Beiträge zur Algebra und Geometrie
Contributions to Algebra and Geometry
Volume 45 (2004), No. 2, 665-676.

Indecomposable Racks of Order p^2

Matías Graña*

MIT, Mathematics Department, 77 Mass. Ave., 02139 Cambridge, MA - USA
Permanent address: Depto. de Matemática, FCEyN - UBA Pab. I, Ciudad Universitaria
1428–Buenos Aires, Argentina
e-mail: matiasg@math.mit.edu

Abstract. We classify indecomposable racks of order p^2 (p a prime). There are $2p^2-2p-2$ isomorphism classes, among which $2p^2-3p-1$ correspond to quandles. In particular, we prove that an indecomposable quandle of order p^2 is affine. As an ingredient of the classification, we prove that the quandle non-abelian second cohomology set of an indecomposable quandle of prime order is trivial.

MSC 2000: 16W30, 57M27

1. Introduction

Racks and quandles have been considered by G. Wraith and J. Conway in 1959 as a generalization of a group with the binary operation given by conjugation. Since then, they appeared once and again in topological contexts (cf. [12, 17, 13, 9, 4]), in logics (cf. [5]), in algebra (cf. [3, 8, 14, 10]).

In topology they were mainly used to provide invariants for knots: any knot has attached a quandle (the *knot quandle*), which is a full invariant up to mirror symmetry (two knots with isomorphic quandles are either isotopic or one is isotopic to a mirror image of the other). This was the fact that attracted the attention of knot theorists to them at first. A generalization of the classic invariant of "colorings" of a knot is given by counting how many quandle homomorphisms there are from the quandle of a knot to a given fixed quandle. A refinement of this invariant is given by taking a 2-cocycle of this fixed quandle with values in an abelian group, and using it to give a "weight" to each homomorphism (similar ideas, with

*This work was supported by CONICET

3-cocycles, were used to give invariants of knotted surfaces, cf. [4]). One of the advantages of this last invariant is that it detects mirror symmetry.

More recently, led by his interest in Homotopical Quantum Field Theories, Turaev introduced in [21] the concept of *crossed categories*. These are monoidal categories which split as a disjoint union of a family of subcategories. This family is indexed by a group, and each element of the group gives, in turn, an endofunctor in the whole category which, at the level of the splitting, behaves like conjugation. If one considers set-theoretical versions of crossed categories, one is immediately led to the notion of a rack.

On the other hand, in [8, 7, 20] and [14, 15] the authors attack a problem proposed by Drinfeld: that of giving set-theoretical solutions to the Yang-Baxter equation. They find that racks not only give a good set of solutions, but that each "good" solution (namely, faithful and non-degenerate, in the words of [20]) has a rack attached. Studying this rack one can have information about the solution. In particular, in [7] Etingof, Guralnick and Soloviev classify indecomposable, faithful, non-degenerate set-theoretical solutions of the Yang-Baxter equation with a prime number of elements. They do so by studying the enveloping group of the attached rack.

Studying the internal structure of modules over the Drinfeld double of a finite group and their relation to pointed Hopf algebras, in [10] I proposed a cohomology theory for racks and quandles, which turned out to be the same as the one considered by knot theorists. A non-abelian version of these theories gives rise to extensions of quandles, cf. [1]. With this help we can pursue the next step in the seemingly wild project of classification of (isomorphism classes) of finite racks. As said before, indecomposable racks of prime order are classified. We classify here indecomposable racks of prime square order. This classification can be used to give new concrete (as opposed to theoretical) invariants of knots and knotted surfaces (some of the racks classified here were indeed used in [16]), to give new solutions to the Yang-Baxter equation (both set-theoretical and "classical"), new set-theoretical versions of Turaev's crossed categories, new examples of pointed Hopf algebras.

2. Definitions and notation

Let us define the object of study:

Definition 2.1. *A rack is a pair $(X, \triangleright)$, where X is a set and $\triangleright\colon X \times X \to X$ is a binary operation satisfying:*

$$\text{The functions } \phi_x : X \to X,\ \phi_x(y) = x \triangleright y \text{ are bijections for all } x \in X, \tag{2.2}$$

$$x \triangleright (y \triangleright z) = (x \triangleright y) \triangleright (x \triangleright z) \quad \forall x, y, z \in X. \tag{2.3}$$

A rack is a quandle if it further satisfies

$$x \triangleright x = x \quad \forall x \in X. \tag{2.4}$$

The main model for racks are unions of conjugacy classes in a group, where the operation is the conjugation $x \triangleright y = xyx^{-1}$. Notice that a rack like this is actually a quandle. As far as the author knows, the problem of finding a necessary and sufficient condition for a quandle to be isomorphic to a union of conjugacy classes in a group is still open.

Definition 2.5. *A rack* $(X, \triangleright)$ *is decomposable if it can be split properly into stable subracks, i.e., if* $X = Y \sqcup Z$ *(a disjoint union), neither of them empty, and* $X \triangleright Y = Y$, $X \triangleright Z = Z$. *A rack is indecomposable if it is not decomposable.*

For X a set, we denote by $\mathbb{S}_X$ the symmetric group $\mathbb{S}_X = \{f : X \to X \mid f \text{ is bijective}\}$. Let X be a rack and let $\phi : X \to \mathbb{S}_X$, $\phi(x) = \phi_x$, (see (2.2)). We denote by G_X^0 the subgroup of $\mathbb{S}_X$ generated by the image of ϕ. This group operates on X by rack automorphisms; i.e., if $\sigma \in G_X^0$ then $\sigma(x \triangleright y) = \sigma(x) \triangleright \sigma(y)$. Moreover, ϕ is a rack homomorphism taking the conjugation in G_X^0.

