ON NICHOLS ALGEBRAS OVER $\mathbf{PGL}(2,q)$ AND $\mathbf{PSL}(2,q)$

SEBASTIÁN FREYRE, MATÍAS GRAÑA, LEANDRO VENDRAMIN

ABSTRACT. We compute necessary conditions on Yetter-Drinfeld modules over the groups $\mathbf{PGL}(2,q) = \mathbf{PGL}(2,\mathbb{F}_q)$ and $\mathbf{PSL}(2,q) = \mathbf{PSL}(2,\mathbb{F}_q)$ to generate finite dimensional Nichols algebras. This is a first step towards a classification of pointed Hopf algebras with group of group-likes isomorphic to one of these groups.

As a by-product of the techniques developed in this work, we prove that any finite-dimensional pointed Hopf algebra over the Mathieu groups M_{20} or $M_{21} = \mathbf{PSL}(3,4)$ is the group algebra.

1. INTRODUCTION

Quantum groups, introduced by Drinfeld and Jimbo in the 1980's, were constructed as a mean to solve the Quantum Yang-Baxter Equation. They are deformations of enveloping algebras of semisimple complex Lie algebras. But they are also pointed Hopf algebras, and this marked the beginning of an algebraic program: classifying pointed Hopf algebras. A new chapter in this program was introduced by Lusztig: when the deformation parameter q is a root of unit, we can consider the so called Frobenius-Lusztig kernels. These are now finite dimensional pointed Hopf algebras, which carry the combinatorial information of a Cartan matrix and a Weyl group.

Soon, the question became how to construct new finite dimensional pointed Hopf algebras, and how Cartan matrices and Weyl groups appear in them. To keep this Introduction short, let us just mention that the Lifting Procedure [AS02] was the answer to the first question and the introduction of a Weyl groupoid [Hec06a] was the answer to the second one.

When the group of grouplikes is abelian, the whole procedure is well understood nowadays. However, when the group is not abelian, we are still far away from the classification. Not only so, but even the construction of finite dimensional pointed Hopf algebras over non abelian groups is an elusive matter [Gr].

Let us recall that, according to the Lifting Procedure, to classify finite dimensional pointed Hopf algebras with a specific group of grouplikes, the key step is to compute the Nichols algebras generated by Yetter-Drinfeld modules over the group which are finite dimensional. With the abelian tools at hand, it is possible to rule out, for a given group (or a family of groups), a large class of Yetter-Drinfeld modules which can be shown to produce infinite dimensional Nichols algebras. Therefore, the next step to classify f.d. pointed Hopf algebras over those groups is to study the Nichols algebras produced by the remaining modules.

One of the key tools to produce Yetter-Drinfeld modules over groups is that of racks and 2-cocycles. They allow to work with the braided vector spaces without

having to resort to groups. However, when trying to classify pointed Hopf algebras parametrized by groups, sometimes the rack 2-cocycles are "too general". When the group is fixed, a conjugacy class can not hold any 2-cocycle, but only some of them. Many times, one can prove that all Nichols algebras produced by a conjugacy class *within* a group are infinite-dimensional, while one is not able to prove that, as a rack, the same thing happens with *any* 2-cocycle. Therefore, we develop in this article the concept of *class of type B*, as follows ($C_G(g)$ is the centralizer of $g \in G$ and $\mathfrak{B}(\mathcal{C}, \rho)$ stands for the Nichols algebra produced by the Yetter-Drinfeld module $M(\mathcal{C}, \rho)$ -see below-):

Definition 1.1. *Let G be a group, $g \in G$ and $\mathcal{C} = \{xgx^{-1} : x \in G\}$ its conjugacy class. We say that $\mathcal{C}$ is a* class of type B *if for any representation $\rho \in \widehat{C_G(g)}$ the Nichols algebra $\mathfrak{B}(\mathcal{C}, \rho)$ is infinite dimensional. We also say that g is* of type B *if its conjugacy class is. We say that the group G is* of type B *if all its conjugacy classes are.*

Remark 1.2. By the lifting procedure, if G is of type B then any finite dimensional pointed Hopf algebra with group of grouplikes (isomorphic to) G is (isomorphic to) the group algebra of G.

Remark 1.3. It is proved in [AFGV08] that if $g \in G$ is of type B and $f : G \hookrightarrow H$ is a monomorphism of groups then $f(g)$ is of type B in H. This is the reason why this concept turns out to be a powerful tool.

In [FGV07] Nichols algebras over $\mathbf{GL}(2,q)$ and $\mathbf{SL}(2,q)$ were studied. In that paper it is proved that $\mathbf{SL}(2,2^n)$ is of type B for $n > 1$. In this paper we deal with the groups $\mathbf{PGL}(2,q)$ and $\mathbf{PSL}(2,q)$ for q a power of an odd prime number (recall that if q is even then $\mathbf{PSL}(2,q) = \mathbf{PGL}(2,q) = \mathbf{SL}(2,q)$). For definitions and elementary properties of these groups, see for example [AB95].

One of the main results of this work is Theorem 1.4.

