arXiv:1003.2792v3 [math.GR] 25 Jul 2013

ON BEAUVILLE STRUCTURES FOR $\mathrm{PSL}_2(q)$

SHELLY GARION

Abstract. We characterize Beauville surfaces of unmixed type with group either $\mathrm{PSL}_2(p^e)$ or $\mathrm{PGL}_2(p^e)$, thus extending previous results of Bauer, Catanese and Grunewald, Fuertes and Jones, and Penegini and the author.

1. Introduction

A *Beauville surface* S (over $\mathbb{C}$) is a particular kind of surface isogenous to a *higher product of curves*, i.e., $S = (C_1 \times C_2)/G$ is a quotient of a product of two smooth curves C_1 and C_2 of genus at least two, modulo a free action of a finite group G which acts faithfully on each curve. For Beauville surfaces the quotients C_i/G are isomorphic to $\mathbb{P}^1$ and both projections $C_i \to C_i/G \cong \mathbb{P}^1$ are coverings branched over three points. Beauville surfaces were introduced by Catanese in [5], inspired by a construction of Beauville [3].

A Beauville surface S is either of *mixed* or *unmixed* type according respectively as the action of G exchanges the two factors (and then C_1 and C_2 are isomorphic) or G acts diagonally on the product $C_1 \times C_2$. The subgroup G_0 (of index ≤ 2) of G which preserves the ordered pair (C_1, C_2) is then respectively of index 2 or 1 in G.

Any Beauville surface S can be presented in such a way that the subgroup G_0 of G acts effectively on each of the factors C_1 and C_2. Catanese called such a presentation *minimal* and proved its uniqueness in [5].

In this paper we shall consider only Beauville surfaces of unmixed type so that $G_0 = G$. A natural question is to determine the finite groups which characterize unmixed Beauville surfaces in a minimal presentation. Since a finite group appears as the underlying group of an unmixed Beauville surface in a minimal presentation if and only if it admits an unmixed Beauville structure (see [1, 2]), the above question is equivalent to determining the finite groups admitting an unmixed Beauville structure.

Definition 1.1. An *unmixed Beauville structure* for a finite group G consists of two triples (a_1, b_1, c_1) and (a_2, b_2, c_2) of elements of G which satisfy

(i) $a_1 b_1 c_1 = 1$ and $a_2 b_2 c_2 = 1$,
(ii) $\langle a_1, b_1 \rangle = G$ and $\langle a_2, b_2 \rangle = G$,
(iii) $\Sigma(a_1, b_1, c_1) \cap \Sigma(a_2, b_2, c_2) = \{1\}$,
where, for $i \in \{1, 2\}$, $\Sigma(a_i, b_i, c_i)$ is the union of the conjugacy classes of all powers of a_i, all powers of b_i, and all powers of c_i.

2000 *Mathematics Subject Classification.* 20D06, 20H10, 14J29, 30F99.

The author was supported by a European Postdoctoral Fellowship (EPDI) and by the SFB 878 "Groups, Geometry and Actions".

Moreover denoting the order of an element g in G by $|g|$, we define the *type* τ_i of (a_i, b_i, c_i) to be the triple $(|a_i|, |b_i|, |c_i|)$. In this situation, we say that G admits an *unmixed Beauville structure of type* (τ_1, τ_2).

The question whether a finite group admits an unmixed Beauville structure of a given type is closely related to the question whether it is a quotient of certain triangle groups. More precisely, a necessary condition for a finite group G to admit an unmixed Beauville structure of type $(\tau_1, \tau_2) = \big((r_1, s_1, t_1), (r_2, s_2, t_2)\big)$ is that G is a quotient with torsion free-kernel of the triangle groups T_{r_1,s_1,t_1} and T_{r_2,s_2,t_2}, where for $i \in \{1, 2\}$,

$$T_{r_i,s_i,t_i} = \langle x, y, z : x^{r_i} = y^{s_i} = z^{t_i} = xyz = 1\rangle.$$

Indeed, conditions *(i)* and *(ii)* of Definition 1.1 are equivalent to the condition that G is a quotient of each of the triangle groups $T_{|a_i|,|b_i|,|c_i|}$, for $i \in \{1, 2\}$, with torsion-free kernel.

When investigating the existence of an unmixed Beauville structure for a finite group, one can consider only types (τ_1, τ_2), where for $i \in \{1, 2\}$, $\tau_i = (r_i, s_i, t_i)$ satisfies $1/r_i + 1/s_i + 1/t_i < 1$. Then T_{r_i,s_i,t_i} is a (infinite non-soluble) hyperbolic triangle group and we say that τ_i is *hyperbolic.*

Indeed, if $1/r_i + 1/s_i + 1/t_i > 1$ then T_{r_i,s_i,t_i} is a finite group, and moreover, it is either dihedral or isomorphic to one of A_4, A_5 or S_4. By [1, Proposition 3.6 and Lemma 3.7], in these cases G cannot admit an unmixed Beauville structure. If $1/r_i + 1/s_i + 1/t_i = 1$ then T_{r_i,s_i,t_i} is one of the (soluble infinite) "wall-paper" groups, and by [1, §6], none of its finite quotients can admit an unmixed Beauville structure.

A considerable effort has been made to classify the finite simple groups which admit an unmixed Beauville structure. A finite abelian simple group clearly does not admit an unmixed Beauville structure, since by [1, Theorem 3.4] the only finite abelian groups admitting an unmixed Beauville structure are the abelian groups of the form $Z_n \times Z_n$ where n is a positive integer coprime to 6. (Here Z_n denotes a cyclic group of order n.) In [1], Bauer, Catanese and Grunewald provided the first results on finite non-abelian simple groups admitting an unmixed Beauville structure, and conjectured that all finite non-abelian simple groups admit an unmixed Beauville structure with the exception of A_5.

This conjecture has received much attention and has recently been proved to hold. Concerning the simple alternating groups, it was established in [8] that A_5 is indeed the only one not admitting an unmixed Beauville structure. In [10, 12], the conjecture is shown to hold for the projective special linear groups $\mathrm{PSL}_2(q)$ (where $q > 5$), the Suzuki groups ${}^2B_2(q)$ and the Ree groups ${}^2G_2(q)$ as well as some other families of finite simple groups of Lie type of small rank (where q is sufficiently large). The next major result concerning the investigation of the conjecture with respect to the finite simple groups of Lie type was pursued by Garion, Larsen and Lubotzky who showed in [11] that the conjecture holds for finite non-abelian simple groups of sufficiently large order. The final step regarding the investigation of the conjecture was carried out by Guralnick and Malle [14] and Fairbairn, Magaard and Parker [7] who established its veracity in general.

There has also been an effort to classify the finite quasisimple groups and almost simple groups which admit an unmixed Beauville structure. Recall that a finite group G is *quasisimple* provided $G/Z(G)$ is a non-abelian simple group and $G = [G, G]$. In [10] it was shown that $\mathrm{SL}_2(q)$ (for $q > 5$) admits an unmixed Beauville structure. Fairbairn, Magaard and Parker [7] showed that with the exceptions of $\mathrm{SL}_2(5)$ and $\mathrm{PSL}_2(5) \cong \mathrm{SL}_2(4) \cong A_5$, every finite quasisimple group admits an unmixed Beauville structure. By [2, 8], the almost simple symmetric groups S_n (where $n \geq 5$) admit an unmixed Beauville structure. Recall that a group G is called *almost simple* if there is a non-abelian simple group G_0 such that $G_0 \leq G \leq \mathrm{Aut}(G_0)$.

Another conjecture of Bauer, Catanese and Grunewald proposed in [1] states that if $\tau_1 = (r_1, s_1, t_1)$ and $\tau_2 = (r_2, s_2, t_2)$ are two hyperbolic types, then almost all alternating groups A_n admit an unmixed Beauville structure of type (τ_1, τ_2). This has recently been proved in [12], based on results of Liebeck and Shalev [17], where a similar conjecture is raised, replacing A_n by a finite simple classical group of Lie type of sufficiently large Lie rank.

In contrast, when the Lie rank is very small, as in the case of $\mathrm{PSL}_2(q)$, such a conjecture does not hold. It is therefore the aim of this paper to characterize the possible types of an unmixed Beauville structure for the projective special linear group $\mathrm{PSL}_2(q)$. This is done in Theorem 1. A similar result for the projective general linear group $\mathrm{PGL}_2(q)$ is described in Theorem 2. In particular we show that the almost simple group $\mathrm{PGL}_2(q)$ (where $q \geq 5$) admits an unmixed Beauville structure.

Beauville structures for $\mathrm{PSL}_2(q)$ and $\mathrm{PGL}_2(q)$. If $H = \mathrm{PSL}_2(q)$ (respectively, $\mathrm{PGL}_2(q)$) with $q \leq 5$ (respectively, $q \leq 4$) then H is isomorphic to one of S_3, S_4, A_4 or A_5. As none of these groups admits an unmixed Beauville structure by [1, Proposition 3.6], we can assume hereafter that $q \geq 7$ or $q \geq 5$ according respectively as $H = \mathrm{PSL}_2(q)$ or $\mathrm{PGL}_2(q)$. Unless otherwise stated, we also let $G = \mathrm{PSL}_2(q)$ and $G_1 = \mathrm{PGL}_2(q)$ where $q = p^e$ for some prime number p and some positive integer e.

Our first result is the characterization of the possible types of unmixed Beauville structures for $\mathrm{PSL}_2(q)$.

Theorem 1. *Let $G = \mathrm{PSL}_2(q)$ where $5 < q = p^e$ for some prime number p and some positive integer e. Let $\tau_1 = (r_1, s_1, t_1)$, $\tau_2 = (r_2, s_2, t_2)$ be two hyperbolic triples of integers. Then G admits an unmixed Beauville structure of type (τ_1, τ_2) if and only if the following hold:*

- (*i*) *G is a quotient of T_{r_1,s_1,t_1} and T_{r_2,s_2,t_2} with torsion-free kernel.*
  Equivalently, (e, τ_1) and (e, τ_2) satisfy the conditions given in Table 4 in Section 3.2.
- (*ii*) *If $p = 2$ or e is odd or $q = 9$, then $r_1s_1t_1$ is coprime to $r_2s_2t_2$.*
  If p is odd, e is even and $q > 9$, then $g = \gcd(r_1s_1t_1, r_2s_2t_2) \in \{1, p, p^2\}$. Moreover, if p divides g and τ_1 (respectively τ_2) is up to a permutation (p, p, n) then $n \neq p$ and n is a good G-order *(see Definition 1.2).*

Definition 1.2. Let q be an odd prime power, let $G = \mathrm{PSL}_2(q)$ and let $n > 1$ be an integer. Then n is called a *good G-order* if one of the following holds:

- n is odd and divides either $q - 1$ or $q + 1$;
- n is even and $4n$ divides either $q - 1$ or $q + 1$.

We deduce from Theorem 1 that for any $q > 7$ the group $\mathrm{PSL}_2(q)$ admits unmixed Beauville structures of types

$$\Big((\frac{q-1}{d}, \frac{q-1}{d}, \frac{q-1}{d}), (\frac{q+1}{d}, \frac{q+1}{d}, \frac{q+1}{d}) \Big),$$

and

$$\Big((\frac{q-1}{d}, \frac{q-1}{d}, \frac{q-1}{d}), (\frac{q+1}{d}, \frac{q+1}{d}, p) \Big),$$

where $d = \gcd(2, q-1)$, thus recovering the results appearing in [12] and [10] respectively (the case $q = 7$ is excluded since the triple $(3,3,3)$ is not hyperbolic). In addition, if $q \geq 7$ and $q \neq 9$ then $\mathrm{PSL}_2(q)$ admits an unmixed Beauville structure of type

$$\Big((\frac{q-1}{d}, \frac{q-1}{d}, p), (\frac{q+1}{d}, \frac{q+1}{d}, \frac{q+1}{d}) \Big),$$

(the case $q = 9$ is excluded since $\mathrm{PSL}_2(9)$ is not a quotient of $T_{3,4,4}$, see Table 6 in Section 3.2).

