\phi_y\phi_x\phi_y\phi_x(a)=(1-g^4)(y-x)=0.$$

(4) Let us define the following elements in A:

$$\begin{aligned}h&=y\triangleright z=(1-g)y+gz,\\s&=x\triangleright y=(1-g)x+gy,\\t&=x\triangleright h=(1-g)x+y-(1-g)z,\\r&=x\triangleright z=(1-g)x+gz,\\b&=x\triangleright(y\triangleright r)=x+y-z.\end{aligned}$$

One can check that $t=s\triangleright r$, $b=y\triangleright t$. It is straightforward to check that any two of these elements satisfy that their difference lies in the kernel of $1-g+g^2$. This is so because each of these is an affine combination of x,y,z whose parameters are polynomials in g (and any such polynomial leaves $\ker(1-g+g^2)$ invariant). By the first part, we have the following relations in $\hat{\mathfrak{B}}_2(V)$:

$$x^2=y^2=z^2=h^2=s^2=t^2=r^2=0,$$

$$hy+yz+zh=sx+xy+ys=tx+xh+ht=rx+xz+zr=0, \tag{6.3}$$

$$sr+rt+ts=by+yt+tb=zsz-szs=0.$$

Notice that for any two of these elements, say x_1,x_2, if we put $x_3=x_2\triangleright x_1$ we then get $x_2x_1+x_3x_2+x_1x_3=0$, and then, since $x_1^2=x_2^2=0$, we have $x_1x_2x_1=x_2x_1x_2$.

This explains the relation $zsz - szs = 0$ above. As in the previous case, we must prove that the image of $xyzxyz + yzxyzx + zxyzxy$ by $\Delta_{1,5}$, $\Delta_{2,4}$, $\Delta_{3,3}$, $\Delta_{4,2}$ and $\Delta_{5,1}$ lies in $J_2 \otimes T(V) + T(V) \otimes J_2$. This is a very long computation, but it is straightforward and we give only two examples: for $\Delta_{5,1}$ we apply ∂_x and for $\Delta_{3,3}$ we apply ∂_{xyx} and ∂_{yxy}. Let us call $W = xyzxyz + yzxyzx + zxyzxy$. We have

$$\partial_x(W) = -srxsr + xyzsr - yzsrx + yzxyz + zsrxs - zxyzs,$$

$$\partial_{xyx}(W) = txb + yzt - ztx,$$

$$\partial_{yxy}(W) = xhb - hby - zxh.$$

It can be seen that relations (6.3) imply that the first of these elements lies in J_2. The second and third elements do not lie in J_2; however, since modulo J_2 we have $xyx = yxy$, in the image by $\Delta_{3,3}$ we have

$$\begin{aligned}&\partial_{xyx}(W) \otimes xyx + \partial_{yxy}(W) \otimes yxy \\ &\quad = (txb + yzt - ztx + xhb - hby - zxh) \otimes xyx \text{ modulo } T(V) \otimes J_2.\end{aligned}$$

Now, it can be seen that relations (6.3) imply that $txb + yzt - ztx + xhb - hby - zxh$ lies in J_2. The proof that W is $\mathrm{Inn}_{\triangleright}(A)$-homogeneous is analogous to that of $xyxy + yxyx$ being homogeneous in part (3). $\square$

Remark 6.14. If $A = \mathbb{F}_{p^t}$, g is the multiplication by $w \neq -1$, then the minimum n in part (1) of the Lemma is always the order of $-w$ as a root of unit in $\mathbb{F}_{p^t}$, except for $x_1 = x_2 = x$. We have then exactly $p^t + \frac{p^{2t} - p^t}{n}$ independent relations in degree 2, and therefore the dimension of $\mathfrak{B}^2(V)$ is $\frac{n-1}{n}(p^{2t} - p^t)$. If $w = -1$, we have the same result with $n = p = \mathrm{char}(\mathbb{F}_{p^t})$. Furthermore, if $n = 4$ then we can apply part (3) for any two elements $x, y \in A$. If $n = 3$ then we can apply part (4) for any three elements $x, y, z \in A$.