Theorem 1.4. *The Mathieu groups M_{20} and $M_{21} = \mathbf{PSL}(3,4)$ are of type B.*

It is interesting to note that M_{20} is non-simple. Also, notice that this is the first example of a non-simple group which is of type B. Other results of this work are (see notations below):

Theorem 1.5. *Let $G = \mathbf{PGL}(2,q)$ (see Table 4 in §5 for the conjugacy classes of G). Then, class $\mathcal{C}_2$ is of type B. Also, the conditions to obtain finite-dimensional Nichols algebras on the representations for classes $\mathcal{C}_3$, $\mathcal{C}_4$, $\mathcal{C}_5$ and $\mathcal{C}_6$ are given in propositions 5.1, 5.2, 5.3 and 5.4.*

Theorem 1.6. *Let $G = \mathbf{PSL}(2,q)$ (see Tables 2 and 3 in §4). Then, classes $\mathcal{C}_i$ are of type B for $i < 6$. Also, the conditions to obtain finite-dimensional Nichols algebras on the representation for class $\mathcal{C}_6$ are given in Proposition 4.2 if $q \equiv 1$ (mod 4), or in Proposition 4.4 if $q \equiv 3$ (mod 4).*

2. Preliminaries

2.1. **Notations.** As said, we use the same notation as in [FGV07]. The number p will be an odd prime number and q a power of p, $E = \mathbb{F}_{q^2}$ will be the quadratic extension of $\mathbb{F}_q$, $\bar{x} = x^q$ will be the Galois conjugate of $x \in E$, k will be an algebraically closed field of characteristic zero, and we will write $\mathcal{R}_n$ for the set of

TABLE 1. Character table of $\mathbb{D}_n$ (n even)

	Degree	r^k	sr^k
χ_1	1	1	1
χ_2	1	1	-1
χ_3	1	$(-1)^k$	$(-1)^k$
χ_4	1	$(-1)^k$	$(-1)^{k+1}$
μ_h $(0 < h < \frac{n}{2})$	2	$2\cos\frac{2\pi hk}{n}$	0

primitive n-th roots of 1 in k. If $q \equiv 1 \pmod 4$ we write $\pm i$ for the square roots of -1 in $\mathbb{F}_q$. Following the notation in [Ada02], we fix an element $\Delta \in \mathbb{F}_q \setminus \mathbb{F}_q^2$ and an element $\delta \in E$ which is a square root of Δ. We consider elements $z \in E$ being written as $z = x + \delta y$, with $x, y \in \mathbb{F}_q$.

If G is a finite group, $\mathcal{C}$ is a conjugacy class of $g \in G$, and ρ is an irreducible representation of the centralizer $C_G(g)$, we write $\mathfrak{B}(\mathcal{C}, \rho)$ (or $\mathfrak{B}(\mathcal{C})$ if no confusion can arise) for the Nichols algebra generated by the Yetter-Drinfeld module $V(g, \rho)$ (see for example [AG99]).

2.2. **Representations of the Dihedral group.** We present the Dihedral group $\mathbb{D}_n$ of order $2n$ by generators r and s and relations

$$r^n = s^2 = 1, \quad srs = r^{-1}.$$

When n is even, the irreducible representations are given in Table 1 (see [Ser77, Section 5.3]). We will not need the Dihedral groups $\mathbb{D}_n$ with n odd.

2.3. **Main tools.** Note that, since ρ is irreducible and $g \in Z(C_G(g))$ (the center of $C_G(g)$), then $\rho(g)$ is a scalar (by Schur lemma). The following lemmas are contained in [AF07a, AF07b, AZ07, FGV07, Hec06b].

Lemma 2.1. *Assume that* $\dim \mathfrak{B}(\mathcal{C}, \rho) < \infty$. *If* $g^{-1} \in \mathcal{C}$ *then* $\rho(g) = -1$.

Proof. See [AZ07]. $\qquad\square$

As in the cited papers, a conjugacy class is called *real* if it contains the inverses of its elements.

Lemma 2.2. *Assume that* $\dim \mathfrak{B}(\mathcal{C}, \rho) < \infty$. *If there exist* $n > 1$ *such that* $g^n \in \mathcal{C}$ *then* $\rho(g) = -1$ *or* $\rho(g) \in \mathcal{R}_3$. *Moreover, if* $g^{n^2} \neq g$ *then* $\rho(g) = -1$.

Proof. For the proof see for example [FGV07]. $\qquad\square$

As in the cited papers, a conjugacy class is called *quasireal* if it contains proper powers of its elements.

The next lemma is useful to treat, for instance, some conjugacy classes of involutions. A particular case of this Lemma appears also in [Fan07].

Lemma 2.3. *Let* G *be a group.*

(1) *Assume that* $g_0, g_1, g_2 \in G$ *are conjugate and commute to each other, that* $x_1 x_2$ *and* $x_2 x_1$ *belong to* $C_G(g_0)$, *(where* x_i *are such that* $g_i = x_i g_0 x_i^{-1}$ *for* $i = 1, 2$), *and that* $g_1 g_2 = g_0^m$ *for an odd integer* m. *Then* g_0 *is of type B.*
(2) *The conjugacy class of involutions in the alternating group* $\mathbb{A}_4$ *is of type B.*
(3) *If* $g_0, x \in G$ *are such that* g_0 *has order* 2 *and both* x *and* $g_0 x$ *have order* 3, *then* g_0 *is of type B.*

Proof. Part 2 is a consequence of Part 1 by taking $g_0 = (1\,2)(3\,4)$, $g_1 = (1\,3)(2\,4)$, $g_2 = (1\,4)(2\,3)$, $x_1 = (2\,4\,3)$ and $x_2 = x_1^{-1}$ (we have $g_1 g_2 = g_0$ in this way). Also, Part 3 is a consequence of Part 2 and Remark 1.3 since, as proved in [Dic58, Theorem 265] (or use GAP to check it), $\mathbb{A}_4$ can be presented by generators g_0 and x and relations

$$g_0^2 = x^3 = (g_0 x)^3 = 1.$$

Therefore, we need to prove Part 1. First notice that, since $g_i g_j = g_j g_i$, there exists $w \in V \setminus \{0\}$ and $\lambda_i \in \mathbb{C}$ such that $\rho(g_i)(w) = \lambda_i w$ for $i = 0, 1, 2$. For any $0 \le i, j \le 2$, let $\gamma_{ij} = x_j^{-1} g_i x_j \in C_G(g_0)$. It is easy to see that

$$\gamma = (\gamma_{ij}) = \begin{pmatrix} g_0 & g_2 & g_1 \\ g_1 & g_0 & g_1^m g_0^{-1} \\ g_2 & g_2^m g_1^{-1} & g_0 \end{pmatrix}.$$