When $q \geq 7$ is odd, $\mathrm{PSL}_2(q)$ admits an unmixed Beauville structure of type

$$\Big((p, p, \frac{q-1}{2}), (\frac{q+1}{2}, \frac{q+1}{2}, \frac{q+1}{2}) \Big),$$

and when $q > 7$, it also admits an unmixed Beauville structure of type

$$\Big((p, p, \frac{q+1}{2}), (\frac{q-1}{2}, \frac{q-1}{2}, \frac{q-1}{2}) \Big),$$

(again, the case $q = 7$ is excluded since the triple $(3,3,3)$ is not hyperbolic).

If $p \geq 7$ is prime then $\mathrm{PSL}_2(p)$ admits unmixed Beauville structures of types

$$\Big((p,p,p), (\frac{p-1}{2}, \frac{p-1}{2}, \frac{p+1}{2}) \Big), \Big((p,p,p), (\frac{p-1}{2}, \frac{p+1}{2}, \frac{p+1}{2}) \Big), \Big((p,p,p), (\frac{p+1}{2}, \frac{p+1}{2}, \frac{p+1}{2}) \Big),$$

and if $p > 7$ is prime, $\mathrm{PSL}_2(p)$ also admits an unmixed Beauville structure of type

$$\Big((p,p,p), (\frac{p-1}{2}, \frac{p-1}{2}, \frac{p-1}{2}) \Big).$$

Note that $\mathrm{PSL}_2(p^e)$ is a quotient of $T_{p,p,p}$ if and only if $e = 1$, by Table 4 in Section 3.2.

Example 1.3. We list below *all* the possible types for Beauville structures for $\mathrm{PSL}_2(q)$ where $q = 7, 8, 9$. This is a direct consequence of Theorem 1, and in particular it follows from Table 6 in Section 3.2. This table describes all the hyperbolic triples satisfying condition *(i)*, and one can construct all possible pairs of these triples and check whether they are coprime, thus also satisfying condition *(ii)*. It can easily be verified by a computer, for example using MAGMA.

- $\mathrm{PSL}_2(7)$:
$$\big((3,7,7),(4,4,4)\big), \big((3,4,4),(7,7,7)\big), \big((3,3,7),(4,4,4)\big),$$
$$\big((4,4,4),(7,7,7)\big), \big((3,3,4),(7,7,7)\big).$$
(see also [9, Theorem 13]).
- $\mathrm{PSL}_2(8)$:
$$\big((2,7,7),(9,9,9)\big), \big((2,9,9),(7,7,7)\big), \big((7,7,7),(9,9,9)\big), \big((2,3,9),(7,7,7)\big),$$
$$\big((3,9,9),(7,7,7)\big), \big((3,3,9),(7,7,7)\big), \big((2,7,7),(3,9,9)\big), \big((2,7,7),(3,3,9)\big).$$
- $\mathrm{PSL}_2(9) \cong A_6$:
$$\big((3,5,5),(4,4,4)\big), \big((4,4,4),(5,5,5)\big), \big((3,3,5),(4,4,4)\big), \big((3,3,4),(5,5,5)\big).$$

Observe that condition *(iii)* of Definition 1.1 is clearly satisfied under the assumption that $r_1s_1t_1$ is coprime to $r_2s_2t_2$. The example of the alternating groups shows that this assumption is not always necessary. But in the case of $\mathrm{PSL}_2(q)$ Theorem 1 shows that this assumption is actually not far from being necessary.

However, by Theorem 1, for any odd prime power $q > 3$ the group $\mathrm{PSL}_2(q^2)$ admits an unmixed Beauville structure of type

$$\left(p, \frac{q^2-1}{2}, \frac{q^2-1}{2}\right), \left(p, \frac{q^2+1}{2}, \frac{q^2+1}{2}\right)\Big) .$$

In particular, $\mathrm{PSL}_2(q^2)$ is a quotient of the hyperbolic triangle groups $T_{p,(q^2\pm1)/2,(q^2\pm1)/2}$ by Table 4 in Section 3.2 and Lemma 3.6, since $\mathrm{PSL}_2(q^2)$ contains elements of orders $(q^2\pm1)/2$, but none of its subfield subgroups contain such elements. In addition, $\mathrm{PSL}_2(q^2)$ also admits unmixed Beauville structures of types

$$\big((p,p,t_1),(p,p,t_2)\big)$$

for certain t_1, t_2 dividing $(q^2-1)/2$, $(q^2+1)/2$ respectively (see Lemma 4.5).

Example 1.4. We list below *all* the possible types of the form $\big((p,p,t_1),(p,p,t_2)\big)$ for Beauville structures for $\mathrm{PSL}_2(q^2)$ where $q = 5, 7, 11, 13$. This is a direct consequence of Theorem 1, and in particular it follows from Table 9 in Section 3.5. This table describes all the *good G-orders*, and so one needs only to check when they are pairwise coprime, thus satisfying condition *(ii)*. It can easily be verified by a computer, for example using MAGMA.

- $\mathrm{PSL}_2(25)$:
$$\big((5,5,6),(5,5,13)\big).$$
- $\mathrm{PSL}_2(49)$:
$$\big((7,7,5),(7,7,6)\big), \big((7,7,5),(7,7,12)\big), \big((7,7,25),(7,7,6)\big), \big((7,7,25),(7,7,12)\big).$$
- $\mathrm{PSL}_2(121)$:
$$\big((11,11,10),(11,11,61)\big), \big((11,11,15),(11,11,61)\big), \big((11,11,30),(11,11,61)\big).$$
- $\mathrm{PSL}_2(169)$:
$$\big((13,13,5),(13,13,14)\big), \big((13,13,5),(13,13,17)\big), \big((13,13,5),(13,13,21)\big),$$
$$\big((13,13,5),(13,13,42)\big), \big((13,13,14),(13,13,17)\big), \big((13,13,14),(13,13,85)\big),$$
$$\big((13,13,17),(13,13,21)\big), \big((13,13,17),(13,13,42)\big), \big((13,13,21),(13,13,85)\big),$$
$$\big((13,13,42),(13,13,85)\big).$$

Our next result characterizes the possible unmixed Beauville structures for $\mathrm{PGL}_2(q)$.

Theorem 2. *Let $G_1 = \mathrm{PGL}_2(q)$ where $3 < q = p^e$ for some odd prime number p and some positive integer e. Let $\tau_1 = (r_1, s_1, t_1)$, $\tau_2 = (r_2, s_2, t_2)$ be two hyperbolic triples of integers. Then G_1 admits a Beauville structure of type (τ_1, τ_2) if and only if the following hold:*

(i) G_1 is a quotient of T_{r_1,s_1,t_1} and T_{r_2,s_2,t_2} with torsion-free kernel.
Equivalently, (e, τ_1) and (e, τ_2) satisfy the conditions given in Table 5 in Section 3.2.

(*ii*) *Each of the integers*

$$\gcd(r_1,r_2),\ \gcd(r_1,s_2),\ \gcd(r_1,t_2),$$
$$\gcd(s_1,r_2),\ \gcd(s_1,s_2),\ \gcd(s_1,t_2),$$
$$\gcd(t_1,r_2),\ \gcd(t_1,s_2),\ \gcd(t_1,t_2),$$

is equal to 1 *or* 2.

(*iii*) *All even elements in one of the triples divide* $q-1$, *while all even elements in the other triple divide* $q+1$.

(*iv*) *The integer* 2 *appears only in a* good involuting triple w.r.t q *(see Definition 1.5).*

Definition 1.5. Let q be an odd prime power. A hyperbolic triple of integers $(r,s,2)$ is called a *good involuting triple w.r.t q* if one of the following holds:

- $q \equiv 1 \bmod 4$, and r,s both divide $q-1$ but not $(q-1)/2$;
- $q \equiv 3 \bmod 4$, and r,s both divide $q+1$ but not $(q+1)/2$;
- $q \equiv 1 \bmod 4$, r divides $q+1$ but not $(q+1)/2$, and s is odd;
- $q \equiv 1 \bmod 4$, s divides $q+1$ but not $(q+1)/2$, and r is odd;
- $q \equiv 3 \bmod 4$, r divides $q-1$ but not $(q-1)/2$, and s is odd;
- $q \equiv 3 \bmod 4$, s divides $q-1$ but not $(q-1)/2$, and r is odd.

We deduce from Theorem 2 that for any odd prime power $q \geq 5$ the group $\mathrm{PGL}_2(q)$ admits an unmixed Beauville structure of type

$$\big((p,q-1,q-1),((q+1)/2,q+1,q+1)\big),$$

and if $q \geq 7$ it also admits unmixed Beauville structures of types

$$\big(((q-1)/2,q-1,q-1),(p,q+1,q+1)\big),$$

and

$$\big(((q-1)/2,q-1,q-1),((q+1)/2,q+1,q+1)\big),$$

(the case $q=5$ is excluded since the triple $(2,4,4)$ is not hyperbolic).

In addition, if $9 \leq q \equiv 1 \bmod 4$ then $\mathrm{PGL}_2(q)$ admits unmixed Beauville structures of types

$$\big((2,p,q+1),(2,q-1,q-1)\big),\ \big((2,p,q+1),((q-1)/2,q-1,q-1)\big),$$
$$\big((2,q-1,q-1),(p,q+1,q+1)\big),\ \big((2,q-1,q-1),((q+1)/2,q+1,q+1)\big),$$
$$\big((2,(q+1)/2,q+1),(2,q-1,q-1)\big),\ \big((2,(q+1)/2,q+1),((q-1)/2,q-1,q-1)\big),$$
$$\big((2,(q+1)/2,q+1),(p,q-1,q-1)\big),$$

whereas if $7 \leq q \equiv 3 \bmod 4$ then $\mathrm{PGL}_2(q)$ admits unmixed Beauville structures of types

$$\big((2,p,q-1),(2,q+1,q+1)\big),\ \big((2,p,q-1),((q+1)/2,q+1,q+1)\big),$$
$$\big((2,q+1,q+1),(p,q-1,q-1)\big),\ \big((2,q+1,q+1),((q-1)/2,q-1,q-1)\big),$$

and if moreover $q \geq 11$ then $\mathrm{PGL}_2(q)$ also admits Beauville structures of types

$$\big((2,(q-1)/2,q-1),(2,q+1,q+1)\big),\ \big((2,(q-1)/2,q-1),((q+1)/2,q+1,q+1)\big),$$
$$\big((2,(q-1)/2,q-1),(p,q+1,q+1)\big).$$

These results follow from Definition 1.5 and Table 8 in Section 3.4.

Example 1.6. We list below *all* the possible types for Beauville structures for $\mathrm{PGL}_2(q)$ where $q = 5, 7, 9$. This is a direct consequence of Theorem 2, and in particular it follows from Table 6 in Section 3.2. This table describes all the hyperbolic triples satisfying condition *(i)*, and one can construct all possible pairs of these triples and check whether they also satisfy conditions *(ii), (iii)* and *(iv)*. It can easily be verified by a computer, for example using Magma.

- $\mathrm{PGL}_2(5)$:

$$\big((3,6,6),(4,4,5)\big).$$

- $\mathrm{PGL}_2(7)$:

$$\big((2,6,7),(2,8,8)\big),\big((2,6,7),(4,8,8)\big),\big((2,8,8),(6,6,7)\big),\big((4,8,8),(6,6,7)\big),$$
$$\big((3,6,6),(4,8,8)\big),\big((2,8,8),(3,6,6)\big),\big((3,6,6),(7,8,8)\big).$$

- $\mathrm{PGL}_2(9)$:

$$\big((4,8,8),(5,10,10)\big),\big((2,5,10),(3,8,8)\big),\big((2,8,8),(5,10,10)\big),\big((2,3,10),(2,8,8)\big),$$
$$\big((2,5,10),(2,8,8)\big),\big((2,5,10),(4,8,8)\big),\big((3,10,10),(4,8,8)\big),$$
$$\big((3,8,8),(5,10,10)\big),\big((2,8,8),(3,10,10)\big),\big((2,3,10),(4,8,8)\big).$$

Example 1.7. We list below *all* the possible types of the form $\big((2,r_1,s_1),(2,r_2,s_2)\big)$ for Beauville structures for $\mathrm{PGL}_2(q)$ where $q = 11, 13$. This is a direct consequence of Theorem 2, and in particular it follows from Table 7 in Section 3.2, in the same way as the previous example.