6.5. *Examples of Nichols algebras and pointed Hopf algebras on affine racks*

We present here two examples. In both we have relations given by Lemma 6.13.

6.5.1. *Nichols algebra related to the vertices of the tetrahedron [G1]*

Let $X = \{1, 2, 3, 4\}$ be the polyhedral crossed set of the vertices of the tetrahedron and consider the braided vector space $(V, c) = (\mathbb{C}X, c^{\mathfrak{q}})$ associated to the cocycle $\mathfrak{q} \equiv -1$.

Theorem 6.15. *The Nichols algebra* $\mathfrak{B}(V)$ *can be presented by generators* $\{1,2,3,4\}$ *with defining relations*

$$\begin{aligned}&1^2,\ 2^2,\ 3^2,\ 4^2,\\ &31+23+12,\ 41+34+13,\ 42+21+14,\ 43+32+24,\\ &321321+213213+132132.\end{aligned}\tag{6.4}$$

To obtain a basis, choose one element per row below, juxtaposing them from top to bottom (e *is the unit element*):

$$\begin{gathered}(e,1),\\ (e,2,21),\\ (e,321),\\ (e,3,32),\\ (e,4).\end{gathered}$$

Its Hilbert polynomial is then $P(t)=t^9+4t^8+8t^7+11t^6+12t^5+12t^4+11t^3+8t^2+4t+1$. Its dimension is 72, its top degree is 9, an integral is given by 121321324.

Proof. As explained in Remark 1.26, the tetrahedron crossed set coincides with the affine crossed set $(\mathbb{F}_4,w)$, where $w^2+w+1=w^2-w+1=0$. Cases (1) with $n=3$ and (4) of Lemma 6.13 apply immediately and we see that the elements in (6.4) are relations in $\mathfrak{B}(V)$. Let J be the ideal generated by these elements. It can be seen that J is $\mathrm{Inn}_{\triangleright}(X)$-stable. Since by Lemma 6.13 part (4) the element $321321+213213+132132$ is $\mathrm{Inn}_{\triangleright}(X)$-homogeneous and Q_2 is compatible with the braiding, then J is compatible with the braiding. Moreover, by Lemma 6.13 part (4) again, it is a coideal. Now, it is straightforward to see that

$$\partial_1\partial_2\partial_3\partial_4\partial_2\partial_4\partial_3\partial_4(121321324)=2\in\mathbb{C}.$$

We now use Theorem 6.4 part (2). $\square$

To realize this example, one can take the affine group $\mathbb{F}_4\rtimes\mathbb{F}_4^{\times}\simeq\mathbb{A}_4$ and its direct product with C_2. That is, we take $G=\mathbb{A}_4\times C_2$. Denote by t the generator of C_2 and let $g=(1\,2\,3)\times t\in G$. Take $\chi\in\hat{G}$, $\chi(\sigma\times t^i)=(-1)^i$. Then $V=M(g,\chi)\in{}^G_G\mathcal{YD}$ is isomorphic to $(\mathbb{C}X,c^{\mathfrak{q}})$. We get a pointed Hopf algebra $\mathfrak{B}(V)\#\mathbb{C}G$ whose dimension is $72\times 24=2^6 3^3$. We get a family of link-indecomposable pointed Hopf algebras replacing C_2 by C_m (m even), $g=(1\,2\,3)\times t$ (t a generator of C_m) and $\chi(\sigma\times t^i)=(-1)^i$.

6.5.2. Nichols algebra related to the affine crossed set $(\mathbb{Z}_5, \triangleright^2)$

Let $X = \{0, 1, 2, 3, 4\}$ be the affine crossed set $(\mathbb{Z}_5, \triangleright^2)$ and consider the braided vector space $(V, c) = (\mathbb{C}X, c^{\mathfrak{q}})$ associated to the cocycle $\mathfrak{q} \equiv -1$. That is, $c(i \otimes j) = -(2j - i) \otimes i$.