Then, $W = \mathrm{span}\{x_1 \otimes w, x_2 \otimes w, x_3 \otimes w\}$ is a braided vector subspace of $M(\mathcal{C}, \rho)$ of abelian type with Dynkin diagram given by
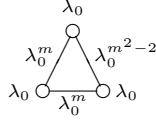
For $\mathfrak{B}(\mathcal{C}, \rho)$ to be finite dimensional, we should have $\lambda_0 = -1$ (see [Hec05, Table 3]) and m should be an even number, which contradicts our assumption. $\square$

3. Two examples: M_{20} and M_{21}

In [Fan07] the five simple Mathieu groups are studied. In this section we will study finite dimensional Nichols algebras over the Mathieu groups M_{20} and M_{21} ($= \mathbf{PSL}(3,4)$). We begin with the non-simple Mathieu group M_{20}. For a definition and elementary properties of this group, see [Hup67, Chapter XII]. Since we do computations with GAP, we use the product in the symmetric groups as they do: the product of two permutations σ and τ means the composition of the permutation σ followed by τ.

We know (see for example [ATLAS]) that $M_{20} = \langle \alpha, \beta \rangle$ as a subgroup of $\mathbb{S}_{20}$, where

$$\alpha = (1, 2, 4, 3)(5, 11, 7, 12)(6, 13)(8, 14)(9, 15, 10, 16)(1, 19, 20, 18),$$
$$\beta = (2, 5, 6)(3, 7, 8)(4, 9, 10)(11, 17, 12)(13, 16, 18)(14, 15, 19).$$

This is a group of order 960. The conjugacy classes are 1A, 2A, 2B, 3A, 4A, 4B, 4C, 5A, 5B (we are using the ATLAS notation for conjugacy classes, the name of a class begins with the order of its elements).

Proposition 3.1. *The Mathieu group M_{20} is of type B.*

Proof. By [AZ07, Remark 1.1] we know that the class 1A gives infinite dimensional Nichols algebras for every representation. Using GAP it is easy to check that all conjugacy classes of M_{20} are real. Therefore, by Lemma 2.1, the conjugacy classes with representatives of odd order (i.e. 3A, 5A, 5B) will also give infinite dimensional Nichols algebras.

All the remaining classes are dealt with Lemma 2.3. We just list the elements g_1, g_2 and x_1 for each of them. In all the cases, we put $g_0 = g_1 g_2$ and $x_2 = x_1^{-1}$. We have

used GAP to find those elements, with the help of some scripts which may be down-loaded from the third author's web page: `http://mate.dm.uba.ar/~lvendram/`.

For class 2A, we take

$$g_1 = (2,3)(5,19)(6,13)(7,18)(8,14)(11,17)(12,20)(15,16),$$
$$g_2 = (2,15)(3,16)(5,18)(6,8)(7,19)(11,12)(13,14)(17,20),$$
$$x_1 = (1,4,10)(3,16,15)(5,11,14)(6,18,17)(7,12,8)(13,19,20).$$

For class 2B,

$$g_1 = (1,15)(2,10)(3,4)(5,13)(6,7)(8,18)(9,16)(14,19),$$
$$g_2 = (1,13)(2,7)(3,19)(4,14)(5,15)(6,10)(8,9)(16,18),$$
$$x_1 = (2,19,8)(3,18,6)(4,9,10)(5,13,15)(7,14,16)(12,17,20).$$

For class 4A,

$$g_1 = (1,2,10,15)(3,4,16,9)(5,14,7,8)(6,19,13,18)(11,12)(17,20),$$
$$g_2 = (1,5,4,19)(2,14,16,13)(3,6,15,8)(7,9,18,10)(11,17)(12,20),$$
$$x_1 = (2,6,5)(3,8,7)(4,10,9)(11,12,17)(13,18,16)(14,19,15).$$

For class 4B,

$$g_1 = (1,3,4,15)(2,10,16,9)(5,8,19,6)(7,14,18,13)(11,20)(12,17),$$
$$g_2 = (1,7,9,19)(2,6,3,14)(4,18,10,5)(8,15,13,16)(11,12)(17,20),$$
$$x_1 = (2,6,5)(3,8,7)(4,10,9)(11,12,17)(13,18,16)(14,19,15).$$

For class 4C,

$$g_1 = (1,16,9,15)(2,10,3,4)(5,6,18,14)(7,13,19,8)(11,17)(12,20),$$
$$g_2 = (1,18,10,19)(2,13,15,6)(3,8,16,14)(4,7,9,5)(11,20)(12,17),$$
$$x_1 = (2,6,5)(3,8,7)(4,10,9)(11,12,17)(13,18,16)(14,19,15).$$

$\square$

We do the same now with M_{21}:

Proposition 3.2. *The Mathieu group $M_{21} = \mathbf{PSL}(3,4)$ is of type B.*

Proof. As in all groups, the trivial class 1A is of type B. Classes 3A, 3B, 5A and 5B are real, as can be checked with GAP using the function `RealClasses`. Then these classes are of type B by Lemma 2.1. Classes 7A and 7B are quasireal, as can be checked with GAP with the function `PowerMaps`. Then these classes are of type B by Lemma 2.2.