- $\mathrm{PGL}_2(11)$:

$$\big((2,4,12),(2,5,10)\big),\big((2,4,12),(2,10,11)\big),\big((2,10,11),(2,12,12)\big),\big((2,5,10),(2,12,12)\big).$$

- $\mathrm{PGL}_2(13)$:

$$\big((2,7,14),(2,12,12)\big),\big((2,4,12),(2,13,14)\big),\big((2,12,12),(2,13,14)\big),\big((2,4,12),(2,7,14)\big).$$

Organization. This paper is organized as follows. In Section 2 we present some of the basic properties of the groups $\mathrm{PSL}_2(q)$ and $\mathrm{PGL}_2(q)$ that are needed later. In Section 3 we describe the results of [15, 16] characterizing, for a given q, the hyperbolic triangle groups which have $\mathrm{PSL}_2(q)$ (respectively, $\mathrm{PGL}_2(q)$) as quotients with torsion-free kernel, and discuss the notions of a *good G-order* and a *good involuting triple w.r.t q*. The proofs of Theorems 1 and 2 are presented in Section 4.

Acknowledgement. I am thankful to Fritz Grunewald for introducing me to the fascinating world of Beauville structures and for giving me inspiration and motivation. He is deeply missed.

I am grateful to Alexandre Zalesski for his enlightening comments. I am thankful to Ingrid Bauer and Fabrizio Catanese for many useful discussions, to Matteo Penegini for many interesting discussions and for his remarks on this manuscript, to Tatiana Bandman for patiently answering my questions, and to Claude Marion for kindly providing me with his recent preprints.

I am grateful to the referee for his careful reading of this manuscript and for his valuable comments.

2. Preliminaries

In this section we shall describe some well-known properties of the groups $\mathrm{PSL}_2(q)$ and $\mathrm{PGL}_2(q)$, their elements and their subgroups (see for example [6], [13, §2.8] and [20, §6]), that will be used later on.

2.1. The groups $\mathrm{PSL}_2(q)$ and $\mathrm{PGL}_2(q)$. We let $\mathbb{F}_q$ denote a finite field of q elements where $q = p^e$ for some prime number p and some positive integer e. Recall that $\mathrm{GL}_2(q)$ is the group of invertible 2×2 matrices over $\mathbb{F}_q$, and $\mathrm{SL}_2(q)$ is the subgroup of $\mathrm{GL}_2(q)$ comprising the matrices with determinant 1. Then $\mathrm{PGL}_2(q)$ and $\mathrm{PSL}_2(q)$ are the quotients of $\mathrm{GL}_2(q)$ and $\mathrm{SL}_2(q)$ by their respective centers. In addition, $\mathrm{PSL}_2(q)$ is simple for $q \neq 2, 3$. We shall denote by G, G_0, G_1 the groups $\mathrm{PSL}_2(q)$, $\mathrm{SL}_2(q)$ and $\mathrm{PGL}_2(q)$ respectively.

Also recall that G can be viewed as a normal subgroup of G_1 whose index is 2 if p is odd, otherwise G can be identified with G_1. Let $d = \gcd(2, q-1)$. Then the orders of G_0, G_1 and G are $q(q-1)(q+1)$, $q(q-1)(q+1)$ and $q(q-1)(q+1)/d$ respectively.

Let $\mathbb{P}_1(q)$ denote the projective line over $\mathbb{F}_q$. Then G_1 acts on $\mathbb{P}_1(q)$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : \quad z \mapsto \frac{az+b}{cz+d}$$

hence, it can be identified with the group of projective transformations on $\mathbb{P}_1(q)$. Under this identification, G is the set of all transformations for which $ad - bc$ is a square in $\mathbb{F}_q$.

2.2. Group elements. One can classify the elements of G and G_1 according to their action on $\mathbb{P}_1(q)$. This is the same as considering the possible Jordan forms of their pre-images. For a matrix $A \in G_0$ we will denote by $\bar{A}$ its image in G.

Table 1 lists the three types of elements according to whether they have $0, 1$ or 2 fixed points in $\mathbb{P}_1(q)$.

type	action on $\mathbb{P}_1(q)$	order in $\mathrm{PGL}_2(q)$	order in $\mathrm{PSL}_2(q)$
unipotent	fixes one point	p	p
split	fixes two points	divides $q-1$	divides $(q-1)/d$
non-split	no fixed points	divides $q+1$	divides $(q+1)/d$

Table 1. Elements in $\mathrm{PGL}_2(q)$ and $\mathrm{PSL}_2(q)$

Table 2 describes the Jordan forms of the three types of elements in G, according to whether the characteristic polynomial $P(\lambda) := \lambda^2 - \alpha\lambda + 1$ of the pre-image $A \in G_0$ (where α is the trace of A) has 0, 1 or 2 distinct roots in $\mathbb{F}_q$.

2.3. Subgroups of $\mathrm{PSL}_2(q)$. Table 3 specifies all the subgroups of $G = \mathrm{PSL}_2(q)$ up to isomorphism following [20, Theorems 6.25 and 6.26].

These subgroups can be divided into the following three classes, following Macbeath [18]. The subgroups isomorphic to $\mathrm{PSL}_2(q_1)$ or $\mathrm{PGL}_2(q_1)$ are usually called *subfield* subgroups (since $\mathbb{F}_{q_1}$ is a subfield of $\mathbb{F}_q$). Since A_4, S_4, A_5 and dihedral groups correspond to the finite triangle groups, that is, triangle groups $T_{r,s,t}$ such that $1/r+1/s+1/t > 1$, we will call them *small* subgroups. For convenience we will refer to the other subgroups, namely subgroups of the Borel and cyclic subgroups, as *structural* subgroups.

type	roots of $P(\lambda)$	Jordan form in $\mathrm{SL}_2(\overline{\mathbb{F}}_p)$	conjugacy classes
unipotent	1 root	$\begin{pmatrix} \pm 1 & 1 \\ 0 & \pm 1 \end{pmatrix}$ $\alpha = \pm 2$	d classes in G which unite in G_1
split	2 roots	$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ where $a \in \mathbb{F}_q^*$ and $a + a^{-1} = \alpha$	one class in G for each α
non-split	no roots	$\begin{pmatrix} a & 0 \\ 0 & a^q \end{pmatrix}$ where $a \in \mathbb{F}_{q^2}^* \setminus \mathbb{F}_q^*$ $a^{q+1} = 1$ and $a + a^q = \alpha$	one class in G for each α

Table 2. Elements in $\mathrm{PSL}_2(q)$ and their Jordan forms

type	maximal order	conditions
p-group	q	–
Frobenius (Borel)	$q(q-1)/d$	–
cyclic (split)	$(q-1)/d$	–
dihedral (split)	$2(q-1)/d$	–
cyclic (non-split)	$(q+1)/d$	–
dihedral (non-split)	$2(q+1)/d$	–
$\mathrm{PSL}_2(q_1)$	–	$q = q_1^m$ $(m \in \mathbb{N})$
$\mathrm{PGL}_2(q_1)$	–	q is odd, $q = q_1^{2m}$ $(m \in \mathbb{N})$
A_4	12	q is odd; or $q = 2^e$, e even
S_4	24	$q^2 \equiv 1 \bmod 16$
A_5	60	$p = 5$ or $q^2 \equiv 1 \bmod 5$

Table 3. Subgroups of $\mathrm{PSL}_2(q)$

Regarding the conjugacy classes of these subgroups, we recall that there is a single conjugacy class in G of dihedral subgroups of order $2(q-1)/d$ (respectively, $2(q+1)/d$), so that there is a single conjugacy class in G of cyclic subgroups of order $(q-1)/d$ (respectively, $(q+1)/d$).

We also recall that for any divisor f of e, G has a G_1-conjugacy class of subgroups isomorphic to $\mathrm{PSL}_2(p^f)$. Moreover, if p is odd and e is even then G has a G_1-conjugacy class of subgroups isomorphic to $\mathrm{PGL}_2(p^f)$ for any f dividing $e/2$.

3. Hyperbolic triangle groups and $\mathrm{PSL}_2(q), \mathrm{PGL}_2(q)$

In order to characterize the possible types of an unmixed Beauville structure for $\mathrm{PSL}_2(q)$ (respectively, $\mathrm{PGL}_2(q)$) it is crucial to know given q the hyperbolic triangle groups which have $\mathrm{PSL}_2(q)$ (respectively, $\mathrm{PGL}_2(q)$) as quotients with torsion-free kernel.

Given a prime power q the hyperbolic triangle groups which have $\mathrm{PSL}_2(q)$ (respectively, $\mathrm{PGL}_2(q)$) as quotients with torsion-free kernel have been determined by Langer and Rosenberger [15] and Levin and Rosenberger [16], following Macbeath [18]. It follows that if (r,s,t) is hyperbolic, then for almost all primes p, there is precisely one group of the form $\mathrm{PSL}_2(p^e)$ or $\mathrm{PGL}_2(p^e)$ which is a homomorphic image of $T_{r,s,t}$ with torsion-free kernel. The remaining primes p satisfy that at least one of r,s,t is a multiple of p which is not p, and for such primes, for all positive integers e, neither $\mathrm{PSL}_2(p^e)$ nor $\mathrm{PGL}_2(p^e)$ contains three elements of orders r,s and t. Recently, Marion [19] has provided another proof for the case where r,s,t are primes relying on probabilistic group theoretical methods.

Before stating these results in §3.2 we introduce some notation in §3.1. In §3.3 we present the main results of Macbeath [18] and explain the concept for a hyperbolic triple (r,s,t) to be *irregular w.r.t q*. In Sections §3.4 and §3.5 we discuss the notions of *good involuting triple w.r.t q* and *good G-order* respectively.

3.1. **Orders and traces.** If n is a positive integer dividing $(q-1)/d$ or $(q+1)/d$ or equal to p, then $G=\mathrm{PSL}_2(q)$ contains an element of order n. In this case, we will say that n is a *G-order*. Similarly, if n is a positive integer dividing $q-1$ or $q+1$ or equal to p, then $G_1=\mathrm{PGL}_2(q)$ contains an element of order n, and we will say that n is a *G_1-order*.

More precisely, one would like to determine the smallest positive integer e such that $\mathrm{PGL}_2(p^e)$ (respectively $\mathrm{PSL}_2(p^e)$) contains an element of order n, hence we introduce the following notation.

For a prime p, a positive integer n coprime to p, and a k-tuple $(n_1,\dots,n_k)$ of positive integers n_i each coprime to p or equal to p, we let

$$\mu_{\mathrm{PGL}}(p,p)=\mu_{\mathrm{PSL}}(p,p)=1,$$

$$\mu_{\mathrm{PGL}}(p,n)=\min\bigl\{f>0\,:\,p^f\equiv\pm1 \bmod n\bigr\},$$

$$\mu_{\mathrm{PSL}}(p,n)=\min\bigl\{f>0\,:\,p^f\equiv\pm1 \bmod (\gcd(2,n)\cdot n)\bigr\},$$

$$\mu_{\mathrm{PGL}}(p;n_1,\dots,n_k)=\mathrm{lcm}\bigl(\mu_{\mathrm{PGL}}(p,n_1),\dots,\mu_{\mathrm{PGL}}(p,n_k)\bigr)$$

and

$$\mu_{\mathrm{PSL}}(p;n_1,\dots,n_k)=\mathrm{lcm}\bigl(\mu_{\mathrm{PSL}}(p,n_1),\dots,\mu_{\mathrm{PSL}}(p,n_k)\bigr).$$

Therefore, $\mu_{\mathrm{PGL}}(p,n)$ (respectively $\mu_{\mathrm{PSL}}(p,n)$) is the smallest positive integer e such that $\mathrm{PGL}_2(p^e)$ (respectively $\mathrm{PSL}_2(p^e)$) contains an element of order n. Also $\mu_{\mathrm{PGL}}(p;n_1,\dots,n_k)$ (respectively $\mu_{\mathrm{PSL}}(p;n_1,\dots,n_k)$) is the smallest positive integer e such that $\mathrm{PGL}_2(p^e)$ (respectively $\mathrm{PSL}_2(p^e)$) contains elements of orders $n_1,\dots,n_k$.

