CONJUGACY CLASSES OF p-CYCLES OF TYPE D IN ALTERNATING GROUPS

FERNANDO FANTINO

Abstract. We classify the conjugacy classes of p-cycles of type D in alternating groups. This finishes the open cases in [AFGV]. Also we determine all the subracks of those conjugacy classes which are not of type D.

1. Introduction

In the context of the Lifting method [AS], the problem of the classification of finite-dimensional complex pointed Hopf algebras over non-abelian groups can be approached by the study of Nichols algebras associated to pairs (X, q), where X is a rack and q a 2-cocyle, see [AG]. Since the computation of all cocycles of a rack is hard, it is useful to have tools that ensure that the corresponding Nichols algebra $\mathfrak{B}(X, q)$ has infinite dimension for any 2-cocycle q; we say that X *collapses* if this happens. It was shown in [AFGV, Thm. 3.6] that any finite rack of *type D* collapses.

The racks of type D have a nice behavior with respect to monomorphisms and epimorphisms of racks. Indeed, if $Y \subseteq X$ is a subrack of type D, then X is of type D, and if $p : Z \to X$ is an epimorphism of racks with Z finite and X of type D, then Z is of type D. Besides, it is well-known that any finite rack can be decomposed as a union of indecomposable subracks and that every indecomposable rack X admits a projection $X \to Y$ with Y a *simple* rack, i. e. a rack without proper quotients. We recall also that the classification of finite simple racks is known, see [AG] and [Jo].

These facts suggest that the notion of racks of type D is useful for an approach for the classification problem of finite-dimensional pointed Hopf algebras over non-abelian groups and it establish a first step for that problem: to classify finite simple racks of type D, see [AFGaV, §2.6].

One of the most important family of finite simple racks are the conjugacy classes of finite non-abelian (almost) simple groups. In [AFGV], all the conjugacy classes of type D in symmetric and alternating groups were determined, except the conjugacy classes of p-cycles in $\mathbb{A}_p$ and $\mathbb{A}_{p+1}$.

2010 *Mathematics Subject Classification.* 16T05;17B37.

Key words and phrases. Pointed Hopf algebras, Nichols algebras, racks.

This work was partially supported by CONICET, SeCyT - Universidad Nacional de Córdoba, MinCyT, Embassy of France in Argentina and Mairie de Paris.

This article is a contribution to the problem of classification of finite simple racks of type D. Explicitly, we determine when the conjugacy classes of elements of order p, with $p \geq 5$ prime, in the alternating groups $\mathbb{A}_p$ and $\mathbb{A}_{p+1}$ are of type D or not.

We summarize our results in the following statement.

Theorem 1.1. *Let p be a prime number, $p \geq 5$, and $m \in \{p, p+1\}$. Let $\mathcal{O}$ be a conjugacy class of p-cycles in $\mathbb{A}_m$.*

(I) *If $m = p$, then $\mathcal{O}$ is of type D if and only if $p \geq 13$ and $p = \frac{r^k-1}{r-1}$, with r a prime power and k is a natural number.*

(II) *If $m = p+1$, then $\mathcal{O}$ is of type D if and only if $p \geq 7$ and $p = \frac{r^k-1}{r-1}$, with r a prime power and k is a natural number.*

This result finishes the open cases in [AFGV, Thm. 4.1], i. e. it concludes the classification of conjugacy classes of type D in alternating groups.

The family of primes p of the form $\frac{r^k-1}{r-1}$, with r a power of a prime number, contains the Mersenne primes and the Fermat primes. The primes p of this form with $p < 1000$ are: 3, 5, 7, 13, 17, 31, 73, 127, 257, 307 and 757, see Remark 3.1.

2. Preliminaries

Throughout the paper M_{11}, M_{12}, M_{23} and M_{24} denote the corresponding Mathieu simple groups and $L_k(r)$ means the projective special linear group, r a prime power. For $m \in \mathbb{N}$, $\mathbb{G}_m$ denotes the m-th roots of 1 in $\mathbb{C}$.

2.1. A *rack* is a pair $(X, \triangleright)$, where X is a non-empty set and $\triangleright : X \times X \to X$ is a function, satisfying the following conditions: for every $x \in X$, the function $x \triangleright - : X \to X$ is bijective and $x \triangleright (y \triangleright z) = (x \triangleright y) \triangleright (x \triangleright z)$, for all x, y, $z \in X$. Any subset of a group G stable by conjugation is a rack with the conjugation as function $\triangleright$. In particular, a conjugacy class of G is a rack.