We are left with classes 2A, 4A, 4B, 4C. By ATLAS, we know that the semidirect product $2^4 : \mathbb{A}_5 = M_{20}$ is a maximal subgroup of $\mathbf{PSL}(3,4)$ (see [CCN⁺85, pp. 23]). Now the result follows from 3.1, by looking at how classes of even order in M_{20} sit into M_{21}, by using the function `PossibleClassFusions`: since M_{20} is a subgroup of M_{21} there exists a monomorphism $f : M_{20} \hookrightarrow M_{21}$ and therefore there exist a fusion of conjugacy classes. Moreover, with GAP we calculate all possible fusion of conjugacy classes and by inspection of all of these fusions it is easy to arrive to the desired result (see the file `fgv.log` for the results).

$\square$

4. NICHOLS ALGEBRAS OVER $\mathbf{PSL}(2,q)$

In this section we deal with the groups $\mathbf{PSL}(2,q) = \mathbf{SL}(2,\mathbb{F}_q)/\{\pm I\}$, which have order $\frac{(q-1)q(q+1)}{2}$. Recall that if $q \neq 2, 3$ then $\mathbf{PSL}(2,q)$ is simple (see eg. [AB95, Theorem 2.6.8]).

TABLE 2. Conjugacy classes of $\mathbf{PSL}(2,\mathbb{F}_q)$ for $q \equiv 1(4)$

	Representative	Number	Size
$\mathcal{C}_1$	$c_1 = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$	1	1
$\mathcal{C}_2$	$c_2 = \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$	1	$\frac{q^2-1}{2}$
$\mathcal{C}_3$	$c_3 = \begin{pmatrix} 1 & \Delta \\ & 1 \end{pmatrix}$	1	$\frac{q^2-1}{2}$
$\mathcal{C}_4$	$c_4(z) = \begin{pmatrix} x & \Delta y \\ y & x \end{pmatrix}$ $(N(z) = x^2 - \Delta y^2 = 1,\ y \neq 0)$	$\frac{q-1}{4}$	$q(q-1)$
$\mathcal{C}_5$	$c_5 = \begin{pmatrix} i & \\ & -i \end{pmatrix}$	1	$\frac{q(q+1)}{2}$
$\mathcal{C}_6$	$c_6(x) = \begin{pmatrix} x & \\ & x^{-1} \end{pmatrix}$ $(x \notin \{\pm 1, \pm i\})$	$\frac{q-5}{4}$	$q(q+1)$

4.1. The case $q \equiv 1(4)$**.** There are $\frac{q+5}{2}$ conjugacy classes, which are listed in Table 2 (see [Ada02]).

Proposition 4.1. *Classes* $\mathcal{C}_i$ *are of type B for* $i = 1, 2, 3, 4, 5$.

Proof. The trivial class is of type B for any group. For class $\mathcal{C}_2$ (resp. $\mathcal{C}_3$) we apply Lemma 2.1, since c_2 and c_2^{-1} (resp. c_3 and c_3^{-1}) are conjugate and have odd order p.

For $i = 4$, we notice that $c_4(z)^{-1} = c_4(z^{-1}) = \begin{pmatrix} x & -\Delta y \\ -y & x \end{pmatrix}$, which is conjugate to $c_4(z)$. Indeed, $c_5 c_4(z) c_5^{-1} = c_4(z^{-1})$. Then the result follows from Lemma 2.1, since the order of $c_4(z)$ is a divisor of $\frac{q+1}{2}$, which is odd.

TABLE 3. Conjugacy classes of $\mathbf{PSL}(2,q)$ for $q \equiv 3(4)$

	Representative	Number	Size
$\mathcal{C}_1$	$c_1 = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$	1	1
$\mathcal{C}_2$	$c_2 = \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$	1	$\frac{q^2-1}{2}$
$\mathcal{C}_3$	$c_3 = \begin{pmatrix} 1 & \Delta \\ & 1 \end{pmatrix}$	1	$\frac{q^2-1}{2}$
$\mathcal{C}_4$	$c_4(z) = \begin{pmatrix} x & \Delta y \\ y & x \end{pmatrix}$ $(N(z) = x^2 - \Delta y^2 = 1,\ xy \neq 0)$	$\frac{q-3}{4}$	$q(q-1)$
$\mathcal{C}_5$	$c_5 = \begin{pmatrix} & -1 \\ 1 & \end{pmatrix}$	1	$\frac{q(q-1)}{2}$
$\mathcal{C}_6$	$c_6(x) = \begin{pmatrix} x & \\ & x^{-1} \end{pmatrix}$ $(x \notin \{\pm 1\})$	$\frac{q-3}{4}$	$q(q+1)$

For $i = 5$, we notice that $\mathbb{A}_4$ is a subgroup of $\mathbf{PSL}(2,q)$ (see [Dic58, Ch. XII] or [Hup67, Satz II.8.18 (b)]). Since the only involutions in $\mathbf{PSL}(2,q)$ lie in class $\mathcal{C}_5$, Lemma 2.3 part 2 and Remark 1.3 say that $\mathcal{C}_5$ is of type B.   □

The centralizer of $c_6(x)$ is isomorphic to $\mathbb{F}_q^* / \{\pm 1\} \simeq \mathbb{Z}/\frac{q-1}{2}$.