For any non-central matrix $A\in G_0$, its trace $\mathrm{tr}(A)$ determines uniquely the G_1-conjugacy class of $\bar{A}$ (see Table 2), and so also the order of $\bar{A}$ is uniquely determined by $\mathrm{tr}(A)$.

Hence, for a G-order n, we denote

$$\mathcal{T}_q(n)=\{\alpha\in\mathbb{F}_q\,:\,\alpha=\mathrm{tr}(A),A\in G_0,|\bar{A}|=n\}. \tag{1}$$

It is easy to see from Table 2 that for any prime power q, $\mathcal{T}_q(2)=\{0\}$, $\mathcal{T}_q(3)=\{\pm1\}$, and for any odd $q=p^e$, $\mathcal{T}_q(p)=\{\pm2\}$. Moreover, when q is odd, then $\alpha\in\mathcal{T}_q(n)$ if and only if $-\alpha\in\mathcal{T}_q(n)$. In fact, for any prime power q and integer $n>1$, $\mathcal{T}_q(n)$ can be effectively computed as follows.

Proposition 3.1. *Denote by $\mathcal{P}_q(n)$ the set of primitive roots of unity of order n in $\mathbb{F}_q$.*

- *Let $q = 2^e$ for some positive integer e and let $n > 1$ be an integer, then*

$$\mathcal{T}_q(n) = \begin{cases} \{0\} & if\ n = 2 \\ \{a + a^{-1} : a \in \mathcal{P}_q(n)\} & if\ n\ divides\ q-1 \\ \{b + b^q : b \in \mathcal{P}_{q^2}(n)\} & if\ n\ divides\ q+1 \\ \emptyset & otherwise \end{cases} \tag{2}$$

- *Let $q = p^e$ for some odd prime p and some positive integer e and let $n > 1$ be an integer, then*

$$\mathcal{T}_q(n) = \begin{cases} \{\pm 2\} & if\ n = p \\ \{\pm(a + a^{-1}) : a \in \mathcal{P}_q(2n)\} & if\ n\ divides\ \frac{q-1}{2} \\ \{\pm(b + b^q) : b \in \mathcal{P}_{q^2}(2n)\} & if\ n\ divides\ \frac{q+1}{2} \\ \emptyset & otherwise \end{cases} \tag{3}$$

Proof. We prove the case where q is odd and n divides $(q-1)/2$. The other cases are similar.

Assume first that n is even. Let a be a primitive root of unity of order $2n$. Then $-a$ is also a primitive root of unity of order $2n$, and $(-a)^n = a^n = -1$. Thus the matrices

$$A = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \quad \text{and} \quad -A = \begin{pmatrix} -a & 0 \\ 0 & -a^{-1} \end{pmatrix}$$

both reduce to the same element $\bar{A} \in G$ of order n. Hence, $a + a^{-1}$ and $-(a + a^{-1})$ both belong to $\mathcal{T}_q(n)$. $\mathcal{T}_q(n)$ contains only the elements of the claimed form, since it suffices to consider only the conjugacy classes of elements of G, described in Table 2.

Now assume that n is odd. Then a is a primitive root of unity of order n if and only if $-a$ is a primitive root of unity of order $2n$. In this case, $(-a)^n = -a^n = -1$. Thus the matrices

$$A = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \quad \text{and} \quad -A = \begin{pmatrix} -a & 0 \\ 0 & -a^{-1} \end{pmatrix}$$

both reduce to the same element $\bar{A} \in G$ of order n. Hence, $a + a^{-1}$ and $-(a + a^{-1})$ both belong to $\mathcal{T}_q(n)$. Again, considering the conjugacy classes appearing in Table 2 shows that $\mathcal{T}_q(n)$ contains only the elements of the claimed form. □

3.2. **Hyperbolic triples and** $\mathrm{PSL}_2(q), \mathrm{PGL}_2(q)$**.** The following theorems summarize the results in [15, Theorems 4.1 and 4.2] and [16, Theorems 1 and 2], which characterize, for a given q, the hyperbolic triangle groups which have $\mathrm{PSL}_2(q)$ (respectively, $\mathrm{PGL}_2(q)$) as quotients with torsion-free kernel. The notion of an *irregular triple w.r.t q* is given in Lemma 3.6 in §3.3.

Theorem 3.2. [15, 16]. *Given a prime p and a hyperbolic triple (r, s, t) of integers, $\mathrm{PSL}_2(p^e)$ is a quotient of $T_{r,s,t}$ with torsion-free kernel if and only if (r, s, t) and e satisfy one of the conditions given in Table 4.*

Theorem 3.3. [15, 16]. *Given an odd prime p and a hyperbolic triple (r, s, t) of integers, $\mathrm{PGL}_2(p^e)$ is a quotient of $T_{r,s,t}$ with torsion-free kernel if and only if (r, s, t) and e satisfy one of the conditions given in Table 5.*

The following corollary follows immediately from Theorems 3.2 and 3.3.

p	(r,s,t)	e	*further conditions*
$p \geq 5$	(p,p,p)	1	-
$p \geq 3$	*permutation of* (p,p,t') $\gcd(t',p)=1$	$\mu_{\mathrm{PSL}}(p,t')$	-
$p \geq 3$	*permutation of* (p,s',t') $\gcd(s't',p)=1$	$\mu_{\mathrm{PSL}}(p;s',t')$	*either at most one of* r,s,t *is even, or: if at least two of* r,s,t *are even then* (r,s,t) *is not irregular w.r.t* p^e
$p \geq 3$	$\gcd(rst,p)=1$	$\mu_{\mathrm{PSL}}(p;r,s,t)$	
$p=2$	-	$\mu_{\mathrm{PSL}}(2;r,s,t)$	-

TABLE 4. Hyperbolic triangle groups $T_{r,s,t}$ which have $\mathrm{PSL}_2(p^e)$ as quotients

(r,s,t)	e	*further conditions*
permutation of (p,s',t') $\gcd(s't',p)=1$	$\mu_{\mathrm{PSL}}(p;s',t')/2$	*at least two of* r,s,t *are even and* (r,s,t) *is irregular w.r.t* p^{2e}
$\gcd(rst,p)=1$	$\mu_{\mathrm{PSL}}(p;r,s,t)/2$	

TABLE 5. Hyperbolic triangle groups $T_{r,s,t}$ which have $\mathrm{PGL}_2(p^e)$ as quotients

Corollary 3.4. *Given a prime p and a hyperbolic triple (r,s,t) of integers, such that each of r,s,t is either coprime to p or equal to p, there exists a unique exponent e such that $\mathrm{PSL}_2(p^e)$ or $\mathrm{PGL}_2(p^e)$ is a quotient of $T_{r,s,t}$ with torsion-free kernel. More precisely, let $e=\mu_{\mathrm{PSL}}(p;r,s,t)$ then*

(a) *If (r,s,t) is* not irregular w.r.t to *p^e then $\mathrm{PSL}_2(p^e)$ is a quotient of $T_{r,s,t}$ with torsion-free kernel.*
(b) *If e is even and (r,s,t) is* irregular w.r.t to *p^e then $\mathrm{PGL}_2(p^{e/2})$ is a quotient of $T_{r,s,t}$ with torsion-free kernel.*

Example 3.5. In Tables 6 and 7 we present *all* the hyperbolic triples (r,s,t) of integers such that $\mathrm{PSL}_2(q)$ (respectively $\mathrm{PGL}_2(q)$) is a quotient of $T_{r,s,t}$ with torsion-free kernel, for $q=3,4,5,7,8,9,11,13$. These triples were computed using MAGMA.

The *irregular triples w.r.t* q^2 are divided according to the three cases of Lemma 3.6, and among them, the *good involuting triples w.r.t* q are marked in **bold** (see §3.3 and §3.4).

3.3. **Generating triples and irregular triples.** Macbeath [18] classified the pairs of elements in G in a way which makes it easy to decide what kind of subgroup they generate. He called a triple (A,B,C) of elements in G (respectively G_0) such that $ABC=1$ a *G-triple* (respectively *G_0-triple*). So if (A,B,C) is a G_0-triple then $(\bar{A},\bar{B},\bar{C})$ is a G-triple.

By [18, Theorem 1], for any $(\alpha,\beta,\gamma)\in\mathbb{F}_q^3$, there exists a G_0-triple (A,B,C) such that A, B and C have respective traces α, β and γ. Hence, if (r,s,t) is a triple of G-orders then there exists a G-triple $(\bar{A},\bar{B},\bar{C})$ such that $\bar{A}$, $\bar{B}$ and $\bar{C}$ have respective orders r, s and t.

Macbeath [18] called a G_0-triple (A,B,C) *singular* if its corresponding traces (α,β,γ) satisfy the equality

$$\alpha^2+\beta^2+\gamma^2-\alpha\beta\gamma-4=0. \tag{4}$$

Moreover, by [18, Theorem 2], a G_0-triple (A,B,C) is singular if and only if the corresponding G-triple $(\bar{A},\bar{B},\bar{C})$ satisfies that $\langle\bar{A},\bar{B}\rangle$ is a *structural* subgroup of G.

q	G-orders	G_1-orders	triples for G	triples for G_1 (irregular)
3	$2,3$	$2,3,$ 4	None	(α) $(3,4,4)$
4	$2,3,5$	$2,3,5$	$(2,5,5)$, $(3,3,5)$, $(3,5,5)$, $(5,5,5)$	None
5	$2,3,5$	$2,3,5,$ $4,6$	$(2,5,5)$, $(3,3,5)$, $(3,5,5)$, $(5,5,5)$	(α) $(3,4,4)$, $(3,4,6)$, $(3,6,6)$, $(4,4,5)$, $(4,5,6)$, $(5,6,6)$ (β) $(2,4,6)$, $(2,6,6)$ (γ) $(2,4,5)$, $(\mathbf{2},\mathbf{5},\mathbf{6})$
7	$2,3,4,7$	$2,3,4,7,$ $6,8$	$(2,3,7)$, $(2,4,7)$, $(2,7,7)$, $(3,3,4)$, $(3,3,7)$, $(3,4,4)$, $(3,4,7)$, $(3,7,7)$, $(4,4,4)$, $(4,4,7)$, $(4,7,7)$, $(7,7,7)$	(α) $(3,6,6)$, $(3,6,8)$, $(3,8,8)$, $(4,6,6)$, $(4,6,8)$, $(4,8,8)$, $(6,6,7)$, $(6,7,8)$, $(7,8,8)$ (β) $(2,6,6)$, $(2,6,8)$, $(\mathbf{2},\mathbf{8},\mathbf{8})$ (γ) $(2,3,8)$, $(2,4,6)$, $(2,4,8)$, $(\mathbf{2},\mathbf{6},\mathbf{7})$, $(2,7,8)$
8	$2,3,7,9$	$2,3,7,9$	$(2,3,7)$, $(2,3,9)$, $(2,7,7)$, $(2,7,9)$, $(2,9,9)$, $(3,3,7)$, $(3,3,9)$, $(3,7,7)$, $(3,7,9)$, $(3,9,9)$, $(7,7,7)$, $(7,7,9)$, $(7,9,9)$, $(9,9,9)$	None
9	$2,3,4,5$	$2,3,4,5,$ $8,10$	$(2,4,5)$, $(2,5,5)$, $(3,3,4)$, $(3,3,5)$, $(3,4,5)$, $(3,5,5)$, $(4,4,4)$, $(4,4,5)$, $(4,5,5)$, $(5,5,5)$	(α) $(3,8,8)$, $(3,8,10)$, $(3,10,10)$, $(4,8,8)$, $(4,8,10)$, $(4,10,10)$, $(5,8,8)$, $(5,8,10)$, $(5,10,10)$ (β) $(\mathbf{2},\mathbf{8},\mathbf{8})$, $(2,8,10)$, $(2,10,10)$ (γ) $(2,3,8)$, $(\mathbf{2},\mathbf{3},\mathbf{10})$, $(2,4,8)$, $(2,4,10)$, $(2,5,8)$, $(\mathbf{2},\mathbf{5},\mathbf{10})$

TABLE 6. Hyperbolic triples for G and hyperbolic triples for G_1 (irregular w.r.t q^2), where $q = 3,4,5,7,8,9$.