A rack $(X, \triangleright)$ is said to be *of type D*[1] if it contains a decomposable subrack $Y = R \coprod S$ such that $r \triangleright (s \triangleright (r \triangleright s)) \neq s$, for some $r \in R$, $s \in S$. It is easy to see that a conjugacy class $\mathcal{O}$ of a group G is a rack of type D if and only if there exist σ, $\tau \in \mathcal{O}$ such that

(Ax. 1) $(\sigma\tau)^2 \neq (\tau\sigma)^2$,

(Ax. 2) σ and τ are not conjugated in $\langle \sigma, \tau \rangle$,

where $\langle \sigma, \tau \rangle$ means the subgroup generated by σ and τ.

The importance of studying racks of type D lies on the following result.

Theorem 2.1. [AFGV, Thm. 3.6] *If X is a finite rack of type D, then $\mathfrak{B}(X, q)$ has infinite dimension for all 2-cocycle q.* □

[1] The letter D stands for decomposable.

This result is based on [HS, Thm. 8.6], a consequence of [AHS].

2.2. Let $\mathbb{S}_m$ and $\mathbb{A}_m$ be the symmetric group and alternating group in m letters, respectively. Let $\sigma \in \mathbb{S}_m$. It is well-known that the conjugacy class $\mathcal{O}_\sigma^{\mathbb{S}_m}$ of σ in $\mathbb{S}_m$ coincides with the set of permutations in $\mathbb{S}_m$ with the same *type*, i. e. the cycle structure, as σ. On the other hand, if $\sigma \in \mathbb{A}_m$ and $\mathcal{O}_\sigma^{\mathbb{A}_m}$ denotes the conjugacy class of σ in $\mathbb{A}_m$, then either $\mathcal{O}_\sigma^{\mathbb{S}_m} = \mathcal{O}_\sigma^{\mathbb{A}_m}$ or else $\mathcal{O}_\sigma^{\mathbb{S}_m} = \mathcal{O}_\sigma^{\mathbb{A}_m} \cup \mathcal{O}_{(1\,2)\triangleright\sigma}^{\mathbb{A}_m}$ a disjoint union of two conjugacy classes in $\mathbb{A}_m$. This last case occurs if and only if σ is a product of disjoint cycles whose lengths are odd and distinct.

Let $m \geq 5$. In [AFGV, Thm. 4.1], it was proven that

- if $\sigma \in \mathbb{A}_m$ and the type of σ is different from
  (i) (3^2), $(2^2, 3)$, $(1^{m-3}, 3)$, (2^4), $(1^2, 2^2)$, $(1, 2^2)$,
  (ii) (p), $(1, p)$, p prime,
  then $\mathcal{O}_\sigma^{\mathbb{A}_m}$ is of type D;
- if $\sigma \in \mathbb{S}_m$ and the type of σ is different from (i), (ii) and
  (iii) $(2, 3)$, (2^3), $(1^{m-2}, 2)$,
  then $\mathcal{O}_\sigma^{\mathbb{S}_m}$ is of type D.

The classes in (i) and (iii) above are not of type D, see [AFGV, Rmk. 4.2].

In the present paper we are concerned about the remaining cases: the conjugacy class of p-cycles, p prime, in $\mathbb{A}_m$ and in $\mathbb{S}_m$ with $m \in \{p, p+1\}$. For some values of p the problem was already considered in [AFGV]:

- if the type of σ is (p), then $\mathcal{O}_\sigma^{\mathbb{A}_p}$ is of type D for $p = 13$, 17, 31, and $\mathcal{O}_\sigma^{\mathbb{A}_p}$ is not of type D for $p = 5$, 7, 11;
- if the type of σ is $(1, p)$, then $\mathcal{O}_\sigma^{\mathbb{A}_{p+1}}$ is of type D for $p = 2^q - 1$ a Mersenne prime, and $\mathcal{O}_\sigma^{\mathbb{A}_{p+1}}$ is not of type D for $p = 5$, 11.