Theorem 6.16. *The Nichols algebra* $\mathfrak{B}(V)$ *can be presented by generators* $\{0, 1, 2, 3, 4\}$ *with defining relations*

$$\begin{aligned}
&0^2,\ 1^2,\ 2^2,\ 3^2,\ 4^2,\\
&32 + 20 + 13 + 01,\ 40 + 21 + 14 + 02,\ 41 + 34 + 10 + 03,\\
&42 + 30 + 23 + 04,\ 43 + 31 + 24 + 12,\\
&1010 + 0101.
\end{aligned} \tag{6.5}$$

To obtain a basis, choose one element per row below, juxtaposing them from top to bottom (*e is the unit element*):

$$\begin{aligned}
&(e, 0),\\
&(e, 1, 10, 101),\\
&(e, 2, 21, 212, 20, 201, 2012, 2010, 20102, 201020),\\
&(e, 3, 31, 312, 30, 303, 3031, 30312),\\
&(e, 4).
\end{aligned}$$

Its Hilbert polynomial is then

$$\begin{aligned}
P(t) &= (1 + t)^2(1 + t + t^2 + t^3)(1 + t + 2t^2 + 2t^3 + 2t^4 + t^5 + t^6)\\
&\quad \times (1 + t + 2t^2 + 2t^3 + t^4 + t^5)\\
&= t^{16} + 5t^{15} + 15t^{14} + 35t^{13} + 66t^{12} + 105t^{11} + 145t^{10} + 175t^9 + 186t^8 + 175t^7\\
&\quad + 145t^6 + 105t^5 + 66t^4 + 35t^3 + 15t^2 + 5t + 1.
\end{aligned}$$

Its dimension is 1280. *Its top degree is* 16. *An integral is given by* 0101201020303124.

Proof. The relations are given by Lemma 6.13, parts (1) and (3). By the same result, if J is the ideal generated by (6.5) then it is a homogeneous coideal. It is not difficult to see that it is also $\mathrm{Inn}_{\triangleright}(X)$-stable, whence it is compatible with the braiding. Using Gröbner bases, it can be seen that relations (6.5) yield the stated dimensions in each degree. Using Theorem 6.4 part (2), it is sufficient to see that 0101201020303124 does not vanish in $\mathfrak{B}(V)$ in order to prove the Theorem. It is straightforward then to compute that

$$\partial_1\partial_0\partial_4\partial_1\partial_4\partial_2\partial_3\partial_4\partial_2\partial_4\partial_3\partial_2\partial_3\partial_4\partial_3\partial_4(0101201020303124) = 1\in\mathbb{C}. \qquad \square$$

To realize this example, one can take the group $G = \mathbb{Z}/5 \rtimes (\mathbb{Z}/5)^{\times}$, $\chi((a,2^j)) = (-1)^j$, $g = (0,2)$. Then $V = M(g,\chi) \in {}^G_G\mathcal{YD}$ is isomorphic to $(\mathbb{C}X, c^{\mathfrak{q}})$. We get a pointed Hopf algebra $\mathfrak{B}(V)\#\mathbb{C}G$ whose dimension is $1280 \times 20 = 2^{10}5^2$. We get a family of link-indecomposable pointed Hopf algebras replacing $(\mathbb{Z}/5)^{\times}$ by C_{4m}, where a generator t of C_{4m} acts as 2, i.e., $tit^{-1} = 2i$ for $i\in\mathbb{Z}/5$. Then take $g = 0 \times t$, $\chi(i \times t^j) = (-1)^j$, $V = M(g,\chi) \in {}^G_G\mathcal{YD}$. The algebra $\mathfrak{B}(V)\#\mathbb{C}G$ has dimension $2^{10}5^2m$.