Observe that if $\langle \bar{A}, \bar{B} \rangle$ is a *small* subgroup, then the corresponding orders (r,s,t) of $(\bar{A}, \bar{B}, \bar{C})$ satisfy that either two of r,s,t equal to 2 or $r,s,t \in \{2,3,4,5\}$, but the converse might not be true. Indeed, if $(\bar{A}, \bar{B}, \bar{C})$ is a G-triple of respective orders (r,s,t) such that (r,s,t) is hyperbolic and $r,s,t \in \{2,3,4,5\}$ then $\langle \bar{A}, \bar{B} \rangle$ is not necessarily a *small* subgroup (see [16]).

In fact, when (r,s,t) is a hyperbolic triple of G-orders, then there is enough freedom in choosing the traces $\alpha \in \mathcal{T}_q(r)$, $\beta \in \mathcal{T}_q(s)$ and $\gamma \in \mathcal{T}_q(t)$, such that Equation (4) does not hold, and in addition, they do not correspond to a G-triple which generates a *small* subgroup (see [15, Lemma 3.3] and [16]). Therefore, if (r,s,t) is a hyperbolic triple of G-orders then there exists a G-triple (A,B,C) such that A, B and C have respective orders r, s and t, and moreover, $\langle A, B \rangle$ is a *subfield* subgroup of G.

q	G-orders	G_1-orders	triples for G		triples for G_1 (irregular)
11	$2,3,$ 5, 6, 11	$2,3,$ 5, 6, 11, 4, 10, 12	$(2,3,11)$, $(2,5,5)$, $(2,5,6)$, $(2,5,11)$, $(2,6,6)$, $(2,6,11)$, $(2,11,11)$, $(3,3,5)$, $(3,3,6)$, $(3,3,11)$, $(3,5,5)$, $(3,5,6)$, $(3,5,11)$, $(3,6,6)$, $(3,6,11)$, $(3,11,11)$, $(5,5,5)$, $(5,5,6)$, $(5,5,11)$, $(5,6,6)$, $(5,6,11)$, $(5,11,11)$, $(6,6,6)$, $(6,6,11)$, $(6,11,11)$, $(11,11,11)$	(α) (β) (γ)	$(3,4,4)$, $(3,4,10)$, $(3,4,12)$, $(3,10,10)$, $(3,10,12)$, $(3,12,12)$, $(4,4,5)$, $(4,4,6)$, $(4,4,11)$, $(4,5,10)$, $(4,5,12)$, $(4,6,10)$, $(4,6,12)$, $(4,10,11)$, $(4,11,12)$, $(5,10,10)$, $(5,10,12)$, $(5,12,12)$, $(6,10,10)$, $(6,10,12)$, $(6,12,12)$, $(10,10,11)$, $(10,11,12)$, $(11,12,12)$ $(2,4,10)$, $(\mathbf{2},\mathbf{4},\mathbf{12})$, $(2,10,10)$, $(2,10,12)$, $(\mathbf{2},\mathbf{12},\mathbf{12})$ $(\mathbf{2},\mathbf{3},\mathbf{10})$, $(2,3,12)$, $(2,4,5)$, $(2,4,6)$, $(2,4,11)$, $(\mathbf{2},\mathbf{5},\mathbf{10})$, $(2,5,12)$, $(2,6,10)$, $(2,6,12)$, $(\mathbf{2},\mathbf{10},\mathbf{11})$, $(2,11,12)$
13	$2,3,$ 6, 7, 13	$2,3,$ 6, 7, 13, $4,12,14$	$(2,3,7)$, $(2,3,13)$, $(2,6,6)$, $(2,6,7)$, $(2,6,13)$, $(2,7,7)$, $(2,7,13)$, $(2,13,13)$, $(3,3,6)$, $(3,3,7)$, $(3,3,13)$, $(3,6,6)$, $(3,6,7)$, $(3,6,13)$, $(3,7,7)$, $(3,7,13)$, $(3,13,13)$, $(6,6,6)$, $(6,6,7)$, $(6,6,13)$, $(6,7,7)$, $(6,7,13)$, $(6,13,13)$, $(7,7,7)$, $(7,7,13)$, $(7,13,13)$, $(13,13,13)$	(α) (β) (γ)	$(3,4,4)$, $(3,4,12)$, $(3,4,14)$, $(3,12,12)$, $(3,12,14)$, $(3,14,14)$, $(4,4,6)$, $(4,4,7)$, $(4,4,13)$, $(4,6,12)$, $(4,6,14)$, $(4,7,12)$, $(4,7,14)$, $(4,12,13)$, $(4,13,14)$, $(6,12,12)$, $(6,12,14)$, $(6,14,14)$, $(7,12,12)$, $(7,12,14)$, $(7,14,14)$, $(12,12,13)$, $(12,13,14)$, $(13,14,14)$ $(\mathbf{2},\mathbf{4},\mathbf{12})$, $(2,4,14)$, $(\mathbf{2},\mathbf{12},\mathbf{12})$, $(2,12,14)$, $(2,14,14)$ $(2,3,12)$, $(\mathbf{2},\mathbf{3},\mathbf{14})$, $(2,4,6)$, $(2,4,7)$, $(2,4,13)$, $(2,6,12)$, $(2,6,14)$, $(2,7,12)$, $(\mathbf{2},\mathbf{7},\mathbf{14})$, $(2,12,13)$, $(\mathbf{2},\mathbf{13},\mathbf{14})$

TABLE 7. Hyperbolic triples for G and hyperbolic triples for G_1 (irregular w.r.t q^2), where $q = 11, 13$

When p is odd and e is even there are G-triples (A,B,C) which generate a projective special linear subgroup $\mathrm{PSL}_2(q_1)$ (respectively projective general linear group $\mathrm{PGL}_2(q_1)$), where $\mathbb{F}_{q_1}$ (respectively $\mathbb{F}_{q_1^2}$) is a subfield of $\mathbb{F}_q$ (see Table 3).

If $q = q_1^2$ and (A,B,C) is a G-triple that generates a subgroup isomorphic to $\mathrm{PGL}_2(q_1)$ then exactly one of (A,B,C) lies in $\mathrm{PSL}_2(q_1)$, and we say that (A,B,C) is an *irregular G-triple* (see [18, §9]). On the other hand, if (r,s,t) is a hyperbolic triple of $\mathrm{PGL}_2(q_1)$-orders then in particular it is a hyperbolic triple of G-orders, hence there exists a G-triple (A,B,C) such that A, B and C have respective orders r, s and t. Consequently, (r,s,t) is said to be *irregular w.r.t q* if (A,B,C) is an irregular G-triple. Langer and Rosenberger determined in [15, Lemma 3.5] the necessary and sufficient condition for (r,s,t) to be irregular w.r.t q.

Lemma 3.6. [15]. *Let $q = p^e$ be an odd prime power and let (r, s, t) be a hyperbolic triple of integers such that* $\gcd(rst, p) = 1$ *or one of r, s, t is equal to p and the two others are coprime to p. Then (r, s, t) is* irregular w.r.t *q if up to a permutation (r', s', t') of (r, s, t) one of the following cases holds:*

Case (α)**:**

- *$r', s', t' > 2$,*
- *r', s' and $e = \mu_{\mathrm{PSL}}(p; r', s', t')$ are all even,*
- *both $\mu_{\mathrm{PGL}}(p, r')$ and $\mu_{\mathrm{PGL}}(p, s')$ divide $\frac{e}{2}$,*
- *both $\mu_{\mathrm{PSL}}(p, r')$ and $\mu_{\mathrm{PSL}}(p, s')$ do not divide $\frac{e}{2}$,*
- *$\mu_{\mathrm{PSL}}(p, t')$ divides $\frac{e}{2}$.*

Case (β)**:**

- *$r', s' > 2$ and $t' = 2$,*
- *r', s' and $e = \mu_{\mathrm{PSL}}(p; r', s')$ are all even,*
- *both $\mu_{\mathrm{PGL}}(p, r')$ and $\mu_{\mathrm{PGL}}(p, s')$ divide $\frac{e}{2}$,*
- *both $\mu_{\mathrm{PSL}}(p, r')$ and $\mu_{\mathrm{PSL}}(p, s')$ do not divide $\frac{e}{2}$.*

Case (γ)**:**

- *$r', s' > 2$, and $t' = 2$,*
- *r' and $e = \mu_{\mathrm{PSL}}(p; r', s')$ are even,*
- *$\mu_{\mathrm{PGL}}(p, r')$ divides $\frac{e}{2}$,*
- *$\mu_{\mathrm{PSL}}(p, r')$ does not divide $\frac{e}{2}$,*
- *$\mu_{\mathrm{PSL}}(p, s')$ divides $\frac{e}{2}$.*

Case (β) is the same as case (α) except that $t' = 2$. Observe that the difference between the last two cases is that an irregular G-triple (A, B, C) in case (β) contains an involution which belongs to $\mathrm{PSL}_2(q_1)$, while in case (γ) the involution belongs to $\mathrm{PGL}_2(q_1) \setminus \mathrm{PSL}_2(q_1)$. We will therefore investigate in detail irregular triples containing involutions in §3.4.

As an example, in Tables 6 and 7 we present all the irregular triples w.r.t q^2, for $q = 3, 5, 7, 9, 11, 13$, divided according to the above cases. These triples were computed using Magma.

3.4. **Irregular triples containing involutions.** In this section we consider irregular G-triples (A, B, C) where C is an involution. We give a numerical criterion to decide whether all the elements of even order in this triple are of the same type, either split or non-split. Such triples, called *"good involuting triples w.r.t q"* (see Definition 1.5), are needed in the classification of Beauville structures for G_1 which include involutions, in Theorem 2*(iv)*.

Recall that all the involutions in $G = \mathrm{PSL}_2(q)$ are conjugate to the image of the matrix $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. They are unipotent if $p = 2$, split if $(q-1)/2$ is even, namely if $q \equiv 1 \bmod 4$, and non-split if $(q+1)/2$ is even, namely if $q \equiv 3 \bmod 4$. Moreover, if q is odd, then there is exactly one G_1-conjugacy class of involutions in $G_1 \setminus G$. They are split if $(q-1)/2$ is odd, namely if $q \equiv 3 \bmod 4$, and non-split if $(q+1)/2$ is odd, namely if $q \equiv 1 \bmod 4$ (see Tables 1 and 2).

Proposition 3.7. *Assume that q is an odd prime power and let (A, B, C) be an irregular* $\mathrm{PSL}_2(q^2)$*-triple of respective orders $(r, s, 2)$. Then one of the following holds:*

- *$q \equiv 1 \bmod 4$, C is split and $(r, s, 2)$ is in case (β).*

- *$q \equiv 1 \bmod 4$, C is non-split and $(r,s,2)$ is in case (γ).*
- *$q \equiv 3 \bmod 4$, C is non-split and $(r,s,2)$ is in case (β).*
- *$q \equiv 3 \bmod 4$, C is split and $(r,s,2)$ is in case (γ).*

Proof. Recall that by Lemma 3.6, an irregular $\mathrm{PSL}_2(q^2)$-triple (A,B,C) of respective orders $(r,s,2)$ is in case (β) if and only if $C \in \mathrm{PSL}_2(q)$, whereas it is in case (γ) if and only if $C \in \mathrm{PGL}_2(q) \setminus \mathrm{PSL}_2(q)$ (up to conjugation). The claim now follows from the above observation. □

Corollary 3.8. *Assume that q is an odd prime power and let (A,B,C) be an irregular $\mathrm{PSL}_2(q^2)$-triple of respective orders $(r,s,2)$ with $r>2$ even.*

If $q \equiv 1 \bmod 4$, then

- *Both A and C are split if and only if r divides $q-1$ and $(r,s,2)$ is in case (β).*
- *Both A and C are non-split if and only if r divides $q+1$ and $(r,s,2)$ is in case (γ).*

If $q \equiv 3 \bmod 4$, then

- *Both A and C are split if and only if r divides $q-1$ and $(r,s,2)$ is in case (γ).*
- *Both A and C are non-split if and only if r divides $q+1$ and $(r,s,2)$ is in case (β).*

The proof of part *(iv)* of Theorem 2 relies on the following corollary which is a consequence of Corollary 3.8. Recall that the notion of a *"good involuting triple w.r.t q"* was given in Definition 1.5.