Remarks 2.2. (a) The two conjugacy classes of p-cycles in $\mathbb{A}_p$ (resp. in $\mathbb{A}_{p+1}$) are isomorphic as racks.

(b) If σ is a p-cycle and $\mathcal{O}_\sigma^{\mathbb{A}_p}$ is of type D, then $\mathcal{O}_\sigma^{\mathbb{A}_{p+1}}$ is of type D.

2.3. **Subgroups of $\mathbb{A}_m$ generated by two p-cyles, p prime.** Let m, $p \in \mathbb{N}$, p odd prime. For $\sigma \in \mathbb{A}_m$ we define $\operatorname{supp}(\sigma) := \{i \in \{1, \dots, m\} : \sigma(i) \neq i\}$, i. e. $\operatorname{supp}(\sigma)$ is the set of points in $\{1, \dots, m\}$ moved by σ.

The main tool to prove Theorem 1.1 is the following result.

Theorem 2.3. [FW] *Let σ, τ two p-cycles in $\mathbb{A}_m$, with $m = |\operatorname{supp}(\sigma) \cup \operatorname{supp}(\tau)|$. Then one of the following must occur:*

(i) *$m = p$ and $\langle \sigma, \tau \rangle \simeq \mathbb{Z}/p\mathbb{Z}$;*

(ii) *$m = 2p$ and $\langle \sigma, \tau \rangle \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$;*

(iii) *$m = p = \frac{r^k - 1}{r - 1}$ and $\langle \sigma, \tau \rangle \simeq L_k(r)$;*

(iv) *$m = p + 2$, p is a Mersenne prime and $\langle \sigma, \tau \rangle \simeq L_2(p + 1)$;*

(v) *$m = p + 1$ and $\langle \sigma, \tau \rangle \simeq L_2(p)$;*

(vi) *$m = p = 11$ and $\langle \sigma, \tau \rangle \simeq L_2(11)$, M_{11};*

(vii) *$m = p = 23$ and $\langle \sigma, \tau \rangle \simeq M_{23}$;*

(viii) *$m = p + 1 = 12$ and $\langle \sigma, \tau \rangle \simeq M_{12}$, M_{11} or $L_2(11)$;*

(ix) *$m = p + 1 = 24$ and $\langle \sigma, \tau \rangle \simeq M_{24}$;*

(x) *$m = p+1$, p is a Mersenne prime and $\langle \sigma, \tau \rangle$ is a Frobenius group with kernel an elementary abelian 2-group of order m and complement of order p;*

(xi) *$m = p + 1$, p is a Mersenne prime, $H = L_k(2)$, $2^k = m$, $k \neq 3$ and $\langle \sigma, \tau \rangle$ is isomorphic to the semi-direct product of an elementary abelian 2-group by H with H acting in its natural action;*

(xii) *$m = p + 1 = 3$ and $\langle \sigma, \tau \rangle \simeq \mathbb{S}_3$; or*

(xiii) *$\langle \sigma, \tau \rangle \simeq \mathbb{A}_m$.*

The proof uses the list of 2, 3-transitive simple groups appearing in [Ca].

2.4. **On projective special linear groups.** Let r, $k \in \mathbb{N}$, with r a prime power. The projective special linear group $L_k(r)$ has order

$$|L_k(r)| = \frac{r^{\frac{k(k-1)}{2}}}{d} \prod_{i=2}^{k} (r^i - 1),$$

where $d = \gcd(k, r-1)$, see [Ar]. Assume that $p := \frac{r^k-1}{r-1}$ is prime. Then k is prime and $d = 1$. The group $L_k(r)$, which coincides with $\mathrm{SL}_k(r)$ in this case, is a primitive group contained in $\mathbb{A}_p$. Indeed, $L_k(r)$ is a 2-transitive permutation group of degree p, see [Is, Lemma 8.29]. Notice that $\mathrm{SL}_k(r)$ has elements of order p see [Da, Corollary 3]. On the other hand, a Sylow p-subgroup of $L_k(r)$ has order p, it is self-centralizer and its normalizer has order pk. Hence, the number of conjugacy classes of elements of order p in $L_k(r)$ is even and equal to $(p-1)/k$. For more information on the number of conjugacy classes in finite classical groups see [M] and [W].

Remark 2.4. Let p be prime as above, with $p \geq 13$.