Proposition 4.2. *If $\dim \mathfrak{B}(C_6, \rho) < \infty$ then $c_6(x)$ has even order and $\rho(c_6(x)) = -1$.*

Proof. Again, $\mathcal{C}_6$ is a real class, since conjugating $c_6(x)$ by $\left(\begin{smallmatrix} & -1 \\ 1 & \end{smallmatrix}\right)$ gives $c_6(x^{-1}) = c_6(x)^{-1}$. The result then follows from Lemma 2.1.   □

4.2. **The case $q \equiv 3(4)$.** There are $\frac{q+5}{2}$ conjugacy classes, which are listed in Table 3 (see [Ada02]).

Proposition 4.3. *Classes $\mathcal{C}_i$ are of type B for $i = 1, 2, 3, 5, 6$.*

Proof. It is entirely analogous to that of Proposition 4.1. The only difference is that now classes $\mathcal{C}_6$ have elements of odd order, instead of classes $\mathcal{C}_4$.   □

The centralizer of $c_4(x)$ is isomorphic to $\mathbb{Z}/\frac{q+1}{2}$. Again, by using Lemma 2.1 we have

Proposition 4.4. *If $\dim \mathfrak{B}(\mathcal{C}_4, \rho) < \infty$, then $c_4(z)$ has even order and $\rho(c_4(z)) = -1$.*

5. Nichols algebras over $\mathbf{PGL}(2,q)$

We deal in this section with $\mathbf{PGL}(2,q) = \mathbf{GL}(2,q)/\{tI : t \in \mathbb{F}_q^\times\}$, which has order $(q-1)q(q+1)$. Since $\mathbf{PGL}(2,3) \simeq \mathbb{S}_4$ and $\mathbf{PGL}(2,5) \simeq \mathbb{S}_5$ (which are treated in [AZ07]) we may assume that $q > 5$. There are $q + 2$ conjugacy classes, which are listed in Table 4 (see [Ada02]).

TABLE 4. Conjugacy classes of $\mathbf{PGL}(2,q)$

	Representative	Number	Size
$\mathcal{C}_1$	$c_1 = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$	1	1
$\mathcal{C}_2$	$c_2 = \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$	1	$q^2 - 1$
$\mathcal{C}_3$	$c_3(x) = \begin{pmatrix} x & \\ & 1 \end{pmatrix} \ (x \neq \pm 1)$	$\frac{q-3}{2}$	$q(q+1)$
$\mathcal{C}_4$	$c_4 = \begin{pmatrix} -1 & \\ & 1 \end{pmatrix}$	1	$\frac{q(q+1)}{2}$
$\mathcal{C}_5$	$c_5(z) = \begin{pmatrix} x & \Delta y \\ y & x \end{pmatrix} \ (xy \neq 0)$	$\frac{q-1}{2}$	$q(q-1)$
$\mathcal{C}_6$	$c_6 = \begin{pmatrix} & \Delta \\ 1 & \end{pmatrix}$	1	$\frac{q(q-1)}{2}$

By considering the inclusion $\mathbf{PSL}(2,q) \hookrightarrow \mathbf{PGL}(2,q)$, we get from the previous section that the following classes are of type B:

$\mathcal{C}_1, \mathcal{C}_2$

$\mathcal{C}_3$ if $q \equiv 3 \pmod 4$ and $x \in \mathbb{F}_q^2$

$\mathcal{C}_4$ if $q \equiv 1 \pmod 4$ (because it is class $\mathcal{C}_5$ in $\mathbf{PSL}(2,q)$)

$\mathcal{C}_5$ if $q \equiv 1 \pmod 4$ and $N(z) = x^2 - \Delta y^2 \in \mathbb{F}_q^2$

$\mathcal{C}_6$ if $q \equiv 3 \pmod 4$ (because it is class $\mathcal{C}_5$ in $\mathbf{PSL}(2,q)$)

We consider now the other cases. They are not of type B, but one can restrict the representations anyway.

The centralizer of $c_3(x)$ is given by the classes in $\mathbf{PGL}(2,q)$ of matrices $\left(\begin{smallmatrix} \sigma & \\ & 1 \end{smallmatrix}\right)$ and therefore it is isomorphic to $\mathbb{F}_q^\times$.

Proposition 5.1. *Let $q \equiv 1 \pmod 4$. If $\dim \mathfrak{B}(\mathcal{C}_3, \rho) < \infty$, then x has even order and $\rho(c_3(x)) = -1$.*

Proof. Notice that $\mathcal{C}_3$ is a real class, and use Lemma 2.1.   □

The centralizer of c_4 is given by the classes in $\mathbf{PGL}(2,q)$ of matrices $\left(\begin{smallmatrix} 1 & \\ & \sigma \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} & 1 \\ \sigma & \end{smallmatrix}\right)$ for $\sigma \in \mathbb{F}_q^\times$. It is easy to see that this group is isomorphic to $\mathbb{D}_{q-1}$. In the presentation by r, s given at §2.2, c_4 corresponds to $r^{\frac{q-1}{2}}$.

Proposition 5.2. *Let $q \equiv 3 \pmod 4$ and let ρ be a representation of $C_{\mathbf{PGL}(2,q)}(c_4)$ with character χ. If $\dim \mathfrak{B}(\mathcal{C}_4) < \infty$, then $\chi \in \{\chi_3, \chi_4, \mu_h \ (h \ odd)\}$ (see Table 1).*

Proof. Since c_4 is an involution, we must have $\rho(c_4) = -1$. Then, the result follows by inspection of the Table.   □

The centralizer of $c_5(z)$ is isomorphic to $E^*/\mathbb{F}_q^* \simeq \mathbb{Z}/q+1$ (see [Ada02]).