6.6. A freeness result for extensions of crossed sets

The concept of extension of crossed sets is not only useful in classification problems of them. It turns out to be useful as well when one wants to compute Nichols algebras, as the following Proposition asserts.

Let X, Y be quandles and let $X \to Y$ be a surjective quandle homomorphism. We assume that X is indecomposable, hence Y is also indecomposable and $X \simeq Y \times_{\alpha} S$ for some dynamical 2-cocycle α and some set S (see Definition 2.2). Let $\mathfrak{q} : Y \times Y \to \mathbb{G}_{\infty}$ be a 2-cocycle. Notice that $\mathfrak{q}_{ii} = \mathfrak{q}_{jj}$ for all $i,j\in Y$. Let $\tilde{\mathfrak{q}}$ be the pull-back of $\mathfrak{q}$ along π, that is $\tilde{\mathfrak{q}}_{xy} := \mathfrak{q}_{\pi(x),\pi(y)}$. Let $(V,c) = (\mathbb{C}X, c^{\tilde{\mathfrak{q}}})$, $(V',c') = (\mathbb{C}Y, c^{\mathfrak{q}})$. Let $P_V(t)$ be the Hilbert series of $\mathfrak{B}(V)$ and $P_{V'}(t)$ the Hilbert series of $\mathfrak{B}(V')$.

Proposition 6.17.

(1) *If the order of* $\mathfrak{q}_{ii}$ *is* >3 *and* $\operatorname{card} S \geq 2$ *then* $\dim\mathfrak{B}(V) = \infty$. *If the order of* $\mathfrak{q}_{ii}$ *is* 3 *and* $\operatorname{card} S \geq 3$ *then* $\dim\mathfrak{B}(V) = \infty$.
(2) *Let* $P_S(t)$ *be the Hilbert polynomial of* $\mathfrak{B}(W)$, *where* $(W, c_W) = (\mathbb{C}S, c^{\mathfrak{q}_{ii}})$ (*i.e., the cocycle is the constant* $\mathfrak{q}_{ii}$)). *Then* $P_S \mid P_V$.
(3) *If* α *is a constant cocycle*, $P_{V'} \mid P_V$.

Proof. (1) follows easily from [G1, Lemma 3.1]. (2) follows at once from [G2, Theorem 3.8.1]. (3) can be proved using a remark right after the proof of [MS, Theorem 3.2]. Actually, this remark is a generalization of Theorem 3.2 in [MS], which in turn is a generalization of [G2, Theorem 3.8.1]. The remark goes as follows: let (R,c), (R',c') be braided Hopf algebras with maps $R' \xrightarrow{i} R \xrightarrow{\phi} R'$ of algebras and coalgebras such that $\phi i = \mathrm{id}$, and such that

$$(i\otimes\mathrm{id})c'(\phi\otimes\mathrm{id}) = (\mathrm{id}\otimes\phi)c(\mathrm{id}\otimes i), \quad c(i\phi\otimes\mathrm{id}) = (\mathrm{id}\otimes i\phi)c. \tag{6.6}$$

Let $\rho : R \to R\otimes R'$, $\rho = (\mathrm{id}\otimes\phi)\Delta_R$, and let $K = R^{\mathrm{co}R'} = \{r\in R \mid \rho(r) = r\otimes 1\}$. Then the conditions on i and ϕ are sufficient to prove that $\mu : K\otimes R' \to R$, $\mu = m_R(\mathrm{id}\otimes i)$ is an isomorphism.