A rack is called *faithful* if ϕ is injective. In this case, X, being isomorphic as a rack to its image, is naturally seen as a union of conjugacy classes inside G_X^0, and then it is a quandle. If X is a rack, we denote by $\mathrm{Aut}(X)$ the group of rack automorphisms of X.

A rack X is said to be *trivial*, or *abelian*, if ϕ is trivial, i.e., if $x \triangleright y = y \ \forall x, y$. A rack X is said to be *simple* if (a) X is not trivial, and (b) any surjective rack homomorphism $X \to Y$ is either an isomorphism or $|Y| = 1$. An example of a simple rack is, for p a prime number, $(\mathbb{Z}_p, \triangleright)$, $x \triangleright y = y + 1$. It is not difficult to see that a simple rack is either isomorphic to one of these, or it is a quandle. Simple quandles are classified in [1] in terms of simple groups.

An *affine quandle* (also called *Alexander quandle*) is a pair (A, g), where A is an abelian group and $g \in \mathrm{Aut}(A)$. Then A is a quandle with the structure $x \triangleright y = (1 - g)(x) + g(y)$ $(x, y \in A)$. It is easy to see that such a quandle is indecomposable iff $1 - g$ is surjective and it is faithful iff $1 - g$ is injective. If A is cyclic, we denote g usually by $g(1)$.

Theorem 2.6. ([7]) *An indecomposable quandle of prime order p is affine, isomorphic to* $(\mathbb{Z}_p, q)$, *where* $q \in \mathbb{Z}_p^* - \{1\}$.

Here, and throughout, for a ring R we denote by R^* the group of its units.

If X is a quandle and H is a group, the *(non-abelian)* 2*-cocycles with values in* H are the functions $\beta : X \times X \to H$ such that

$$\beta(x, y \triangleright z)\beta(y, z) = \beta(x \triangleright y, x \triangleright z)\beta(x, z) \quad \forall x, y, z \in X.$$

We denote by $Z^2(X, H)$ the set of 2-cocycles with values in H. Two 2-cocycles β and β' are *cohomologous* if there exists a function $\gamma : X \to H$ such that

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

We denote by $H^2(X, H)$ the set of cohomology classes of 2-cocycles. A non-abelian 2-cocycle is said to be a *quandle cocycle* if $\beta(x, x) = 1 \ \forall x \in X$. We denote by $H_Q^2(X, H)$ the set of cohomology classes of quandle 2-cocycles.

If X is a rack, S is a set and $\beta : X \times X \to \mathbb{S}_S$ is a 2-cocycle, then there is a structure of rack in the product $X \times S$, given by

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

We denote by $X \times_\beta S$ the rack with this structure. Two cohomologous cocycles give rise to isomorphic structures. If X is a quandle then $X \times S$ is a quandle iff β is a quandle cocycle.

More general extensions are obtained by dynamical 2-cocycles. If $(X, \triangleright)$ is a rack and S is a set, a function $\alpha : X \times X \times S \to \mathbb{S}_S$ is called *dynamical* 2*-cocycle* if the set $X \times S$ is a rack under the operation $(x, s) \triangleright (y, t) = (x \triangleright y, \alpha(x, y, s)(t))$. A non-abelian cocycle β gives a dynamical cocycle by taking $\alpha(x, y, s) = \beta(x, y)$. See [1] for a detailed treatment of dynamical cocycles.

Let X be a rack, let $\iota : X \to X$ be defined by $x \triangleright \iota(x) = x$. Define $(X, \triangleright^\iota)$ as X with the structure $x \triangleright^\iota y = x \triangleright \iota(y)$. It can be seen that ι is a bijection and $(X, \triangleright^\iota)$ is a quandle. Notice that $x \triangleright (\iota(x) \triangleright z) = (x \triangleright \iota(x)) \triangleright (x \triangleright z) = x \triangleright (x \triangleright z)$, whence $\phi_x = \phi_{\iota(x)}$.

For an integer n, we denote its p-valuation by $v_p(n)$, i.e., $v_p(n) = r$ if $n = p^r q$ where q is coprime to p.

3. Racks of order p^2

Theorem 3.1. *Let X be an indecomposable rack of order p^2, p a prime number. Then X is isomorphic to one of the racks in this list:*

$$\mathbb{Z}_p \oplus \mathbb{Z}_p, \quad (x_1, x_2) \triangleright (y_1, y_2) = ((1-\alpha)x_1 + \alpha y_1, (1-\beta)x_2 + \beta y_2) \qquad \alpha, \beta \in \mathbb{Z}_p^* - \{1\} \tag{3.2}$$

$$\mathbb{Z}_p \oplus \mathbb{Z}_p, \quad (x_1, x_2) \triangleright (y_1, y_2) = ((1-\alpha)x_1 + \alpha y_1, (1-\alpha)x_2 + \alpha y_2 + y_1 - x_1) \qquad \alpha \in \mathbb{Z}_p^* - \{1\} \tag{3.3}$$

$$\mathbb{F}_{p^2}, \quad x \triangleright y = (1-\alpha)x + \alpha y \qquad \alpha \in \mathbb{F}_{p^2} - \mathbb{F}_p \tag{3.4}$$

$$\mathbb{Z}_{p^2}, \quad x \triangleright y = (1-\alpha)x + \alpha y \qquad \alpha \not\equiv 0, 1 \mod p \tag{3.5}$$

$$\mathbb{Z}_{p^2}, \quad x \triangleright y = y + 1 \tag{3.6}$$

$$\mathbb{Z}_p \oplus \mathbb{Z}_p, \quad (x_1, x_2) \triangleright (y_1, y_2) = ((1-\alpha)x_1 + \alpha y_1, y_2 + 1) \qquad \alpha \in \mathbb{Z}_p^* - \{1\} \tag{3.7}$$