(a) We claim that $t := (p-1)/k \geq 4$. Indeed, this is easy to see for $k = 2$ and $k = 3$. For $k \geq 5$, the result follows from $p \geq 2^k - 1 \geq 4k + 1$ which can be proven by induction on k.

Let σ be an element of order p in $L_k(r) \subset \mathbb{A}_p$. We recall that $\mathcal{O} \cap \langle \sigma \rangle = \{\sigma^\ell \,|\, J(\ell, p) = 1\}$, where $J(\ell, p)$ is the Jacobi symbol of ℓ and p, see [AFGV, Claim 1, p. 240]. Let $\mathfrak{K} := \{\mathcal{C}_1, \dots, \mathcal{C}_t\}$ be the set of conjugacy classes of elements of order p in $L_k(r)$ and take ℓ such that $J(\ell, p) = -1$. The set $\mathfrak{K}$ splits into two sets $\mathfrak{K}_1 := \{\mathcal{C}_i \,|\, \mathcal{C}_i \subset \mathcal{O}_\sigma^{\mathbb{A}_p}\}$ and $\mathfrak{K}_2 := \{\mathcal{C}_i \,|\, \mathcal{C}_i \subset \mathcal{O}_{(1\,2) \triangleright \sigma}^{\mathbb{A}_p}\}$. It is easy to see that $\mathfrak{K}_1$ and $\mathfrak{K}_2$ have the same cardinality. Indeed, if $\mathcal{C}_i \in \mathfrak{K}_1$, then $\mathcal{C}_i^\ell := \{x^\ell \,|\, x \in \mathcal{C}_i\} \in \mathfrak{K}_2$; now, the result follows using that the function

$\varphi_\ell : \mathcal{O}_\sigma^{\mathbb{A}_p} \to \mathcal{O}_{(1\,2)\triangleright\sigma}^{\mathbb{A}_p}$, given by $\varphi_\ell(x) = x^\ell$, is bijective and it induces a bijection between $\mathfrak{R}_1$ and $\mathfrak{R}_2$.

(b) If $\mathcal{O}_1$ and $\mathcal{O}_2$ are two conjugacy classes of elements of order p in $L_k(r)$, then there exist $\sigma \in \mathcal{O}_1$ and $\tau \in \mathcal{O}_2$ such that the order of the element $\sigma\tau$ is different from 1, 2 and p. This follows from [Go, Thm. 2] which states that in any finite simple group of Lie type G the product of any two conjugacy classes consisting of regular semisimple elements contains all semisimple elements of the group. We recall that an element $g \in G$ is called *regular semisimple* if the order of its centralizer in G is relatively prime to the characteristic of the corresponding finite field. In our case, any element of order p has centralizer of order p, thus it is regular semisimple since p and r are relatively prime.

2.5. Let G be a finite group, $\mathcal{O}$ a non-trivial conjugacy class of G, and σ, $\tau \in \mathcal{O}$. Assume that $(\sigma\tau)^2 = (\tau\sigma)^2$; this amounts to saying that $\tau\sigma\tau$ commutes with σ or, equivalently, that $\sigma\tau\sigma$ commutes with τ.

Lemma 2.5. *If the centralizer of σ in G is cyclic of order $|\sigma|$, then the order of $\langle\sigma, \tau\rangle$ is at most $|\sigma|^2$. If, in addition, $|\sigma|$ is prime, then σ and τ commute or $|\sigma\tau| = 2$.*

Proof. Since $\tau\sigma\tau$ commutes with σ, we have that $\tau\sigma\tau = \sigma^i$, for some i. Thus, $\langle\sigma, \tau\rangle$ is at most $|\sigma|^2$. We also have that $\sigma\tau\sigma = \tau^j$, for some j. Then $\sigma^{i+1} = \tau^{j+1}$ because of the assumption $(\sigma\tau)^2 = (\tau\sigma)^2$. Assume that $|\sigma| = p$, with p prime. If $j + 1 \neq 0 \mod (p)$, then $\tau \in \langle\sigma\rangle$, whereas if $j + 1 = 0 \mod (p)$, then $\sigma\tau\sigma = \tau^{-1}$, and $|\sigma\tau| = 2$. □

Lemma 2.6. *Let G be a finite group and let $\mathcal{O}$ be a conjugacy class of G whose elements have order p, with p an odd prime. Assume that*

(a) *the centralizer in G of an element in $\mathcal{O}$ has order p, and*
(b) *there exists a subgroup H of G such that $\mathcal{O}$ contains two different conjugacy classes $\mathcal{O}_1$, $\mathcal{O}_2$ of H.*

If for some $\sigma \in \mathcal{O}_1$ fixed

$$\text{there exists } \tau \in \mathcal{O}_2 \text{ such that } |\sigma\tau| \neq 1, 2, p, \tag{1}$$

then $\mathcal{O}$ is of type D.