Proposition 5.3. *Let $q \equiv 3 \pmod 4$. If $\dim \mathfrak{B}(\mathcal{C}_5, \rho) < \infty$, then $c_5(z)$ has even order and $\rho(g) = -1$.*

Proof. In a similar way as the proof of Prop. 4.1, we see that classes $\mathcal{C}_5$ are real by conjugating $c_5(z)$ with c_4. Now, we apply Lemma 2.1.   □

The centralizer of c_6 is given by the classes in $\mathbf{PGL}(2,q)$ of matrices $\left(\begin{smallmatrix} x & \pm\Delta y \\ y & x \end{smallmatrix}\right)$. It is easy to see that this group is isomorphic to $\mathbb{D}_{q+1}$. In the presentation by r, s given at §2.2, c_6 corresponds to $r^{\frac{q+1}{2}}$.

Proposition 5.4. *Let $q \equiv 1 \pmod 4$ and let χ be the character of the representation ρ. If $\dim \mathfrak{B}(\mathcal{C}_6) < \infty$, then $\chi \in \{\chi_3, \chi_4, \mu_h \ (h \ odd)\}$ (see Table 1).*

Proof. Analogous to that of Prop. 5.2.   □

6. THE CLASS OF ORDER 4 IN $\mathbf{SL}(2,q)$

In this section we use the tools in the present paper to improve a result in [FGV07]. There, we considered in $\mathbf{SL}(2,q)$ the classes $\mathcal{C}_7$ of $c_7(x) = \left(\begin{smallmatrix} x & 0 \\ 0 & x^{-1} \end{smallmatrix}\right)$, and $\mathcal{C}_8$ of $c_8(z) = \left(\begin{smallmatrix} x & \Delta y \\ y & x \end{smallmatrix}\right)$, where $z = x + \delta y \in E \setminus \mathbb{F}_q$. Propositions 3.4 (resp. 3.5) in [FGV07] prove that in order for $\mathfrak{B}(\mathcal{C}_7)$ (resp. $\mathfrak{B}(\mathcal{C}_8)$) to be finite dimensional, the order of x (resp. z) must be even. On the other hand, when $q = 3$ there is only one class $\mathcal{C}_8$, and it is proved in [AFGV08] that it is of type B. We prove here that

$\mathbf{SL}(2,3)$ is a subgroup of $\mathbf{SL}(2,q)$. This implies that when $q \equiv 1 \pmod 4$ and x has order 4, the class of $c_7(x) \in \mathbf{SL}(2,q)$ is of type B, and when $q \equiv 3 \pmod 4$ and z has order 4, the class of $c_8(z) \in \mathbf{SL}(2,q)$ is of type B.

One possible presentation of $\mathbf{SL}(2,3)$ is given by generators x, y and relations $x^3 = y^4 = (xy^3)^3 = 1$, $xy^2 = y^2x$. In fact, one can take

$$x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad y = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

Then, if a group G has elements A, B, C of orders 3, 3 and 4 respectively such that $ABC = [B, C^2] = 1$, then G has a subgroup isomorphic to $\mathbf{SL}(2,3)$. Indeed, take the map $x \mapsto B$, $y \mapsto C^3$. It is easy to see that this defines a map $\mathbf{SL}(2,3) \to G$. It is injective because otherwise the orders of A, B or C would be smaller than stated, as can be seen by considering the normal subgroups of $\mathbf{SL}(2,3)$ (the non-trivial ones being isomorphic to C_2 and the quaternion group Q of order 8). Also, any $C \in \mathbf{SL}(2,q)$ has order 4 if and only if $\operatorname{tr} C = 0$. Indeed, it is easy to see that if $\alpha = \operatorname{tr} C$, then $C^4 = (\alpha^3 - 2\alpha)C + (1 - \alpha^2)$, which implies the claim. Therefore, there is only one class in $\mathbf{SL}(2,q)$ of order 4. This means that the embedding we shall find $\mathbf{SL}(2,3) \hookrightarrow \mathbf{SL}(2,q)$ sends the class of $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix} \right) \in \mathbf{SL}(2,3)$ of type B to it.

We prove now the existence of the embedding $\mathbf{SL}(2,3) \hookrightarrow \mathbf{SL}(2,q)$. Since $\mathbf{SL}(2,p)$ embeds in $\mathbf{SL}(2,q)$, it is enough to prove that $\mathbf{SL}(2,3)$ embeds in $\mathbf{SL}(2,p)$. Let $x \in \mathbb{F}_p^\times$ be of order $p - 1$ and let $\mathcal{G}_l$ be the class of $c_7(x^l)$. Let $z \in E$ generate the group $\{a + \delta b \in E \mid a^2 - \Delta b^2 = 1\}$ and let $\mathcal{H}_m$ be the class of $c_8(z^m)$. The character table of $\mathbf{SL}(2,p)$ restricted to the classes $\mathcal{G}_l$ and $\mathcal{H}_m$ is given in Table 5, where we write $c[\frac{a}{b}] = e^{\frac{2\pi i a}{b}} + e^{-\frac{2\pi i a}{b}}$. There, $1 \le i \le \frac{p-3}{2}$ for ζ_i and $1 \le i \le \frac{p-1}{2}$ for θ_i.

TABLE 5. Character table on classes $\mathcal{G}_l$ and $\mathcal{H}_m$.