Two racks in different rows are not isomorphic. The non-trivial isomorphisms inside each row are as follows: in (3.2)*, the rack associated to (α, β) is isomorphic to that associated to (β, α); in* (3.4) *the rack associated to α is isomorphic to that associated to $\sigma(\alpha)$, where σ is the non-trivial element of the Galois group* $\mathrm{Gal}(\mathbb{F}_{p^2}|\mathbb{F}_p)$*.*

Proof. If X is faithful then X is a quandle and we prove in 3.10 below that it is affine. If X is not faithful, then we consider its associated quandle $(X, \triangleright^\iota)$, which is also non-faithful. Then $\phi(X)$ has order either 1 or p. In the first case $(X, \triangleright^\iota)$ is trivial, and then $(X, \triangleright)$ is given by a permutation $\sigma \in \mathbb{S}_{p^2}$: $x \triangleright y = \sigma(y)$. Since $(X, \triangleright)$ is indecomposable, σ must be a p^2-cycle. Then it is of the form (3.6). In the second case, we have by [1, Prop. 2.11] that $(X, \triangleright^\iota)$ is a non-abelian extension of $\phi(X)$ by some set S of order p, i.e., $(X, \triangleright^\iota) \simeq (\mathbb{Z}_p, \alpha) \times_\beta S$ for some β a 2-cocycle in $Z^2((\mathbb{Z}_p, \alpha), \mathbb{S}_S)$. By Lemma 6.1 below, β is cohomologous to the trivial cocycle, and hence we may assume that β is trivial, i.e., $(x, s) \triangleright^\iota (y, t) = ((1-\alpha)x + \alpha y, t)$. Since $\phi_x = \phi_{\iota x}$, we have that ι restricts to the fibers, i.e., $\iota|_{\{x\} \times S} : \{x\} \times S \to \{x\} \times S$. Let $\iota_x : S \to S$, $x \times \iota_x(s) = \iota|_{\{x\} \times S}(x \times s)$. The structure in X can be recovered from $\triangleright^\iota$ as $(x, s) \triangleright (y, t) = (x, s) \triangleright^\iota (\iota^{-1}(y, t)) = ((1-\alpha)x + \alpha y, \iota_y^{-1}(t))$. Now, it is easy to see that (2.3) implies $\iota_{y \triangleright z}^{-1} \iota_z^{-1} = \iota_{x \triangleright z}^{-1} \iota_z^{-1}$ $\forall x, y, z \in (\mathbb{Z}_p, \alpha)$, and thus $\iota_x^{-1} = \iota_y^{-1}$ $\forall x, y$. We can call then $f = \iota_x^{-1}$, and we have $(x, s) \triangleright (y, t) = (x \triangleright y, f(t))$. But for this rack to be indecomposable f must be a p-cycle whence X is isomorphic to a rack in (3.7).

To see that (3.2), (3.3), (3.4), (3.5) cover all the affine cases, simply notice that there are two groups of order p^2: $\mathbb{Z}_p \oplus \mathbb{Z}_p$ and $\mathbb{Z}_{p^2}$. For $\mathbb{Z}_p \oplus \mathbb{Z}_p$ the isomorphism $g \in \mathrm{GL}_2(\mathbb{Z}_p)$ can be either diagonalizable (class (3.2)), it can be given by a Jordan block (class (3.3)) or its minimal polynomial can be irreducible over $\mathbb{Z}_p$ (class (3.4)). For $\mathbb{Z}_{p^2}$ any automorphism is given by an element in $\mathbb{Z}_{p^2}^*$, and we get class (3.5). The conditions on α and β in the statement are equivalent for these quandles to be indecomposable.

Now, by [1, Lemma 1.33] two indecomposable affine quandles (A, g) and (B, h) are isomorphic iff there is an isomorphism of the pairs (A, g) and (B, h); i.e., iff there exists an isomorphism $T : A \to B$ such that $Tg = hT$. This proves that the classes have no intersection and shows also that the isomorphisms inside each class are those in the statement. □

Before dealing with the rest of the proof, we derive two corollaries:

Corollary 3.8. *If X is an indecomposable rack of order p^2 then $v_p(|G_X^0|) = 2$ or 3.*

Proof. For affine quandles, it is a consequence of [1, Cor. 1.25]. For the other cases, it follows by inspection. □

Corollary 3.9. *The cardinalities of the classes in 3.1 are as follows:*

Type	*Class*	#
Affine quandle over $\mathbb{Z}_p^2$; diagonalizable isomorphism	(3.2)	$\frac{1}{2}(p^2 - 3p + 2)$
Affine quandle over $\mathbb{Z}_p^2$; Jordan block	(3.3)	$p - 2$
Affine quandle over $\mathbb{Z}_p^2$; irreducible polynomial (simple)	(3.4)	$\frac{1}{2}p(p - 1)$
Affine quandle over $\mathbb{Z}_{p^2}$	(3.5)	$p^2 - 2p$
Rack which is not a quandle with $|\phi(X)| = 1$	(3.6)	1
Rack which is not a quandle with $|\phi(X)| = p$	(3.7)	$p - 2$

□

We now finish the proof of 3.1.

Proposition 3.10. *Indecomposable quandles of order p^2 are affine. In particular, they are faithful.*

Proof. Since for $p = 2$ this is known, we may assume that $p \neq 2$ (the tools used here work also for the case $p = 2$, though sometimes the formulas are easier if we have $\frac{1}{2} \in \mathbb{Z}_p$).