Proof. Let $\sigma \in \mathcal{O}_1$. The condition (1) implies that there exists $\tau \in \mathcal{O}_2$ such that τ does not commute with σ and $|\sigma\tau| \neq 2$. By the previous discussion, $(\sigma\tau)^2 \neq (\tau\sigma)^2$. Now, since σ and τ are not conjugated in H, the condition (Ax. 2) holds. □

Corollary 2.7. *Let p be a prime number, $p \geq 5$, and let $\mathcal{O}$ be the conjugacy class of p-cycles in $\mathbb{S}_p$. Then $\mathcal{O}$ is of type D.*

Proof. It follows from Lemma 2.6 with $\sigma = (1\,2\,\cdots\,p)$, $H = \mathbb{A}_p$, $\mathcal{O}_1 = \mathcal{O}_\sigma^{\mathbb{A}_p}$, $\mathcal{O}_2 = \mathcal{O}_{(1\,2)\triangleright\sigma}^{\mathbb{A}_p}$ and $\tau = (1\,3) \triangleright \sigma$. □

3. Proof of the main result

Let $p \in \mathbb{N}$ be an odd prime, with $p \geq 5$, and $m \in \{p, p+1\}$. Define the p-cycle $\sigma = (1\,2\,\cdots\,p)$ and let $\mathcal{O}$ be the conjugacy class of σ in $\mathbb{A}_m$. We will determine when there exists $\tau \in \mathcal{O}$ such that (Ax. 1) and (Ax. 2) hold using Theorem 2.3. Notice that if $\langle\sigma, \tau\rangle \simeq \mathbb{Z}/p\mathbb{Z}$ or $\mathbb{A}_m$, with $\tau \in \mathcal{O}$, then (Ax. 1) does not hold for $\mathbb{Z}/p\mathbb{Z}$ and (Ax. 2) does not hold for $\mathbb{A}_m$.

(I) Assume that $m = p$.

Suppose that p is not of the form $\frac{r^k-1}{r-1}$, with r a prime power. If $p \neq 11, 23$, and $\tau \in \mathcal{O}$, then $\langle\sigma, \tau\rangle \simeq \mathbb{Z}/p\mathbb{Z}$ or $\mathbb{A}_p$; hence, $\mathcal{O}$ is not of type D. If $p = 11$ and $\tau \in \mathcal{O}$, then $H := \langle\sigma, \tau\rangle \simeq \mathbb{Z}/11\mathbb{Z}$, $\mathbb{A}_{11}$, $L_2(11)$ or M_{11}. In the last two cases, (Ax. 2) does not hold since each of the groups $L_2(11)$ and M_{11} have two conjugacy classes of elements of order 11 and each of them is contained in different conjugacy classes in $\mathbb{A}_{11}$; indeed, if $h \in H$ and $|h| = 11$, then each of the two conjugay classes of elements of order 11 in $\mathbb{A}_{11}$ contains some power h^ℓ, $1 \leq \ell \leq 10$. Hence, $\mathcal{O}$ is not of type D. The case $p = 23$ follows analogously.

Suppose that $p = \frac{r^k-1}{r-1}$, with r a prime power. By Subsection 2.4, $\mathbb{A}_p$ contains a subgroup H such that $\sigma \in H$ and $H \simeq L_k(r)$. Assume that $p \geq 13$. By Remark 2.4 (a), there are at least two conjugacy classes $\mathcal{O}_1$ and $\mathcal{O}_2$ of H contained in $\mathcal{O}$. We can assume $\sigma \in \mathcal{O}_1$; then condition (Ax. 2) holds for any $\tau \in \mathcal{O}_2$. By Lemma 2.6 and Remark 2.4 (b), condition (Ax. 1) holds for some $\tau \in \mathcal{O}_2$, and $\mathcal{O}$ yields of type D. Finally, if $p = 5$ or 7, then $\mathcal{O}$ is not of type D. Indeed, if H is a subgroup generated by two p-cycles, then $H \simeq \mathbb{Z}/5\mathbb{Z}$ or $\mathbb{A}_5 \simeq L_2(4)$ when $p = 5$, whereas $H \simeq \mathbb{Z}/7\mathbb{Z}$, $\mathbb{A}_7$ or $L_2(7)$ when $p = 7$. Notice that $L_2(7)$ has only two conjugacy classes of elements of order 7.