Thus, we can find $i : \mathfrak{B}(V') \to \mathfrak{B}(V)$ and $\phi : \mathfrak{B}(V) \to \mathfrak{B}(V')$ satisfying the previous conditions. By the definitions of Nichols algebras, to give an algebra and coalgebra map it is enough to give the maps at degree 1 and verify that they commute with the braidings. That is, $V' \overset{i}{\to} V \overset{\phi}{\to} V'$ such that $c(i \otimes i) = (i \otimes i)c'$ and similarly with ϕ. We take $i(y) = \frac{1}{|S|} \sum_{\pi(x)=y} x$, $\phi(x) = \pi(x)$. It is immediate to see that i and ϕ commute with the braidings, using that π is a map of crossed sets and $\tilde{\mathfrak{q}} = \pi^{-1}(\mathfrak{q})$. The conditions in (6.6) are also easy to verify; for the second one it is used that α is a constant cocycle. $\square$

Acknowledgments

We thank R. Guralnick for kindly communicating us Theorem 3.7. We are grateful to P. Etingof and J. Alev for interesting discussions, as well as to J.S. Carter, A. Harris and M. Saito for pointing out several misprints and statements which needed some clarification in earlier versions of the manuscript. Our deep gratitude is due to F. Fantino for carefully reading the paper and sharing with us his comments. We thank S. Natale for encouraging us with Section 6.

Results of this paper were announced at the XIV Coloquio latinoamericano de Álgebra, La Falda, august 2001, by the second-named author. Part of the work of the first author was done during a visit to the University of Reims (October 2001–January 2002); he is very grateful to J. Alev for his kind hospitality.

References

[A] N. Andruskiewitsch, About finite dimensional Hopf algebras, Quantum Symmetries in Theoretical Physics and Mathematics, Contemp. Math. 294 (2002).

[AD] N. Andruskiewitsch, S. Dăscălescu, On quantum groups at −1, Algebra Represent. Theory, to appear.

[AG] N. Andruskiewitsch, M. Graña, Braided Hopf algebras over non-abelian groups, Bol. Acad. Ciencias (Córdoba) 63 (1999) 45–78 Also in `math.QA/9802074`.

[AS1] N. Andruskiewitsch, H.-J. Schneider, Finite quantum groups and Cartan matrices, Adv. Math. 154 (2000) 1–45.

[AS2] N. Andruskiewitsch, H.-J. Schneider, Pointed Hopf algebras, in: S. Montgomery, H.-J. Schneider (Eds.), New Directions in Hopf Algebras, Cambridge University Press, Cambridge, pp. 1–68.

[B] E. Brieskorn, Automorphic sets and singularities, Contemp. Math. 78 (1988) 45–115.

[CES] J.S. Carter, M. Elhamdadi, M. Saito, Twisted quandle homology theory and Cocycle knot invariants, Algebra Geom. Topol. 2 (2002) 95–135.

[CENS] J.S. Carter, M. Elhamdadi, M.A. Nikiforou, M. Saito, Extensions of quandles and cocycle knot invariants, `math.GT/0107021`.

[CHNS] J.S. Carter, A. Harris, M.A. Nikiforou, M. Saito, Cocycle knot invariants, quandle extensions, and Alexander matrices, `math.GT/0204113`.

[CJKLS] J.S. Carter, D. Jelsovsky, S. Kamada, L. Langford, M. Saito, State-sum invariants of knotted curves and surfaces from quandle cohomology, Trans. Amer. Math. Soc., to appear. Also in `math.GT/9903135`.

[CJKS] J.S. Carter, D. Jelsovsky, S. Kamada, M. Saito, Quandle homology groups, their Betti numbers, and virtual knots, J. Pure Appl. Algebra 157 (2001) 135–155.

[CS] J.S. Carter, M. Saito, Quandle homology theory and cocycle knot invariants, math.GT/0112026.

[De] P. Dehornoy, Braids and self-distributivity, Prog. Math. 192 (2000).

[Dr] V G. Drinfeld, On some unsolved problems in quantum group theory, in: Quantum Groups (Leningrad, 1990), Lecture Notes in Mathematics, Vol. 1510, Springer, Berlin, 1992, pp. 1–8.