For simple quandles the result is a consequence of [1, Thm. 3.12]. Let X be an indecomposable non-simple quandle of order p^2. Then by [1, Cor. 2.10] we have $X \simeq Y \times_\alpha S$, where Y is an indecomposable quandle of order p, S is a set of order p and α is a dynamical 2-cocycle. For $y \in Y$, let us denote by X_y the fibers $y \times S$. These are quandles, and, since Y is indecomposable, they are all isomorphic, i.e., $X_y \simeq X_{y'}$ as quandles. We claim that either X_y is indecomposable or it is trivial. To see this, take for each $y \in Y$ the decomposition $X_y = \sqcup_n X_y^n$, where X_y^n is the union of the orbits of X_y with cardinality n. Take $(y, s) \in X$; since $\phi_{(y,s)} : X_z \to X_{y \triangleright z}$ is a quandle isomorphism, it must send X_z^n to $X_{y \triangleright z}^n$. Thus, we have a decomposition of X as $X = \sqcup_n(\sqcup_y X_y^n)$. But X is indecomposable, hence all the orbits in X_y (any y) have the same cardinality. And since S has a prime cardinality, either there is one orbit of order p (and X_y is indecomposable) or there are p orbits of order 1 (and X_y is trivial), proving the claim.

We suppose first that X is faithful. By [7, Thm. A.2] the group G_X^0 is an extension of a cyclic group by a p-group. That is, $G_X^0 = N \rtimes_f C$, N a p-group, C cyclic and f a 2-cocycle. Let M be the order of C and let t be a generator of it. We have the structure $(a, t^i)(b, t^j) = (a\alpha^i(b)f(i, j), t^{i+j})$, where $f(i, j) = 1 \in N$ if $i + j < M$ and t acts by α on N. Since X is indecomposable, the image of ϕ is contained in $\{(a, t^i) \mid i = i_0\}$ for some i_0. As this image must generate G_X^0, we can assume that $i_0 = 1$ (otherwise we re-name t to t^{i_0}). The structure of X is given then by

$$(a, t) \triangleright (b, t) = (a, t)(b, t)(a, t)^{-1} = (a, t)(b, t)(1, t)^{-1}(a^{-1}, 1) = (a\alpha(ba^{-1}), t). \tag{3.11}$$

Furthermore, G_X^0 has trivial center; in particular if $g \in Z(N)$ then $\alpha(g) \neq g$, and, since any p group has a non-trivial center, $\alpha \neq \mathrm{id}$. Thus, to classify X we can seek what pairs N, α can arise and then look for the structure of the orbits for the action $a \triangleright b = a\alpha(ba^{-1})$. The strategy of the proof in [7] is the same as this one; however in that case X can be seen as an orbit in the symmetric group $\mathbb{S}_p$ (actually, the faithfulness condition is immediate), whence $1 \leq v_p(|N|) \leq v_p(|\mathbb{S}_p|) = 1$; thus $N \simeq \mathbb{Z}_p$. With a similar reasoning we can prove that $v_p(|N|) \leq v_p(|\mathbb{S}_{p^2}|) = p + 1$, but this gives too much freedom to N. However, the group N is rather small: we claim that $|N| \leq p^3$. To see this, if X_y is indecomposable we have by [7] that it is affine and $v_p(|\operatorname{Aut}(X_y)|) = v_p(|\mathbb{Z}_p \rtimes \mathbb{Z}_p^*|) = 1$. If X_y is not indecomposable, we have that it is trivial and then $v_p(|\operatorname{Aut}(X_y)|) = v_p(|\mathbb{S}_{X_y}|) = 1$. Since X is indecomposable, Y is indecomposable and again $v_p(|G_Y^0|) = 1$. By [1, Lemma 1.13] we have a morphism of groups $G^0(\pi) : G_X^0 \to G_Y^0$ induced by the projection $\pi : X \to Y$. We look to its kernel $K = \ker G^0(\pi)$. By an abuse of notation, we denote the elements of Y by those of $\mathbb{Z}_p$. Let $w \in K$, we have $w(X_y) = X_y\ \forall y \in Y$. Then we can restrict w to X_0 and X_1, i.e., we have a homomorphism of groups $R : K \to \operatorname{Aut}(X_0) \times \operatorname{Aut}(X_1)$. But $X_0 \cup X_1$ generates X as a quandle, since 0 and 1 generate Y. Then R is injective, which proves that the order of K divides that of $\operatorname{Aut}(X_0) \times \operatorname{Aut}(X_1) \subseteq \operatorname{Aut}(\mathbb{S}_{X_0}) \times \operatorname{Aut}(\mathbb{S}_{X_1})$. Then $v_p(|K|) \leq 2 \times v_p(|\operatorname{Aut}(\mathbb{S}_{X_0})|) = 2$, and $v_p(|G_X|) \leq v_p(|K|) + v_p(|G_Y|) \leq 3$, proving the claim.

If N is abelian we are done, since in this case (3.11) defines an affine structure. Thus, if N has order p or p^2, there is nothing else to prove. The classification of groups of order p^3 is well known (cf. [2]); there are 3 abelian groups and two groups which are not abelian. We must concentrate the attention on the later. We prove in sections 4 and 5 that for each of them we get affine quandles.

Suppose now that X is not faithful. The image of $\phi : X \to G_X^0$ must have order p, since otherwise X would be trivial. Let $Y = \phi(X)$; as before it is an indecomposable quandle and then $Y \simeq (\mathbb{Z}_p, q)$, where $q \in \mathbb{Z}_p^* - \{1\}$. By [1, Prop. 2.11], we have $X = Y \times_\beta S$, where S is a set of order p and $\beta : Y \times Y \to \mathbb{S}_S$ is a non-abelian quandle 2-cocycle. Now, we prove in 6.1 that this set is trivial; whence any of these quandles is isomorphic to the product $Y \times S$, S a trivial quandle; but this implies that $Y \times S$ is decomposable. $\square$