(II) Assume that $m = p + 1$.

Suppose that p is not of the form $\frac{r^k-1}{r-1}$, with r a prime power. If $p \neq 11, 23$, and $\tau \in \mathcal{O}$, then $\langle\sigma, \tau\rangle \simeq \mathbb{Z}/p\mathbb{Z}$, $\mathbb{A}_{p+1}$, $\mathbb{A}_p$ or $L_2(p)$. In the last two cases, condition (Ax. 2) does not hold since these groups have two conjugacy classes of elements of order p (see [FH] or [Ad] for the groups $L_2(p)$) and each of them is contained in different conjugacy classes in $\mathbb{A}_{p+1}$. Hence, $\mathcal{O}$ is not of type D. If $p = 11$ and $\tau \in \mathcal{O}$, then $\langle\sigma, \tau\rangle \simeq \mathbb{Z}/11\mathbb{Z}$, $\mathbb{A}_{12}$, $\mathbb{A}_{11}$, M_{11}, M_{12} or $L_2(11)$. In the last four cases, condition (Ax. 2) does not hold since these groups have two conjugacy classes of elements of order 11 and each of them is contained in different conjugacy classes in $\mathbb{A}_{12}$. Hence, $\mathcal{O}$ is not of type D.

If $p = 23$ and $\tau \in \mathcal{O}$, then $\langle \sigma, \tau \rangle \simeq \mathbb{Z}/23\mathbb{Z}$, $\mathbb{A}_{24}$, $\mathbb{A}_{23}$ or M_{24}; therefore, $\mathcal{O}$ is not of type D as above.

Suppose that $p = \frac{r^k - 1}{r-1}$, with r a prime power. By (I) and Remark 2.2 (b), if $p \geq 13$, then $\mathcal{O}$ is of type D. If $p = 5$, then the subgroup generated by two 5-cycles is $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{A}_6$ or $\mathbb{A}_5$; thus, $\mathcal{O}$ is not of type D. Finally, if $p = 7$, or more generally, $p = 2^h - 1$, with $h \geq 3$, is a Mersenne prime, then $\mathcal{O}$ is of type D. Indeed, set $q = 2^h$; then, the group $H = \mathbb{F}_q \rtimes \mathbb{F}_q^{\times} \simeq \mathbb{F}_q \rtimes \mathbb{Z}/p\mathbb{Z}$ acts on $\mathbb{F}_q$ by translations and dilations. Now, if we identify $\{1, \dots, q\}$ with $\mathbb{F}_q$, then H is isomorphic to a subgroup of $\mathbb{S}_q$, see [AFGV].

This finishes the proof of Theorem 1.1.

Remark 3.1. The prime numbers p of the form $(r^k - 1)/(r - 1)$, with r a prime power and $p < 1000$ are: $3 = 2^2 - 1$, $5 = \frac{4^2-1}{4-1}$, $7 = 2^3 - 1$, $13 = \frac{3^3-1}{3-1}$, $17 = \frac{16^2-1}{16-1}$, $31 = 2^5 - 1 = \frac{5^3-1}{5-1}$, $73 = \frac{8^3-1}{8-1}$, $127 = 2^7 - 1$, $257 = \frac{256^2-1}{256-1}$, $307 = \frac{17^3-1}{17-1}$, $757 = \frac{27^3-1}{27-1}$.

It is not known if the family of this kind of primes is finite or not. Indeed, it contains the families of Mersenne primes and Fermat primes. A discussion on numbers of this form can be found in [EGSS].

Remark 3.2. (a) The abelian subracks T of $\mathcal{O}$, with $\sigma \in T$, are contained in $\mathcal{O} \cap \langle \sigma \rangle$, see Remark 2.4 (a). Thus, any maximal abelian subrack of $\mathcal{O}$ has $(p - 1)/2$ elements and it is isomorphic to $\mathcal{O} \cap \langle \sigma \rangle$.