[EG] P. Etingof, M. Graña, On rack cohomology, J. Pure Appl. Algebra, to appear. Also in math.QA/0201290.

[EGS] P. Etingof, R. Guralnik, A. Soloviev, Indecomposable set-theoretical solutions to the quantum Yang–Baxter equation on a set with prime number of elements, J. Algebra 242 (2) (2001) 709–719.

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

[FR] R. Fenn, C. Rourke, Racks and links in codimension two, J. Knot Theory Ramifications 1 (4) (1992) 343–406.

[FK] S. Fomin, A.N. Kirilov, Quadratic algebras, Dunkl elements, and Schubert calculus, Progr. Math. 172 (1999) 146–182.

[G1] M. Graña, On Nichols algebras of low dimension, in: New Trends in Hopf Algebra Theory, Contemp. Math. 267 (2000) 111–136.

[G2] M. Graña, A freeness theorem for Nichols algebras, J. Algebra 231 (1) (2000) 235–257.

[G3] M. Graña, Indecomposable racks of order p^2, math.QA/0203157.

[J1] D. Joyce, A classifying invariant of knots, the knot quandle, J. Pure Appl. Algebra 23 (1982) 37–65.

[J2] D. Joyce, Simple quandles, J. Algebra 79 (2) (1982) 307–318.

[K] L. Kauffman, Knots and Physics, World Scientific, Singapore, 1991, 1994, 2001.

[LN] R.A. Litherland, S. Nelson, The Betti numbers of some finite racks, math.GT/0106165.

[LYZ1] Jiang-Hua Lu, Min Yan, Yong-Chang Zhu, On set-theoretical Yang–Baxter equation, Duke Math. J. 104 (2000) 1–18.

[LYZ2] Jiang-Hua Lu, Min Yan, Yong-Chang Zhu, On Hopf algebras with positive bases, J. Algebra 237 (2) (2001) 421–445.

[LYZ3] Jiang-Hua Lu, Min Yan, Yong-Chang Zhu, Quasi-triangular structures on Hopf algebras with positive bases, in New Trends in Hopf Algebra Theory, Contemp. Math. 267 (2000) 339–356.

[Ma] S.V. Matveev, Distributive groupoids in knot theory, Mat. Sbornik (N.S.) 119 (1) (1982) 78–88, 160, 161.

[Mo] T. Mochizuki, Some calculations of cohomology groups of Alexander quandles, preprint available at http://math01.sci.osaka-cu.ac.jp/~takuro.

[M] S. Montgomery, Indecomposable coalgebras, simple comodules, and pointed Hopf algebras, Proc. Amer. Math. Soc. 123 (8) (1995) 2343–2351.

[MS] A. Milinski, H.-J. Schneider, Pointed indecomposable Hopf algebras over coxeter groups, in: New Trends in Hopf Algebra Theory, Contemp. Math. 267 (2000) 215–236.

[Ne] S. Nelson, Classification of finite Alexander quandles, math.GT/0202281.

[N] W. Nichols, Bialgebras of type one, Comm. Algebra 6 (15) (1978) 1521–1552.

[Opal] B. Keller, A noncommutative Gröbner basis system, program available at http://people.cs.vt.edu/~keller/opal/.

[O] T. Ohtsuki (Ed.), Problems on Invariants in Knots and 3-Manifolds, preprint available at http://www.ms.u-tokyo.ac.jp/~tomotada/proj01.

[Q] D. Quillen, Homotopical Algebra, in: Lecture Notes in Mathematics, Vol. 43, Springer, Berlin, 1967.

[So] A. Soloviev, Non-unitary set-theoretical solutions to the quantum Yang–Baxter equation, Math. Res. Lett. 7 (5–6) (2000) 577–596.

[Tk] M. Takeuchi, Survey of braided Hopf algebras, in: New Trends in Hopf Algebra Theory, Contemp. Math. 267 (2000) 301–324.