	1	ψ	ζ_i	ξ_1	ξ_2	θ_i	η_1	η_2
deg	1	p	$p+1$	$\frac{1}{2}(p+1)$	$\frac{1}{2}(p+1)$	$p-1$	$\frac{1}{2}(p-1)$	$\frac{1}{2}(p-1)$
$\mathcal{G}_l$	1	1	$c[\frac{il}{p-1}]$	$(-1)^l$	$(-1)^l$	0	0	0
$\mathcal{H}_m$	1	-1	0	0	0	$-c[\frac{im}{p+1}]$	$(-1)^{m+1}$	$(-1)^{m+1}$

When $p \equiv 1 \pmod 3$, classes $\mathcal{G}_l$ have order 3 for $l = \frac{p-1}{3}$ and $l = \frac{2(p-1)}{3}$. On the other hand, when $p \equiv 2 \pmod 3$, classes $\mathcal{H}_m$ have order 3 for $m = \frac{p+1}{3}$ and $m = \frac{2(p+1)}{3}$. We use then classes $\mathcal{G}_l$ and $\mathcal{H}_m$ for A, B or C depending on the class of $p \pmod{12}$.

We apply then the well-known formula (see e.g. [Go68, Theorem 2.12])

$$S(\mathcal{C}_i, \mathcal{C}_j, \mathcal{C}_k) = \frac{|\mathcal{C}_i||\mathcal{C}_j||\mathcal{C}_k|}{|G|} \sum_\chi \frac{\chi(\mathcal{C}_i)\chi(\mathcal{C}_j)\chi(\mathcal{C}_k)}{\chi(1)}$$

which counts solutions of the equation $abc = 1$ with a, b, c respectively in classes $\mathcal{C}_i$, $\mathcal{C}_j$ and $\mathcal{C}_k$. Therefore, it is enough to see that for any p we have $S(\mathcal{C}_i, \mathcal{C}_j, \mathcal{C}_k) > 0$, where classes $\mathcal{C}_i$, $\mathcal{C}_j$ and $\mathcal{C}_k$ have orders 3, 3 and 4. We have then the following possibilities:

- If $p \equiv 5 \pmod{12}$, the element of order 4 belongs to the class $\mathcal{G}$ with $l = \frac{p-1}{4}$ and the element of order 3 belongs to the class $\mathcal{H}$ with $m = \frac{p+1}{3}$.

Then,

$$S(\mathcal{H}, \mathcal{H}, \mathcal{G}) = \frac{p^3(p-1)^2(p+1)}{p(p-1)(p+1)}\left(1 + \frac{1}{p}\right) = (p-1)p(p+1) > 0.$$

- If $p \equiv 7 \pmod{12}$, the element of order 4 belongs to the class $\mathcal{H}$ with $m = \frac{p+1}{4}$ and the element of order 3 belongs to the class $\mathcal{G}$ with $l = \frac{p-1}{3}$. Then,

$$S(\mathcal{G}, \mathcal{G}, \mathcal{H}) = \frac{p^3(p+1)^2(p-1)}{p(p-1)(p+1)}\left(1 - \frac{1}{p}\right) = (p-1)p(p+1) > 0.$$

- If $p \equiv 1 \pmod{12}$

$$S(\mathcal{G}_{\frac{p-1}{3}}, \mathcal{G}_{\frac{p-1}{3}}, \mathcal{G}_{\frac{p-1}{4}})$$

$$= \frac{p^2(p+1)^2}{p-1}\left(1 + \frac{1}{p} + \sum_{j=1}^{\frac{p-3}{2}} \frac{1}{p+1}c[\frac{j}{3}]^2 c[\frac{j}{4}] + 4\frac{(-1)^{\frac{p-1}{4}}}{p+1}\right)$$

$$\geq \frac{p^2(p+1)^2}{p-1}\left(1 + \frac{1}{p} + \sum_{j=1}^{\frac{p-3}{2}} \frac{8}{p+1}\cos(\frac{2\pi j}{3})^2 \cos(\frac{2\pi j}{4}) - \frac{4}{p+1}\right)$$

$$= \frac{p^2(p+1)^2}{p-1}\left(1 + \frac{1}{p} + \frac{8}{p+1}\sum_{l=1}^{[\frac{p-3}{4}]} \cos(\frac{4\pi l}{3})^2 \cos(\pi l) - \frac{4}{p+1}\right)$$

$$= \frac{p^2(p+1)^2}{p-1}\left(1 + \frac{1}{p} + \frac{8}{p+1}\left(\sum_{\substack{l=1 \\ l\equiv 0(3)}}^{[\frac{p-3}{4}]} \cos(\pi l) + \sum_{\substack{l=1 \\ l\not\equiv 0(3)}}^{[\frac{p-3}{4}]} \frac{1}{4}\cos(\pi l)\right) - \frac{4}{p+1}\right)$$

$$= \frac{p^2(p+1)^2}{p-1}\left(1 + \frac{1}{p} + \frac{2}{p+1}\left(\sum_{\substack{l=1 \\ l\equiv 0(3)}}^{[\frac{p-3}{4}]} 3\cos(\pi l) + \sum_{l=1}^{[\frac{p-3}{4}]} \cos(\pi l)\right) - \frac{4}{p+1}\right)$$

$$\geq \frac{p^2(p+1)^2}{p-1}\left(1 + \frac{1}{p} - \frac{12}{p+1}\right) > 0$$

- If $p \equiv 11 \pmod{12}$

$$S(\mathcal{H}_{\frac{p+1}{3}}, \mathcal{H}_{\frac{p+1}{3}}, \mathcal{H}_{\frac{p+1}{4}})$$

$$= \frac{p^2(p-1)^2}{p+1}\left(1 - \frac{1}{p} - \sum_{j=1}^{\frac{p-1}{2}} \frac{1}{p-1}c[\frac{j}{3}]^2 c[\frac{j}{4}] + 4\frac{(-1)^{\frac{p+5}{4}}}{p-1}\right)$$