(b) Let $\mathcal{O}_{(p)}$ be a conjugacy class of p-cycles in $\mathbb{A}_p$ not of type D. By the Theorem 1.1, $p = 5$, 7 or p is not of the form $(r^k - 1)/(r - 1)$, with r a prime power. It is clear that a subrack X of $\mathcal{O}_{(p)}$ is the union of the conjugacy classes $\mathcal{O}_x^H$, $x \in X$, where H is the subgroup of $\mathbb{A}_p$ generated by the elements of X. Notice that H is a simple group since it is generated by p-cicles in $\mathbb{A}_p$.

Clearly, H is abelian if and only if X is an abelian subrack. Assume that H is not abelian. Then H must be a 2-transitive simple group of prime degree; this follows as in the step 5) of the proof of Theorem 2.3 given in [FW]. Then it occurs that H is as in the cases (iii), (vi), (vii) or (xiii) of Theorem 2.3. Hence, the non-abelian subracks of $\mathcal{O}_{(p)}$ are conjugacy classes of elements of order p in the subgroups appearing in that cases.

Therefore, the only cases where $\mathcal{O}_{(p)}$ has proper non-abelian subracks are $p = 7$, 11 and 23, and these subracks are isomorphic to a conjugacy class of elements of order p in $L_2(7)$, $L_2(11)$ or M_{11}, and M_{23}, respectively. For instance, any proper non-abelian subrack X of $\mathcal{O}_{(p)}$ has 24 elements for $p = 7$ and 60 or 720 elements for $p = 11$; moreover, X is not fixed by conjugation of any element in $\mathcal{O}_{(p)} \setminus X$.

(c) Let $\mathcal{O}$ be a conjugacy class of p-cycles in $\mathbb{A}_{p+1}$ not of type D. By the Theorem 1.1, $p=5$ or p is not of the form $(r^k-1)/(r-1)$, with r a prime power. As in (b) above, the proper non-abelian subracks of $\mathcal{O}$ are conjugacy classes of elements of order p in the corresponding subgroups appearing in the proof of Theorem 1.1. They are: $\mathbb{A}_5$ for $p=5$; $\mathbb{A}_{11}$, $L_2(11)$, M_{11} and M_{12} for $p=11$; $\mathbb{A}_{23}$, M_{23} and M_{24} for $p=23$; $\mathbb{A}_p$ and $L_2(p)$ otherwise.

(d) For the racks $\mathcal{O}$ described in (b) and (c) above it would be possible to decide if the dimension of $\mathfrak{B}(\mathcal{O},q)$ is not finite, for some 2-cocycle q, as mentioned in [AFGaV, §2.6]. Indeed, for an abelian subrack T of $\mathcal{O}$ and any 2-cocycle q we could determine if the diagonal braiding associated with q gives rise to a Nichols algebra of infinite dimension; in that case $\mathfrak{B}(\mathcal{O},q)$ would be also of infinite dimension. For this we can use the classification of finite-dimensional Nichols algebras of diagonal type [H].

In that sense, we compute using RiG (see [GV]) the second abelian rack cohomology group of some of this racks:

- $H^2(\mathcal{O}_{(5)},\mathbb{C}^\times)=\mathbb{C}^\times\times\mathbb{G}_{10}$. Notice that $\mathcal{O}_{(5)}\simeq Q_{12,3}$ in [V].
- $H^2(X,\mathbb{C}^\times)=\mathbb{C}^\times\times\mathbb{G}_{14}$, with $X\subset\mathcal{O}_{(7)}$, $|X|=24$.

See [AG] for the considered cohomology theory of racks and [AFGaV] for the use of RiG in our cases. It would be expected that $H^2(\mathcal{O}_{(p)},\mathbb{C}^\times)=\mathbb{C}^\times\times\mathbb{G}_{2p}$.

Acknowledgement. The author is grateful to the referee for several helpful suggestions. I thank R. Guralnick and A. Hulpke for very important comments on linear simple groups. I also thank L. Vendramin for interesting discussions about RiG. Part of this work was done during a postdoctoral position at Université Paris Diderot – Paris 7; I am very grateful to Prof. Marc Rosso for his kind hospitality.