4. The group $(\mathbb{Z}_p \oplus \mathbb{Z}_p) \rtimes C_p$

Let $G = (\mathbb{Z}_p \oplus \mathbb{Z}_p) \rtimes C_p$ be the group with t a generator of C_p acting on $\mathbb{Z}_p \oplus \mathbb{Z}_p$ by $t(x,y)t^{-1} = (x, x+y)$. We denote the elements of G as $(x,y)t^z$ $x,y,z \in \mathbb{Z}_p$. Let $\alpha \in \mathrm{Aut}(G)$. As $(0,1)$ generates the center of G, we must have $\alpha(0,1) = (0,q)$ for some $q \in \mathbb{Z}_p^*$, and since α must act non-trivially on the elements of the center, $q \neq 1$. We denote $\alpha((1,0)) = (a,j)t^b$, $\alpha(t) = (c,k)t^d$. We have $\alpha((x,y)) = ((a,j)t^b)^x(0,yq) = (xa, xj + ab\frac{x(x-1)}{2} + yq)t^{bx}$ and $\alpha(t^z) = ((c,k)t^d)^z = (zc, zk + cd\frac{z(z-1)}{2})t^{dz}$, whence

$$\alpha((x,y)t^z) = (xa + zc\ ,\ bcxz + xj + zk + ab\frac{x(x-1)}{2} + cd\frac{z(z-1)}{2} + yq)t^{bx+dz}.$$

It is easy to check that for α to be a group homomorphism we must have $q = da - bc$.

As said, for $h \in G$, we consider the orbits $\mathcal{O}_h$ under the action $g \triangleright h = g\alpha(hg^{-1})$. We seek the conditions on α that give orbits of order p^2. Take $g = 1$; we get that $\{\alpha^n(h) \mid 0 \leq n < N\} \subseteq \mathcal{O}_h$. Take $g = (0,y)$ and notice that $(0,y) \triangleright h = (0,y)\alpha(h)(0,-qy) = \alpha(h)(0,(1-q)y)$. Then $\{\alpha^n(h)(0,*)\} \subseteq \mathcal{O}_h$. Let us compute the orbit of $\zeta = (0,1)$. We have $\{(0,*)\} \subseteq \mathcal{O}_\zeta$. Acting by $(-x,0)t^{-z}$, we get

$$\begin{aligned}(-x,0)t^{-z} \triangleright (0,*) &= (-x,0)t^{-z}\alpha((0,*)t^z(x,0)) = (-x,0)t^{-z}\alpha((x,*)t^z)\\ &= (-x,0)t^{-z}(xa + zc, *)t^{bx+dz} = ((a-1)x + cz, *)t^{bx+(d-1)z}.\end{aligned}$$

Let $A = \left(\begin{smallmatrix} a & c \\ b & d\end{smallmatrix}\right)$. We get that $\mathcal{O}_\zeta = G$ if $A-1$ is invertible. We assume thus that $A-1$ is degenerate. It can be seen that if $A = 1$, then all the orbits have order p. Thus, we consider $A \neq 1$.

Suppose that the first row of $A-1$ is non-trivial. Then $A = \left(\begin{smallmatrix} r+1 & s \\ ur & us+1\end{smallmatrix}\right)$ for some $r,s,u \in \mathbb{Z}_p$, $(r,s) \neq (0,0)$. We compute the orbit of $(\lambda, *)$:

$$\begin{aligned}(-x,0)t^{-z} \triangleright (\lambda,*)t^\mu &= (-x,0)t^{-z}((r+1)(\lambda+x) + s(\mu+z), *)t^{ur(\lambda+x)+(us+1)(\mu+z)}\\ &= ((\lambda r + xr + \mu s + zs) + \lambda, *)t^{u(\lambda r + xr + \mu s + zs)+\mu},\end{aligned}$$

whence the orbits are characterized as $\mathcal{O}^C := \{(\nu,\sigma)t^\tau \mid \tau - u\nu = C\}$, and they have order p^2, as wanted.

If the first row of $A-1$ is trivial we have $A = \left(\begin{smallmatrix} 1 & 0 \\ r & s+1\end{smallmatrix}\right)$, $(r,s) \neq (0,0)$, and the orbits are

$$\begin{aligned}(-x,0)t^{-z} \triangleright (\lambda,*)t^\mu &= (-x,0)t^{-z}(\lambda + x, *)t^{r(\lambda+x)+(s+1)(\mu+z)}\\ &= (\lambda, *)t^{r\lambda + rx + s\mu + sz + \mu},\end{aligned}$$

whence the orbits are characterized as $\mathcal{O}^C := \{(\lambda,\sigma)t^\tau \mid \lambda = C\}$, also of order p^2.

We compute now the rack structure of the orbits $\mathcal{O}^C$ in these cases. We do it first for the case $A = \left(\begin{smallmatrix} r+1 & s \\ ur & us+1\end{smallmatrix}\right)$. Let $\Delta_x = \bar{x} - x$, $\Delta_y = \bar{y} - y$. Notice that $q = 1 + r + us$. A straightforward computation shows that in $\mathcal{O}^C$:

$$\begin{aligned}&((x,y)t^{C+ux}) \triangleright ((\bar{x},\bar{y})t^{C+u\bar{x}})\\ &\quad = (x,y)t^{C+ux}\alpha((\bar{x},\bar{y})t^{u(\bar{x}-x)}(-x,-y))\\ &\quad = (q\Delta_x + x\ ,\ \Delta_x^2(\frac{u}{2}rq + \frac{u^2}{2}sq) + \Delta_x(j + uk - \frac{u}{2}(r+1)r - \frac{u}{2}s(us+1) + Cq)\\ &\qquad + q\Delta_y + y)\ t^{uq\Delta_x + C + ux}.\end{aligned}$$