$$\geq \frac{p^2(p-1)^2}{p+1}\left(1 - \frac{1}{p} - \sum_{j=1}^{\frac{p-1}{2}} \frac{8}{p-1}\cos(\frac{2\pi j}{3})^2 \cos(\frac{2\pi j}{4}) - \frac{4}{p-1}\right)$$

$$= \frac{p^2(p-1)^2}{p+1}\left(1 - \frac{1}{p} - \frac{8}{p-1}\sum_{l=1}^{[\frac{p-1}{4}]}\cos(\frac{4\pi l}{3})^2 \cos(\pi l) - \frac{4}{p-1}\right)$$

$$= \frac{p^2(p-1)^2}{p+1}\left(1 - \frac{1}{p} - \frac{8}{p-1}\Big(\sum_{\substack{l=1\\l\equiv 0(3)}}^{[\frac{p-1}{4}]}\cos(\pi l) + \sum_{\substack{l=1\\l\not\equiv 0(3)}}^{[\frac{p-1}{4}]}\frac{1}{4}\cos(\pi l)\Big) - \frac{4}{p-1}\right)$$

$$= \frac{p^2(p-1)^2}{p+1}\left(1 - \frac{1}{p} - \frac{2}{p-1}\Big(\sum_{\substack{l=1\\l\equiv 0(3)}}^{[\frac{p-1}{4}]}3\cos(\pi l) + \sum_{l=1}^{[\frac{p-1}{4}]}\cos(\pi l)\Big) - \frac{4}{p-1}\right)$$

$$\geq \frac{p^2(p-1)^2}{p+1}\left(1 - \frac{1}{p} - \frac{4}{p-1}\right) > 0$$

REFERENCES

[AB95] J. L. Alperin and R. Bell. *Groups and representations*, volume 162 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[Ada02] J. Adams. Characters tables of $\mathbf{GL}(2,q)$, $\mathbf{SL}(2,q)$, $\mathbf{PGL}(2,q)$ and $\mathbf{PSL}(2,q)$, http://www.math.umd.edu/∼jda/characters/, 2002.

[AF07a] N. Andruskiewitsch and F. Fantino. On pointed Hopf algebras associated with alternating and dihedral groups, 2007. *Rev. Unión Mat. Argent.* 48:3, 57-71, 2007.

[AF07b] N. Andruskiewitsch and F. Fantino. On pointed Hopf algebras associated with unmixed conjugacy classes in $\mathbb{S}_m$. *J. Math. Phys.*, 48(3):033502, 26, 2007.

[AFGV08] N. Andruskiewitsch, F. Fantino, M. Graña and L. Vendramin, Pointed Hopf algebras over alternating groups are trivial. arXiv:00812.4628.

[AG99] N. Andruskiewitsch and M. Graña. Braided Hopf algebras over non-abelian finite groups. *Bol. Acad. Nac. Cienc. (Córdoba)*, 63:45–78, 1999. Colloquium on Operator Algebras and Quantum Groups (Spanish) (Vaquerías, 1997).

[AS02] 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.

[AZ07] N. Andruskiewitsch and S. Zhang. On pointed Hopf algebras associated to some conjugacy classes in $\mathbb{S}_n$. *Proc. Amer. Math. Soc.*, 135(9):2723–2731 (electronic), 2007.

[CCN+85] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of finite groups*. Oxford University Press, Eynsham, 1985. Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray.

[Dic58] L. Dickson, *Linear groups: With an exposition of the Galois field theory*, Dover Publications Inc., New York, 1958.

[Fan07]   F. Fantino. On pointed hopf algebras associated with the mathieu simple groups, 2007. J. Algebra Appl., accepted, arXiv:0711.3142.

[FGV07] S. Freyre, M. Graña, and L. Vendramin. On Nichols algebras over $\mathbf{SL}(2, \mathbb{F}_q)$ and $\mathbf{GL}(2, \mathbb{F}_q)$. *J. Math. Phys.*, 48(12):123513, 24, 2007.

[GAP]   The GAP Group, 2006. GAP – Groups, Algorithms, and Programming, Version 4.4.9, `http://www.gap-system.org`.

[Go68]   Daniel Gorenstein. *Finite groups*, Harper & Row Publishers, New York, 1968.

[Gr]   Matías Graña, *Nichols algebras of nonabelian group type*, web page at `http://mate.dm.uba.ar/~matiasg/zoo.html`

[Hec05]   I. Heckenberger. Classification of arithmetic root systems of rank 3. *Actas of XVI Colloquium Latinoamericano de Álgebra*, 2005.

[Hec06a] I. Heckenberger. The Weyl groupoid of a Nichols algebra of diagonal type. *Invent. Math.*, 164(1):175–188, 2006.

[Hec06b] I. Heckenberger. Classification of arithmetic root systems. Adv. Math. **220** (2009) 59–124.

[Hup67]   B. Huppert. Endliche Gruppen. I, Die Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin, 1967.

[Ser77]   J-P. Serre. *Linear representations of finite groups*. Springer-Verlag, New York, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.

[ATLAS]   R. Wilson, P. Walsh, J. Tripp, I. Suleiman, R. Parker, S. Norton, S. Nickerson, S. Linton, J. Bray and R. Abbott. Atlas of finite group representationsVersion 3 http://brauer.maths.qmul.ac.uk/Atlas/v3/.

SF, MG, LV: Departamento de Matemática - FCEyN, Universidad de Buenos Aires, Pab I - Ciudad Universitaria, (1428) Buenos Aires - Argentina

LV: Instituto de Ciencias, Universidad Nacional General Sarmiento, J. M. Gutierrez 1150 - Los Polvorines (1613), Provincia de Buenos Aires - Argentina

E-mail address: `(sfreyre|matiasg|lvendramin)@dm.uba.ar`