References

[Ad] J. Adams, *Characters tables of* GL$(2,q)$*,* SL$(2,q)$*,* PGL$(2,q)$ *and* PSL$(2,q)$, `http://www.math.umd.edu/~jda/characters/`.

[AFGaV] N. Andruskiewitsch, F. Fantino, G. A. Garcia, and L. Vendramin, *On Nichols algebras associated to simple racks*, Groups, algebras and applications, 31–56, Contemp. Math., **537**, Amer. Math. Soc., Providence, RI, 2011.

[AFGV] N. Andruskiewitsch, F. Fantino, M. Graña and L. Vendramin, *Finite-dimensional pointed Hopf algebras with alternating groups are trivial*, Ann. Mat. Pura Appl (4) **190** (2011), no. 2, 225–245.

[AG] N. Andruskiewitsch and M. Graña, *From racks to pointed Hopf algebras*, Adv. Math. **178** (2003), no. 2, 177–243.

[AHS] N. Andruskiewitsch, I. Heckenberger and H.-J. Schneider, *The Nichols algebra of a semisimple Yetter-Drinfeld module*, Amer. J. Math. **132** (2010), no. 6, 1493–1547.

[AS] N. Andruskiewitsch and H.-J. Schneider, *Pointed Hopf Algebras*, in “New directions in Hopf algebras", 1–68, Math. Sci. Res. Inst. Publ. **43**, Cambridge Univ. Press, Cambridge, 2002.

[Ar] E. Artin, *The Orders of the Classical Simple Groups*, Comm. Pure Appl. Math. **8** (1955), 455–472.

[Ca] P. J. Cameron, *Finite permutation groups and finite simple groups*, Bull. London Math. Soc. **13** (1981), no. 1, 1–22.

[Da] M. R. Darafsheh, *Order of elements in the groups related to the general linear group*, Finite Fields Appl. **11** (2005), no. 4, 738–747.

[EGSS] D. Estes, R. Guralnick, M Schacher and E. Straus, *Equations in prime powers*, Pacific J. Math. **118** (1985), no. 2, 359–367.

[FW] K. R. Fawcett and G. L. Walls, *Groups generated by two p-cycles*, Arch. Math. **50** (1988), no. 5, 391–393.

[FH] W. Fulton and J. Harris, *Representation theory. A first course.* Graduate Texts in Mathematics, **129**. Readings in Mathematics. Springer-Verlag, New York, 1991.

[Go] R. Gow, *Commutators in finite simple groups of Lie type*, Bull. London Math. Soc. 32 (2000), no. 3, 311–315.

[GV] M. Graña and L. Vendramin, *RiG. A GAP package for racks, quandles and Nichols Algebras*, available at `http://code.google.com/p/rig/`.

[H] I. Heckenberger, *Classification of arithmetic root systems*, Adv. Math. **220** (2009), no. 1, 59–124.

[HS] I. Heckenberger and H.-J. Schneider, *Root systems and Weyl groupoids for Nichols algebras*, Proc. Lond. Math. Soc. (3) **101** (2010), no. 3, 623–654.

[Is] I. M. Isaacs, *Finite group theory.* Graduate Studies in Mathematics, **92**, American Mathematical Society, Providence, RI, 2008.

[Jo] D. Joyce, *Simple quandles*, J. Algebra **79** (1982), no. 2, 307–318.

[M] I. G. Macdonald, *Numbers of conjugacy classes in some finite classical groups*, Bull. Austral. Math. Soc. **23** (1981), no. 1, 23–48.

[V] L. Vendramin, *On the classification of quandles of low order*, J. Knot Theory Ramifications **21** (2012), no. 9, 1250088, 10 pp.

[W] G. E. Wall, *Conjugacy classes in projective and special linear groups*, Bull. Austral. Math. Soc. **22** (1980), no. 3, 339–364.

Département de Mathématiques, Université Paris Diderot (Paris 7), 175, rue du Chevaleret, 75013, Paris, France

Facultad de Matemática, Astronomía y Física, Universidad Nacional de Córdoba, CIEM – CONICET. Medina Allende s/n (5000) Ciudad Universitaria, Córdoba, Argentina

E-mail address: `fantino@famaf.unc.edu.ar`