Corollary 3.9. *Let q be an odd prime power and let (A,B,C) be an irregular $\mathrm{PSL}_2(q^2)$-triple of respective orders $(r,s,2)$. Then all the elements of even order in this triple are of the same type (either split or non-split) if and only if $(r,s,2)$ is a* good involuting triple w.r.t *q (see Definition 1.5).*

Proof. Again, let $G=\mathrm{PSL}_2(q)$ and $G_1=\mathrm{PGL}_2(q)$. Without loss of generality we may assume that $A \in G_1 \setminus G$ and thus $r>2$ is even. By Corollary 3.8 one of the following necessarily holds:

- $q \equiv 1 \bmod 4$, r divides $q-1$ and $(r,s,2)$ is in case (β). In case (β), both $A,B \in G_1 \setminus G$, and so s is also even. Since A,B are split, then r,s both divide $q-1$ but not $(q-1)/2$.
- $q \equiv 1 \bmod 4$, r divides $q+1$ and $(r,s,2)$ is in case (γ). Since $A \in G_1 \setminus G$ then r does not divide $(q+1)/2$. In case (γ), $B \in G$, and so s is a G-order. If s is even then s divides $(q-1)/2$, and so B is split. But A is non-split, yielding a contradiction. Hence, s is necessarily odd.
- $q \equiv 3 \bmod 4$, r divides $q-1$ and $(r,s,2)$ is in case (γ). Since $A \in G_1 \setminus G$ then r does not divide $(q-1)/2$. In case (γ), $B \in G$, and so s is a G-order. If s is even then s divides $(q+1)/2$, and so B is non-split. But A is split, yielding a contradiction. Hence, s is necessarily odd.
- $q \equiv 3 \bmod 4$, r divides $q+1$ and $(r,s,2)$ is in case (β). In case (β), both $A,B \in G_1 \setminus G$, and so s is also even. Since A,B are non-split, then r,s both divide $q+1$ but not $(q+1)/2$.

□

As an example, in Tables 6 and 7 we mark in **bold** all the *good involuting triples w.r.t q* where $q=5,7,9,11,13$. These triples were computed using MAGMA.

q		case	elements of even order	good involuting triple w.r.t q
$q \equiv 1 \bmod 4$	$q > 5$	(β)	split	$(2, q-1, q-1)$
$q \equiv 1 \bmod 4$	$q \geq 5$	(γ)	non-split	$(2, p, q+1)$
	$q > 5$			$(2, (q+1)/2, (q+1))$
$q \equiv 3 \bmod 4$	$q \geq 7$	(γ)	split	$(2, p, q-1)$
	$q > 7$			$(2, (q-1)/2, q-1)$
$q \equiv 3 \bmod 4$	$q \geq 7$	(β)	non-split	$(2, q+1, q+1)$

TABLE 8. Good involuting triples w.r.t q

Example 3.10. Table 8 presents some general examples for *good involuting triples w.r.t q*.

Note that in case (β) we exclude $q = 5$ since the triple $(2, 4, 4)$ is not hyperbolic, and in case (γ) the second triple is excluded when $q = 5$ or 7 since the triple $(2, 3, 6)$ is not hyperbolic.

3.5. **Generating triples containing unipotents.** In this section we consider G-triples (A, B, C) where A and B are unipotent elements and C is not unipotent. We give a numerical criterion on the order of C to decide whether A is G-conjugate to B, which is called a *"good G-order"* (see Definition 1.2). Such triples are needed in the classification of Beauville structures for G which include unipotents, in Theorem 1*(ii)*.

Assume that q is odd and consider the following matrices in $G_0 = \mathrm{SL}_2(q)$:

$$U_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad U_{-1} = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix},$$

$$U_1' = XU_1X^{-1} = \begin{pmatrix} 1 & x^2 \\ 0 & 1 \end{pmatrix} \in G_0, \quad U_{-1}' = XU_{-1}X^{-1} = \begin{pmatrix} -1 & x^2 \\ 0 & -1 \end{pmatrix} \in G_0,$$

where $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ satisfies that $x^2 \in \mathbb{F}_q$ and $X = \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \in \mathrm{SL}_2(q^2)$.

The following proposition and its corollary are immediate observations.

Proposition 3.11. *Assume that q is odd. Then, for any $A \in G_0$, $XAX^{-1} \in G_0$. Moreover,*

- *If $A \neq I$ and $\mathrm{tr}(A) = 2$ then A is G_0-conjugate to either U_1 or U_1'.*
- *If $A \neq -I$ and $\mathrm{tr}(A) = -2$ then A is G_0-conjugate to either U_{-1} or U_{-1}'.*

Proof. Indeed, if $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_0$ then $XAX^{-1} = \begin{pmatrix} a & bx^2 \\ cx^{-2} & d \end{pmatrix} \in G_0$. Moreover, U_1 is not G_0-conjugate to $U_1' = XU_1X^{-1}$, since x^2 is not a square of some element in $\mathbb{F}_q$. Hence, any $I \neq A \in G_0$ with $\mathrm{tr}(A) = 2$ is G_0-conjugate to either U_1 or U_1' (see Table 2). □

Corollary 3.12. *Assume that q is odd. Then, for any $\bar{A} \in G$, $\bar{X}\bar{A}\bar{X}^{-1} \in G$. If, moreover, $\bar{A}$ is unipotent then it is G-conjugate to either $\bar{U}_1$ or $\bar{U}'_1 = \bar{X}\bar{U}_1\bar{X}^{-1}$. In addition,*

- *If $q \equiv 1 \bmod 4$ then $\bar{U}_1$ and $\bar{U}_{-1}$ are G-conjugate.*
- *If $q \equiv 3 \bmod 4$ then $\bar{U}_1$ and $\bar{U}'_{-1}$ are G-conjugate.*

The following lemma is needed later in Section 4.2, to decide whether a unipotent element $\bar{A} \in G$ is G-conjugate to some power of $\bar{U}_1$ or not.

Lemma 3.13. *Assume that p is odd and let $q = p^e$. Let $\bar{A} \in G$ be a unipotent element.*

- *If e is odd, then there exists some $0 < i < p$ such that $\bar{A}^i$ is G-conjugate to $\bar{U}_1$.*
- *If e is even, then for every $0 < i < p$, $\bar{A}^i$ is G-conjugate to $\bar{A}$.*

Proof. Consider the set $I = \{i : 0 < i < p\}$. Observe that if p is odd and e is even then all the elements in I are squares in $\mathbb{F}_q$. If p is odd and e is odd, then half of the elements in I are squares in $\mathbb{F}_q$ and half are non-squares.

Hence, if e is odd then there exists some $i \in I$ such that U_1^i is G_0-conjugate to U_1' and so $\bar{U}_1^i$ is G-conjugate to $\bar{U}'_1$. If e is even then for every $i \in I$, U_1^i is G_0-conjugate to U_1 and so $\bar{U}_1^i$ is G-conjugate to $\bar{U}_1$. □

We now consider G-triples (A, B, C) such that A and B are unipotent elements and C is not unipotent.

Proposition 3.14. *Assume that q is odd. Let (A, B, C) be a G_0-triple such that $A, B \neq \pm I$ and $\mathrm{tr}(A), \mathrm{tr}(B) \in \{\pm 2\}$. Denote $\gamma = \mathrm{tr}(C)$.*

1. *If $\mathrm{tr}(A) = \mathrm{tr}(B)$, then A is G_0-conjugate to B if and only if $2-\gamma$ is a square in $\mathbb{F}_q$.*
2. *If $\mathrm{tr}(A) = -\mathrm{tr}(B)$, then A is G_0-conjugate to $-B$ if and only if $2+\gamma$ is a square in $\mathbb{F}_q$.*

Proof. Without loss of generality we may assume that $A = U_1$.

(1) If $B = MU_1M^{-1}$ for some matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_0$, then

$$\gamma = \mathrm{tr}(C) = \mathrm{tr}(AB) = \mathrm{tr}(U_1MU_1M^{-1}) = \mathrm{tr}\begin{pmatrix} 1-ac-c^2 & 1+ac+a^2 \\ -c^2 & 1+ac \end{pmatrix} = 2 - c^2,$$

and so $2-\gamma$ is a square in $\mathbb{F}_q$.
If $B = MU_1'M^{-1}$ for some matrix $M \in G_0$, then

$$\gamma = \mathrm{tr}(C) = \mathrm{tr}(AB) = \mathrm{tr}(U_1MU_1'M^{-1}) = 2 - x^2c^2,$$

and since $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ then $2-\gamma$ is a non-square in $\mathbb{F}_q$.

(2) Similarly, if $B = M(-U_1)M^{-1}$ for some matrix $M \in G_0$, then

$$\gamma = \mathrm{tr}(C) = \mathrm{tr}(AB) = \mathrm{tr}(U_1M(-U_1)M^{-1}) = -2 + c^2,$$

and so $2+\gamma$ is a square in $\mathbb{F}_q$.
If $B = M(-U_1')M^{-1}$ for some matrix $M \in G_0$, then

$$\gamma = \mathrm{tr}(C) = \mathrm{tr}(AB) = \mathrm{tr}(U_1M(-U_1')M^{-1}) = -2 + x^2c^2,$$

and so $2+\gamma$ is a non-square in $\mathbb{F}_q$.

□

Therefore, in order to decide whether in a G-triple (A, B, C) of respective orders (p, p, t), $t \neq p$, A is G-conjugate to B, one needs to determine whether for $\gamma \in \mathcal{T}_q(t)$, $2-\gamma$ or $2+\gamma$ is a square in $\mathbb{F}_q$. In the following we prove that this is equivalent to decide whether t is a *good G-order* or not. Recall that $G = \mathrm{PSL}_2(q)$, $G_0 = \mathrm{SL}_2(q)$ and the notion of a *"good G-order"* was given in Definition 1.2.

Proposition 3.15. *Assume that q is odd. Let $C \in G_0$, $\gamma = \mathrm{tr}(C)$ and $t = |\bar{C}|$. Assume that $\gamma \neq \pm 2$ (or equivalently, $t \neq p$). Then one of $2+\gamma$, $2-\gamma$ is a square in $\mathbb{F}_q$ if and only if t is a* good G-order *(see Definition 1.2).*

Proof. As $t \neq p$ is a G-order then t divides either $(q-1)/2$ or $(q+1)/2$.

If t divides $(q-1)/2$ then $\gamma = a + a^{-1}$ or $\gamma = -(a + a^{-1})$, for some primitive root of unity a of order $2t$ in $\mathbb{F}_q$ (see Proposition 3.1). Hence,

$$\{2+\gamma, 2-\gamma\} = \{a + 2 + a^{-1}, (-a) + 2 + (-a)^{-1}\}.$$

Therefore, $2+\gamma$ or $2-\gamma$ is a square in $\mathbb{F}_q$ if and only if $a = c^2$ or $-a = c^2$ for some $c \in \mathbb{F}_q$. Indeed, $a + 2 + a^{-1}$ is a square if and only if $(a+1)^2/a$ is a square if and only if a is a square in $\mathbb{F}_q$, and similarly for $(-a) + 2 + (-a)^{-1}$.

Now, one the following necessarily holds:

- If t is even then $-a$ is also a primitive root of unity of order $2t$. Hence, a is a square in $\mathbb{F}_q$ if and only if $-a$ is a square is $\mathbb{F}_q$. In addition, a is a square in $\mathbb{F}_q$ if and only if $\mathbb{F}_q$ contains a primitive root of unity of order $4t$, namely, if and only if $4t$ divides $q-1$.
- If t is odd and $q \equiv 1 \bmod 4$ then $4t$ divides $q-1$, and so $\mathbb{F}_q$ contains a primitive root of unity of order $4t$. Thus a, which is a primitive root of unity of order $2t$, is a square in $\mathbb{F}_q$, as required.
- If t is odd and $q \equiv 3 \bmod 4$ then $\mathbb{F}_q$ contains a primitive root of unity of order $2t$ but does not contain a primitive root of unity of order $4t$, and so, a is a non-square in $\mathbb{F}_q$. However, $-a$ is a primitive root of unity of order t, and so, it is necessarily a square in $\mathbb{F}_q$, as required.