Now we use the following bijection: $f : \mathcal{O}^C \to \mathbb{Z}_p \oplus \mathbb{Z}_p$, $f((x,y)t^{ux+C}) = (x, y - u\frac{x(x-1)}{2})$. We compute then the quandle structure of $\mathcal{O}^C$ transported to $\mathbb{Z}_p \oplus \mathbb{Z}_p$ by f. It is easy to see that

$$\begin{aligned} f(f^{-1}(x,y) \triangleright f^{-1}(\bar{x},\bar{y})) &= f((x, y + u\frac{x(x-1)}{2})t^{ux+C} \triangleright (\bar{x}, \bar{y} + u\frac{\bar{x}(\bar{x}-1)}{2})t^{u\bar{x}+C}) \\ &= f((q\Delta_x + x\ ,\ \Delta_x^2(\frac{u}{2}rq + \frac{u^2}{2}sq)\Delta_x(j + uk - \frac{u}{2}(r+1)r - \frac{u}{2}s(us+1) + Cq) \\ &\quad + q\Delta_y + y + \frac{u}{2}q(\bar{x}^2 - \bar{x} - x^2 + x) + \frac{u}{2}x(x-1))t^{uq\Delta_x + C + ux}) \\ &= (q\Delta_x + x\ ,\ q\Delta_y + y + \Delta_x(j + uk - \frac{u}{2}qr + \frac{u}{2}usr - \frac{u}{2}sq + \frac{u}{2}sr + Cq)). \end{aligned}$$

This means that $\mathcal{O}^C$ is isomorphic to the affine quandle $(\mathbb{Z}_p \oplus \mathbb{Z}_p, g)$, where

$$g(x,y) = (qx, qy + (j + uk - \frac{u}{2}qr + \frac{u}{2}usr - \frac{u}{2}sq + \frac{u}{2}sr + Cq)x).$$

We consider now the case $A = \left(\begin{smallmatrix} 1 & 0 \\ r & s+1 \end{smallmatrix}\right)$. Notice that here $q = s+1$. Let $\Delta_z = \bar{z} - z$. We have for the orbit $\mathcal{O}^C$:

$$\begin{aligned} (C,y)t^z \triangleright (C,\bar{y})t^{\bar{z}} &= (C,y)t^z\alpha((C,\bar{y})t^{\bar{z}-z}(-C,-y)) = (C,y)t^z\alpha((0, \Delta_y - \Delta_z C)t^{\Delta_z}) \\ &= (C,y)t^z(0, \Delta_z k + q\Delta_y - Cq\Delta_z)t^{(s+1)\Delta_z} \\ &= (C, q\Delta_y + y + \Delta_z(k - Cq))t^{q\Delta_z + z}. \end{aligned}$$

Then, taking the bijection $f : \mathcal{O}^C \to \mathbb{Z}_p \oplus \mathbb{Z}_p$ given by $f((C,y)t^z) = (y,z)$ we get on $\mathbb{Z}_p \oplus \mathbb{Z}_p$ the affine quandle $(\mathbb{Z}_p \oplus \mathbb{Z}_p, g)$ with g given by $g(y,z) = (qy + (k - Cq)z, qz)$.

In both cases, we get an affine quandle.

5. The group $\mathbb{Z}_{p^2} \rtimes C_p$

Let $G = \mathbb{Z}_{p^2} \rtimes C_p$, where C_p is generated by t and the action is given by $tat^{-1} = a(p+1)$. Notice that $(at^b)^n = a(n + pb\frac{n(n-1)}{2})t^{bn}$. In particular (at^b) has order p iff $p|a$.

Take $\alpha \in \mathrm{Aut}(G)$, $\alpha(1) = at^b$, $\alpha(t) = ct^d$. Let us compute the conditions on a, b, c, d for α to be a homomorphism. It is easy to check that $\alpha(t)\alpha(1) = \alpha(1+p)\alpha(t)$ implies that either $pad = pa + pbc \mod p^2$, or $a(d-1) = bc \mod p$. On the other hand, $\alpha(t)$ must have order p, whence $c = 0 \mod p$. This means that either $a = 0 \mod p$ or $d = 1 \mod p$. The first possibility is excluded since $\alpha(1)$ must have order p^2. Then, $d = 1$ and $\alpha(t) = (pc')t$. Thus,

$$\begin{aligned} \alpha(nt^m) &= (at^b)^n(pc't)^m = (a(n + pb\frac{n(n-1)}{2}))t^{bn}(pc'm)t^m \\ &= (an + pab\frac{n(n-1)}{2} + pc'm(1 + pbn))t^{bn+m} = (an + p(ab\frac{n(n-1)}{2} + c'm))t^{bn+m}. \end{aligned}$$

It is thus straightforward to check that, taking $\Delta_n = \bar{n} - n$ and $\Delta_m = \bar{m} - m$, we have

$$\begin{aligned} (nt^m) \triangleright (\bar{n}t^{\bar{m}}) &= (nt^m)\alpha(\bar{n}t^{\Delta_m}(-n)) \\ &= (\bar{n} - (1-a)\Delta_n + p(c'\Delta_m + a(-\Delta_m\bar{n} + \Delta_n\bar{m}) \\ &\quad + ab\frac{\Delta_n(\Delta_n - 1)}{2}))t^{b\Delta_n + \bar{m}}. \end{aligned}$$

We write now $n = r + ps$ ($p \nmid r$), and $D = \bar{n} - r$, and we get

$$\begin{aligned}(nt^m) \triangleright (\bar{n}t^{\bar{m}}) &= (\bar{n} - (1-a)D + p((1-a)s + c'\Delta_m + a(-\Delta_m\bar{n} + D\bar{m}) \\ &\quad + ab\frac{D(D-1)}{2}))t^{bD+\bar{m}} \\ &= (\bar{n} - (1-a)D + p((1-a)s + (c' - a\bar{n})\Delta_m + aD\bar{m} \\ &\quad + ab\frac{D(D-1)}{2}))t^{bD+\bar{m}}.\end{aligned} \tag{5.1}$$

Suppose first that $a \neq 1 \mod p$ and put $C = \bar{m} - \frac{b}{a-1}\bar{n}$. We have

$$\mathcal{O}_{\bar{n}t^{\bar{m}}} \subseteq \mathcal{O}^C := \{xt^{\frac{b}{a-1}x+C} \mid x \in \mathbb{Z}_{p^2}\}.$$