In conclusion, $a = c^2$ or $-a = c^2$ for some $c \in \mathbb{F}_q$ if and only if either t is odd and divides $q-1$ or t is even and $4t$ divides $q-1$.

If t divides $(q+1)/2$ then $\gamma = a + a^q$ or $\gamma = -(a + a^q)$, for some primitive root of unity a of order $2t$ in $\mathbb{F}_{q^2}$ (see Proposition 3.1). Hence,

$$\{2+\gamma, 2-\gamma\} = \{a + 2 + a^q, (-a) + 2 + (-a)^q\}.$$

Therefore, $2+\gamma$ or $2-\gamma$ is a square in $\mathbb{F}_q$ if and only if $a = c^2$ or $-a = c^2$ for some $c \in \mathbb{F}_{q^2}$ satisfying $c^{q+1} = 1$.

Now, one the following necessarily holds:

- If t is even then $-a$ is also a primitive root of unity of order $2t$. Hence, $a = c^2$ for some $c \in \mathbb{F}_{q^2}$ satisfying $c^{q+1} = 1$ if and only if $-a = b^2$ for some $b \in \mathbb{F}_{q^2}$ satisfying $b^{q+1} = 1$. This is equivalent to the condition that $4t$ divides $q+1$.
- If t is odd and $q \equiv 3 \bmod 4$ then $\mathbb{F}_{q^2}$ contains a primitive root of unity b of order $4t$ satisfying $b^{q+1} = 1$. Hence, $a = c^2$ for some $c \in \mathbb{F}_{q^2}$ satisfying $c^{q+1} = 1$, as required.
- If t is odd and $q \equiv 1 \bmod 4$ then $\mathbb{F}_{q^2}$ does not contain a primitive root of unity c of order $4t$ satisfying $c^{q+1} = 1$. However, in this case, $-a = b^2$ for some $b \in \mathbb{F}_{q^2}$ satisfying $b^{q+1} = 1$, as required.

In conclusion, $a = c^2$ or $-a = c^2$ for some $c \in \mathbb{F}_{q^2}$ satisfying $c^{q+1} = 1$ if and only if either t is odd and divides $q+1$ or t is even and $4t$ divides $q+1$. □

Corollary 3.16. *Assume that $q = p^e$ for some odd prime p and some positive integer e. Let (A, B, C) be a G-triple of respective orders (p, p, t), $t \neq p$. Then A is G-conjugate to B if and only if t is a* good G-order.

Proof. Let (A,B,C) be a G_0-triple and assume that its image in G, $(\bar{A},\bar{B},\bar{C})$ has respective orders (p,p,t), $t \neq p$. Denote $\gamma = \mathrm{tr}(C)$. Then $\bar{A}$ and $\bar{B}$ are unipotent if and only if $A, B \neq \pm I$ and $\mathrm{tr}(A), \mathrm{tr}(B) \in \{\pm 2\}$. Moreover, $\bar{A}$ and $\bar{B}$ are G-conjugate if and only if either $\mathrm{tr}(A) = \mathrm{tr}(B)$ and A and B are G_0-conjugate or $\mathrm{tr}(A) = -\mathrm{tr}(B)$ and A and $-B$ are G_0-conjugate. From Proposition 3.14 we deduce that $\bar{A}$ and $\bar{B}$ are G-conjugate if and only if $2-\gamma$ or $2+\gamma$ is a square in $\mathbb{F}_q$. By Proposition 3.15, the latter is equivalent to t being a good G-order. □

Lemma 3.17. *Assume that $q = p^e$ where p is odd and $5 \leq q \neq 9$. There exists a G-triple (A,B,C) of respective orders (p,p,t), $t \neq p$, such that $\langle A,B\rangle = G$ and A is G-conjugate to B if and only if $e = \mu_{\mathrm{PSL}}(p;t)$ and t is a* good G-order.

Proof. Let (A,B,C) be a G-triple of respective orders (p,p,t), $t \neq p$. If $\langle A,B\rangle = G$ then Theorem 3.2 implies that $e = \mu_{\mathrm{PSL}}(p;t)$, and if moreover A is G-conjugate to B then Corollary 3.16 implies that t is a good G-order.

If $e = \mu_{\mathrm{PSL}}(p;t)$ then there exists a G-triple (A,B,C) of respective orders (p,p,t) (see Section 3.3). If moreover t is a good G-order then A is G-conjugate to B, by Corollary 3.16.

We now use the methodology described in Section 3.3. Let $\gamma \in \mathcal{T}_{p^e}(t)$. Observe that Equation (4) is equivalent in this case to $(\gamma \pm 2)^2 = 0$. Since $t \neq p$ then $\gamma \neq \pm 2$, and so this equality does not hold, implying that $\langle A,B\rangle$ is not a structural subgroup, by [18, Theorem 2]. As $e = \mu_{\mathrm{PSL}}(p;t)$, it follows from Table 6 that if $5 < q \neq 9$ then either $p > 5$; or $p = 5$ and $e > 1$ implying that $t \neq 2,3,5$; or $p = 3$ and $e > 2$ implying that $t > 5$. Therefore, $\langle A,B\rangle$ cannot be a small subgroup. If $q = 5$ then $\langle A,B\rangle \cong A_5 = G$ as required. In addition, (A,B,C) is clearly not an irregular G-triple. The condition that $e = \mu_{\mathrm{PSL}}(p;t)$ now ensures that $\langle A,B\rangle = G$. □

Remark 3.18. In the case $G = \mathrm{PSL}_2(9)$ one needs to consider the G-orders 4 and 5.

- 4 is not a good G-order, and so, if (A,B,C) is a G-triple of respective orders $(3,3,4)$ then A, B are not G-conjugate.
- 5 is a good G-order. However, if (A,B,C) is a G-triple of respective orders $(3,3,5)$ and A is G-conjugate to B, then one can verify that $\langle A,B\rangle \cong A_5$ is a small subgroup of G (see also [13, §2, Theorem 8.4]).

Example 3.19. Table 9 presents for $p = 5,7,11,13$ *all* the G-orders $t \neq p$ such that $e = \mu_{\mathrm{PSL}}(p;t) \in \{1,2\}$, divided according to whether they are *good G-orders* or not. They were computed using MAGMA.

	good G-orders	not good G-orders		good G-orders	not good G-orders
$q=5$	3	2	$q=25$	$6,13$	$4,12$
$q=7$	$2,3$	4	$q=49$	$5,6,12,25$	$8,24$
$q=11$	$3,5$	$2,6$	$q=121$	$10,15,30,61$	$4,12,20,60$
$q=13$	$3,7$	$2,6$	$q=169$	$5,14,17,21,42,85$	$4,12,28,84$

TABLE 9. Good G-orders for $q = 5,7,11,13,25,49,121,169$

4. BEAUVILLE STRUCTURES FOR $\mathrm{PSL}_2(q)$ AND $\mathrm{PGL}_2(q)$

In this section we prove Theorems 1 and 2.

4.1. **Cyclic groups.** The following elementary lemma is needed for the proof of Theorems 1 and 2.

Lemma 4.1. *Let $\mathcal{C}$ be a finite cyclic group, and let x and y be non-trivial elements in $\mathcal{C}$. If the orders of x and y are not relatively prime, then there exist some integers k and l such that $x^k = y^l \neq 1$.*

Proof. Let a and b denote the orders of x and y respectively and set $c = \gcd(a, b)$. Note that by assumption $c \neq 1$. Also write $a = a'c$ and $b = b'c$ where $\gcd(a', b') = 1$, so that $x^{a'}$ and $y^{b'}$ have order c.

Observe that $\mathcal{C}$ has a unique (cyclic) subgroup of order c, and let z be a generator of this subgroup. Thus,

$$\langle x^{a'} \rangle = \langle z \rangle = \langle y^{b'} \rangle.$$

Therefore, there exist some integers k and l such that

$$x^{a'k} = z = y^{b'l} \neq 1,$$

where the latter inequality follows from the fact that z is of order $c > 1$. □

4.2. **Elements and conjugacy classes in $\mathrm{PSL}_2(q)$ and $\mathrm{PGL}_2(q)$.** Let $H = \mathrm{PSL}_2(q)$ or $\mathrm{PGL}_2(q)$ where $q = p^e$ for some prime p and some positive integer e. In this section, we determine the elements A_1, A_2 of H such that $\Sigma(A_1) \cap \Sigma(A_2) = \{1\}$, where for elements $A_1, \dots, A_m$ of H,

$$\Sigma(A_1, \dots, A_m) = \bigcup_{A \in H} \bigcup_{j=1}^{\infty} \{AA_1^j A^{-1}, \dots, AA_m^j A^{-1}\}.$$

Given two triples (A_1, A_2, A_3) and (B_1, B_2, B_3) of H, this will enable us to determine whether $\Sigma(A_1, A_2, A_3) \cap \Sigma(B_1, B_2, B_3) = \{1\}$ which is a necessary condition for H to admit an unmixed Beauville structure (see Definition 1.1*(iii)*). Indeed the condition $\Sigma(A_1, A_2, A_3) \cap \Sigma(B_1, B_2, B_3) = \{1\}$ is equivalent to the condition

$$\Sigma(A_i) \cap \Sigma(B_j) = \{1\} \quad \forall 1 \leq i, j \leq 3.$$

Lemma 4.2. *Let $G = \mathrm{PSL}_2(q)$ where $q = p^e$ for some prime number p and some positive integer e. Let $A_1, A_2 \in G$. Then $\Sigma(A_1) \cap \Sigma(A_2) = \{1\}$ if and only if one of the following occurs:*

(a) *The orders $|A_1|$ and $|A_2|$ are relatively prime.*
(b) *The prime p is odd, e is even, $|A_1| = |A_2| = p$ and A_1, A_2 are not G-conjugate.*

Proof. If the orders of A_1 and A_2 are relatively prime then every two non-trivial powers A_1^i and A_2^j have distinct orders, and thus $\Sigma(A_1) \cap \Sigma(A_2) = \{1\}$ as required.

Now, assume that the orders of A_1 and A_2 are not relatively prime.

Observe that $(q-1)/d$ and $(q+1)/d$ are coprime, where $d = \gcd(q-1, 2)$. Thus, if there exists some prime $r \neq p$ which divides both $|A_1|$ and $|A_2|$, then r divides exactly one of $(q-1)/d$ or $(q+1)/d$. Hence, $|A_1|$ and $|A_2|$ both divide exactly one of $(q-1)/d$ or $(q+1)/d$, and so A_1 and A_2 are G-conjugate to two elements C_1 and C_2 which belong to the same cyclic group, either of order $(q-1)/d$ or of order $(q+1)/d$ (see Section 2.3). Lemma 4.1 now implies that there exist some integers i and j such that $A_1^i \neq 1$ and $A_2^j \neq 1$ are G-conjugate, and so $\Sigma(A_1) \cap \Sigma(A_2) \neq \{1\}$.

It now remains to treat the case where $|A_1| = |A_2| = p$, that is when A_1 and A_2 are unipotent elements. If $p = 2$ then necessarily A_1 and A_2 are G-conjugate and so $\Sigma(A_1) \cap \Sigma(A_2) \neq \{1\}$. However, when p is odd then A_1 and A_2 are not necessarily G-conjugate (see Table 2 and Section 3.5).