Thus, all orbits have order $\leq p^2$. On the other hand, by (5.1), all orbits have order $\geq p^2$, and then they coincide with the sets $\mathcal{O}^C$. We look to the rack structure in the orbit $\mathcal{O}^C$. Put $\Delta_x = \bar{x} - x$;

$$\begin{aligned}xt^{\frac{-b}{1-a}x+C} \triangleright \bar{x}t^{\frac{-b}{1-a}\bar{x}+C} &= (\bar{x} - (1-a)\Delta_x + p(c'\frac{-b}{1-a}\Delta_x + a(\frac{b}{1-a}\Delta_x\bar{x} \\ &\quad - \Delta_x\frac{b}{1-a}\bar{x} + \Delta_x C) + ab\frac{\Delta_x(\Delta_x - 1)}{2}))t^{b\Delta_x - \ frac b1-a\bar{x}+C} \\ &= (\bar{x} - (1-a)\Delta_x + p((\frac{-bc'}{1-a} + aC - \frac{ab}{2})\Delta_x + \frac{ab}{2}\Delta_x^2))t^{b\Delta_x - \frac{b}{1-a}\bar{x}+C}.\end{aligned}$$

Consider now the function

$$f : \mathbb{Z}_{p^2} \to G, \quad f(x) = (x - p\frac{b}{1-a}\frac{x(x-1)}{2})t^{\frac{-b}{1-a}x+C}.$$

We translate the structure of $\mathcal{O}^C$ to $\mathbb{Z}_{p^2}$ via f. We have $f^{-1}(xt^{\frac{-b}{1-a}x+C}) = x + p\frac{b}{1-a}\frac{x(x-1)}{2}$, and then one can check that

$$\begin{aligned}f^{-1}(f(x) \triangleright f(\bar{x})) &= f^{-1}((\bar{x} - (1-a)\Delta_x + p(-\frac{b}{1-a}\frac{\bar{x}(\bar{x}-1)}{2} + \frac{b}{2}(\bar{x}^2 - \bar{x} - x^2 + x) \\ &\quad + (\frac{-bc'}{1-a} + aC - \frac{ab}{2})\Delta_x + \frac{ab}{2}\Delta_x^2))t^{b\Delta_x - \frac{b}{1-a}\bar{x}+C}) \\ &= \bar{x} - (1-a)\Delta_x + p\Delta_x(\frac{-bc'}{1-a} + aC - \frac{ab}{2}).\end{aligned}$$

Thus, $\mathcal{O}^C$ is affine, isomorphic to $(\mathbb{Z}_{p^2}, g)$, with $g(x) = (a + p(\frac{-bc'}{1-a} + aC - \frac{ab}{2}))x$.

Suppose now that $a = 1 \mod p$ and put $C = \bar{n}$. We have

$$\mathcal{O}_{\bar{n}t^{\bar{m}}} \subseteq \mathcal{O}^C := \{(C + px)t^y \mid x, y \in \mathbb{Z}_p\}.$$

By (5.1), for the orbit $\mathcal{O}_{\bar{n}t^{\bar{m}}}$ to be of order p^2, we must have $b \neq 0$ and $c' - \bar{n} = c' - a\bar{n} \neq 0 \mod p$. We look to the rack structure in $\mathcal{O}^C$. Put $\Delta_y = \bar{y} - y$; from (5.1) we get (notice that $D = 0$)

$$(C + px)t^y \triangleright (C + p\bar{x})t^{\bar{y}} = (C + p(\bar{x} + (c' - C)\Delta_y))t^{\bar{y}}.$$

But this shows that $\mathcal{O}^C$ is in this case decomposable as $\sqcup_y \mathcal{O}^C_y$, with $\mathcal{O}^C_y = \{(C + px)t^y \mid x \in \mathbb{Z}_p\}$, and we are not dealing with this case.

Therefore, an indecomposable rack with $G^0_X \simeq \mathbb{Z}_{p^2} \rtimes C_p$ is affine.

6. Non-abelian cohomology of the quandle $(\mathbb{Z}_p, q)$

Let $(X, \triangleright) = (\mathbb{Z}_p, q)$, $q \in \mathbb{Z}_p^* - \{1\}$, and let H be a group.

Lemma 6.1. *$H_Q^2(X, H)$ is trivial.*

Proof. Let $\beta : X \times X \to H$ be a quandle non-abelian 2-cocycle. Let $\gamma : X \to H$ be defined by

$$\gamma(x) = \beta(x/(1-q), 0)^{-1}.$$

We deform β by γ, i.e., we take the cohomologous cocycle $\beta'(x,y) = \gamma(x \triangleright y)\beta(x,y)\gamma(y)^{-1}$. We then have

$$\beta'(x,0) = \gamma((1-q)x)\beta(x,0)\gamma(0)^{-1} = \beta(x,0)^{-1}\beta(x,0)\beta(0,0) = 1.$$

Also $\beta'(x,x) = 1\ \forall x \in X$. We then assume that β has these properties. The cocycle condition reads as

$$\beta((1-q)x + qy, (1-q)x + qz)\beta(x,z) = \beta(x, (1-q)y + qz)\beta(y,z).$$

Take $x = -qz/(1-q)$, and get $\beta(-qz + qy, 0)\beta(\frac{-qz}{1-q}, z) = \beta(\frac{-qz}{1-q}, (1-q)y + qz)\beta(y,z)$, i.e.,

$$\beta(\frac{-qz}{1-q}, z) = \beta(\frac{-qz}{1-q}, (1-q)y + qz)\beta(y,z).$$

Take now $y = -qz/(1-q)$, and get $\beta((1-q)x - \frac{q^2 z}{1-q}, (1-q)x + qz)\beta(x,z) = \beta(x,0)\beta(\frac{-qz}{1-q}, z)$, i.e.,

$$\beta((1-q)x - \frac{q^2 z}{1-q}, (1-q)x + qz)\beta(x,z) = \beta(\frac{-qz}{1-q}, z).$$

In particular, $\beta(\frac{-qz}{1-q}, (1-q)x + qz)\beta(x,z) = \beta((1-q)x - \frac{q^2 z}{1-q}, (1-q)x + qz)\beta(x,z)$, and then

$$\beta(\frac{-qz}{1-q}, (1-q)x + qz) = \beta((1-q)x - \frac{q^2 z}{1-q}, (1-q)x + qz).$$

Put now $t = (1-q)x + qz$ and get $\beta(\frac{-qz}{1-q}, t) = \beta(t - qz - \frac{q^2 z}{1-q}, t) = \beta(t - \frac{qz}{1-q}, t)$. Put $s = -qz/(1-q)$ and get

$$\beta(s,t) = \beta(t+s, t) \quad \forall s, t \in X.$$

If $t \neq 0$, then t generates $\mathbb{Z}_p$ and then $\beta(s,t) = \beta(t,t) = 1\ \forall s$. Since for $t = 0$ we have $\beta(s,t) = 1$, we are done. $\square$

Acknowledgments. I thank N. Andruskiewitsch, P. Etingof and V. Turaev for valuable comments. I also thank T. Ohtsuki who, by giving a list of indecomposable quandles of order 9, encouraged me to write this paper. I thank the warm hospitality of MIT and its productive atmosphere in which I wrote the preliminary version of the paper. Finally, I thank the kind invitation of J. Alev and the University of Reims, where I polished it.

References

[1] Andruskiewitsch, N.; Graña, M.: *From racks to pointed Hopf algebras*. Adv. Math. **178**(2) (2003), 177–243. Also in `math.QA/0202084` Zbl 1032.16028

[2] Burnside, W.: *Theory of groups of finite order*. 2nd edition, Dover Pub., New York 1955. Zbl 0064.25105

[3] Brieskorn, E.: *Automorphic sets and braids and singularities*. Braids (Santa Cruz, CA, 1986), Amer. Math. Soc., Providence, RI, Contemp. Math. **78** (1988), 45–115. Zbl 0716.20017

[4] Carter, J. S.: Jelsovsky, D.; Kamada, S.; Langford, L.; Saito, M.: *State-sum invariants of knotted curves and surfaces from quandle cohomology*. Electron. Res. Announc. Amer. Math. Soc. **5** (1999), 146–156 (electronic). Also in `math.GT/9903135`. Zbl 0995.57004

[5] Dehornoy, P.: *Braids and self-distributivity*. Progress in Mathematics **192**. Birkhäuser Verlag, Basel 2000. Zbl 0958.20033

[6] Etingof, P.; Graña, M.: *On rack cohomology*. J. Pure Appl. Algebra **177**(1) (2003), 49–59. Zbl pre01878448

[7] Etingof, P.; Guralnick, R.; Soloviev, A.: *Indecomposable set-theoretical solutions to the Quantum Yang–Baxter Equation on a set with prime number of elements*. J. Algebra **242** (2001), 709–719. Zbl 1018.17007

[8] Etingof, P.; Schedler, T.; Soloviev, A.: *Set-theoretical solutions to the quantum Yang-Baxter equation*. Duke Math. J. **100**(2) (1999), 169–209. Zbl 0969.81030

[9] Fenn, R.; Rourke, C.: *Racks and links in codimension two*. J. Knot Theory Ramifications **1**(4) (1992), 343–406. Zbl 0787.57003

[10] Graña, M.: *On Nichols algebras of low dimension*. In: New Trends in Hopf Algebra Theory. Contemp. Math. **267** (2000), 111–134. Zbl 0974.16031

[11] Graña, M.: *Quandle knot invariants are quantum knot invariants*. J. Knot Theory Ramifications **11**(5) (2002), 673–681. Zbl 1027.57014

[12] Joyce, D.: *A Classifying Invariant of Knots, The Knot Quandle*. J. Pure Appl. Alg. **23** (1982), 37–65. Zbl 0474.57003

[13] Kauffman, L. H.: *Knots and Physics*. World Scientific Pub. Co. (1991, 1994, 2001). Zbl 0868.57001 Zbl pre01666800

[14] Lu, Jiang-Hua; Yan, Min; Zhu, Yong-Chang: *On the set-theoretical Yang-Baxter equation*. Duke Math. J. **104**(1) (2000), 1–18. Zbl 0960.16043

[15] Lu, Jiang-Hua; Yan, Min; Zhu, Yong-Chang: *Quasi-triangular structures on Hopf algebras with positive bases*. New trends in Hopf algebra theory (La Falda, 1999), Amer. Math. Soc., Providence, RI. Contemp. Math. **267** (2000), 339–356. Zbl 0978.16034

[16] Litherland, R.: *Quadratic quandles and their link invariants*. Preprint available at `math.GT/0207099`.

[17] Matveev, S. V.: *Distributive groupoids in knot theory*. Mat. Sb. Nov. Ser. **119** (161) (1982), no. 1, 78–88, 160. Zbl 0523.57006

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

[19] Ohtsuki, T.: *Problems on invariants in knots and* 3*-manifolds*. Preprint available at `http://www.is.titech.ac.jp/~tomotada/proj01/problem.ps`

[20] Soloviev, A.: *Non-unitary set-theoretical solutions to the quantum Yang-Baxter equation*. Math. Res. Lett. **7**(5-6) (2000), 577–596. Zbl 01585085

[21] Turaev, V.: *Homotopy field theory in dimension* 3 *and crossed group-categories*. `math.GT/0005291`.

Received March 31, 2003