If p is odd and e is odd then by Lemma 3.13, there exist some integers i and j such that $A_1^i \neq 1$ and $A_2^j \neq 1$ are G-conjugate, and so $\Sigma(A_1) \cap \Sigma(A_2) \neq \{1\}$. If p is odd and e is even then by Lemma 3.13, for any two integers $1 \leq i, j < p$, A_1^i and A_2^j are G-conjugate to A_1 and A_2 respectively. Thus, $\Sigma(A_1) \cap \Sigma(A_2) = \{1\}$ if and only if A_1 and A_2 are not G-conjugate. □

Proposition 4.3. *Let $G = \mathrm{PSL}_2(q)$ where $q = p^e$ for some odd prime p and even integer e. Take some $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ such that $x^2 \in \mathbb{F}_q$, and let $X \in \mathrm{PSL}_2(q^2)$ denote the image of the matrix $\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \in \mathrm{SL}_2(q^2)$.*

Let $A_1, A_2, B_1, B_2 \in G$ such that $|A_1| = |A_2| = |B_1| = |B_2| = p$. Then, XA_2X^{-1}, $XB_2X^{-1} \in G$, and A_1 is G-conjugate to either A_2 or XA_2X^{-1}. Moreover,

- *(i) Either $\Sigma(A_1) \cap \Sigma(A_2) = \{1\}$ or $\Sigma(A_1) \cap \Sigma(XA_2X^{-1}) = \{1\}$.*
- *(ii) $\Sigma(A_1, B_1) \cap \Sigma(A_2) = \{1\}$ or $\Sigma(A_1, B_1) \cap \Sigma(XA_2X^{-1}) = \{1\}$ if and only if A_1 is G-conjugate to B_1.*
- *(iii) $\Sigma(A_1, B_1) \cap \Sigma(A_2, B_2) = \{1\}$ or $\Sigma(A_1, B_1) \cap \Sigma(XA_2X^{-1}, XB_2X^{-1}) = \{1\}$ if and only if A_1 is G-conjugate to B_1 and A_2 is G-conjugate to B_2.*

Proof. By Corollary 3.12, $XA_2X^{-1}, XB_2X^{-1} \in G$, A_1 is G-conjugate to either A_2 or XA_2X^{-1}, and B_1 is G-conjugate to either B_2 or XB_2X^{-1}.

(i) If A_1 and A_2 are not G-conjugate then by Lemma 4.2, $\Sigma(A_1) \cap \Sigma(A_2) = \{1\}$. On the other hand, if A_1 and A_2 are G-conjugate, then A_1 and XA_2X^{-1} are not G-conjugate, and again by Lemma 4.2, $\Sigma(A_1) \cap \Sigma(XA_2X^{-1}) = \{1\}$.

(ii) Assume that A_1 and B_1 are G-conjugate. If A_2 is not G-conjugate to A_1 (and to B_1) then by Lemma 4.2, $\Sigma(A_1) \cap \Sigma(A_2) = \{1\}$ (and $\Sigma(B_1) \cap \Sigma(A_2) = \{1\}$), implying $\Sigma(A_1, B_1) \cap \Sigma(A_2) = \{1\}$. Otherwise, XA_2X^{-1} is not G-conjugate to A_1 (and to B_1) and so, similarly, $\Sigma(A_1, B_1) \cap \Sigma(XA_2X^{-1}) = \{1\}$.

Now assume that A_1 and B_1 are not G-conjugate. In this case, A_2 is G-conjugate to either A_1 or B_1. If A_2 is G-conjugate to A_1 then XA_2X^{-1} is G-conjugate to B_1, and so by Lemma 4.2, $\Sigma(A_1) \cap \Sigma(A_2) \neq \{1\}$ and $\Sigma(B_1) \cap \Sigma(XA_2X^{-1}) \neq \{1\}$. Otherwise, A_2 is G-conjugate to B_1 and so XA_2X^{-1} is G-conjugate to A_1, thus, similarly, $\Sigma(B_1) \cap \Sigma(A_2) \neq \{1\}$ and $\Sigma(A_1) \cap \Sigma(XA_2X^{-1}) \neq \{1\}$.

(iii) Assume that A_1 is G-conjugate to B_1 and A_2 is G-conjugate to B_2. If A_2 (and B_2) are not G-conjugate to A_1 (and B_1) then by Lemma 4.2, $\Sigma(A_1, B_1) \cap \Sigma(A_2, B_2) = \{1\}$. Otherwise, A_2 (and B_2) are G-conjugate to A_1 (and B_1), and so, XA_2X^{-1} (and XB_2X^{-1}) are not G-conjugate to A_1 (and B_1), hence, similarly, $\Sigma(A_1, B_1) \cap \Sigma(XA_2X^{-1}, XB_2X^{-1}) = \{1\}$.

If A_1 is not G-conjugate to B_1, then by *(ii)*, $\Sigma(A_1, B_1) \cap \Sigma(A_2) \neq \{1\}$ and $\Sigma(A_1, B_1) \cap \Sigma(XA_2X^{-1}) \neq \{1\}$. Similarly, if A_2 is not G-conjugate to B_2, then by *(ii)*, $\Sigma(A_1) \cap \Sigma(A_2, B_2) \neq \{1\}$ and $\Sigma(A_1) \cap \Sigma(XA_2X^{-1}, XB_2X^{-1}) \neq \{1\}$. □

Lemma 4.4. *Let $G_1 = \mathrm{PGL}_2(q)$ where $q = p^e$ for some odd prime number p and some positive integer e. Let $A_1, A_2 \in G_1$. Then $\Sigma(A_1) \cap \Sigma(A_2) = \{1\}$ if and only if one of the following occurs:*

(a) *The orders $|A_1|$ and $|A_2|$ are relatively prime.*
(b) *A_1 is split, A_2 is non-split and* $\gcd(|A_1|, |A_2|) = 2$.
(c) *A_1 is non-split, A_2 is split and* $\gcd(|A_1|, |A_2|) = 2$.

Proof. If $\gcd(|A_1|, |A_2|) = 1$ then any two non-trivial powers A_1^i and A_2^j have distinct orders, thus $\Sigma(A_1) \cap \Sigma(A_2) = \{1\}$, as required.

If A_1 is split and A_2 is non-split, then necessarily $\gcd(|A_1|, |A_2|) \leq 2$, since $\gcd(q-1, q+1) = 2$. In this case, any non-trivial power of A_1 is a split element, while any non-trivial power of A_2 is a non-split element, and so they are not G_1-conjugate, implying that $\Sigma(A_1) \cap \Sigma(A_2) = \{1\}$, as required.

If $\gcd(|A_1|, |A_2|) = 2$ and both A_1 and A_2 are split (respectively non-split) elements, then A_1 and A_2 are G_1-conjugate to two elements C_1 and C_2 which belong to the same cyclic group of order $q-1$ (respectively $q+1$). Lemma 4.1 now implies that there exist some integers i and j such that $A_1^i \neq 1$ and $A_2^j \neq 1$ are G_1-conjugate, and so $\Sigma(A_1) \cap \Sigma(A_2) \neq \{1\}$.

If $|A_1| = |A_2| = p$, then A_1 and A_2 are unipotent, and so they are G_1-conjugate, implying that $\Sigma(A_1) \cap \Sigma(A_2) \neq \{1\}$.

Otherwise, $\gcd(|A_1|, |A_2|) = r$, where $2 < r \neq p$, and so r divides exactly one of $q-1$ or $q+1$, implying that $|A_1|$ and $|A_2|$ both divide exactly one of $q-1$ or $q+1$. Hence, A_1 and A_2 are G_1-conjugate to two elements C_1 and C_2 which belong to the same cyclic group, either of order $q-1$ or of order $q+1$. Lemma 4.1 implies again that there exist some integers i and j such that $A_1^i \neq 1$ and $A_2^j \neq 1$ are G_1-conjugate, and so $\Sigma(A_1) \cap \Sigma(A_2) \neq \{1\}$. □

4.3. Proof of Theorem 1.

The conditions are sufficient. Let $\tau_1 = (r_1, s_1, t_1)$ and $\tau_2 = (r_2, s_2, t_2)$ be two hyperbolic triples of integers. Assume that $G = \mathrm{PSL}_2(q)$ is a quotient of the triangle groups T_{r_1,s_1,t_1} and T_{r_2,s_2,t_2} with torsion-free kernel. Then one can find elements $A_1, B_1, C_1, A_2, B_2, C_2$ in G of orders $r_1, s_1, t_1, r_2, s_2, t_2$ respectively, such that $A_1B_1C_1 = 1 = A_2B_2C_2$ and $\langle A_1, B_1\rangle = G = \langle A_2, B_2\rangle$, and so conditions *(i)* and *(ii)* of Definition 1.1 are fulfilled.

Moreover, the condition that $r_1s_1t_1$ is coprime to $r_2s_2t_2$ implies that each of r_1, s_1, t_1 is coprime to each of r_2, s_2, t_2, and so by Lemma 4.2, $\Sigma(A_1, B_1, C_1) \cap \Sigma(A_2, B_2, C_2) = \{1\}$, hence condition *(iii)* of Definition 1.1 is fulfilled, thus $\big((A_1, B_1, C_1), (A_2, B_2, C_2)\big)$ is an unmixed Beauville structure of type (τ_1, τ_2).

It is left to consider the case where p is odd, e is even, $q = p^e > 9$ and $\gcd(r_1s_1t_1, r_2s_2t_2) \in \{p, p^2\}$, which can be reduced to the following three cases.

(1) $r_1 = r_2 = p$ and $s_1, s_2, t_1, t_2 \neq p$.
Let X be as in Proposition 4.3, and denote $A_2' = XA_2X^{-1}$, $B_2' = XB_2X^{-1}$ and $C_2' = XC_2X^{-1}$. Then also $A_2'B_2'C_2' = 1$ and $\langle A_2', B_2'\rangle = G$. By Proposition 4.3,

$$\text{either } \Sigma(A_1) \cap \Sigma(A_2) = \{1\} \text{ or } \Sigma(A_1) \cap \Sigma(A_2') = \{1\}.$$

Moreover, since p is coprime to s_2t_2 then by Lemma 4.2,

$$\Sigma(A_1) \cap \Sigma(B_2, C_2) = \{1\},\ \Sigma(A_1) \cap \Sigma(B_2', C_2') = \{1\}.$$

Similarly, since s_1t_1 is coprime to ps_2t_2, then by Lemma 4.2,

$$\Sigma(B_1,C_1)\cap\Sigma(A_2,B_2,C_2)=\{1\},\ \Sigma(B_1,C_1)\cap\Sigma(A'_2,B'_2,C'_2)=\{1\}.$$

Therefore, either $\Sigma(A_1,B_1,C_1)\cap\Sigma(A_2,B_2,C_2)=\{1\}$ or $\Sigma(A_1,B_1,C_1)\cap\Sigma(A'_2,B'_2,C'_2)=\{1\}$.

(2) $r_1=r_2=s_1=p$ and $s_2,t_1,t_2\neq p$.
Let (A'_2,B'_2,C'_2) be as in Case (1). By the assumption of the theorem, in this case, t_1 is a *good G-order*. Hence by Lemma 3.17, there exist $A_1,B_1,C_1\in G$ of respective orders p,p,t_1 such that A_1 is G-conjugate to B_1, $A_1B_1C_1=1$ and $\langle A_1,B_1\rangle=G$. By Proposition 4.3,

$$\text{either } \Sigma(A_1,B_1)\cap\Sigma(A_2)=\{1\} \text{ or } \Sigma(A_1,B_1)\cap\Sigma(A'_2)=\{1\}.$$

Moreover, since p is coprime to s_2t_2, then by Lemma 4.2,

$$\Sigma(A_1,B_1)\cap\Sigma(B_2,C_2)=\{1\},\ \Sigma(A_1,B_1)\cap\Sigma(B'_2,C'_2)=\{1\}.$$

Similarly, since t_1 is coprime to ps_2t_2, then by Lemma 4.2,

$$\Sigma(C_1)\cap\Sigma(A_2,B_2,C_2)=\{1\},\ \Sigma(C_1)\cap\Sigma(A'_2,B'_2,C'_2)=\{1\},$$

Therefore, either $\Sigma(A_1,B_1,C_1)\cap\Sigma(A_2,B_2,C_2)=\{1\}$ or $\Sigma(A_1,B_1,C_1)\cap\Sigma(A'_2,B'_2,C'_2)=\{1\}$.

(3) $r_1=r_2=s_1=s_2=p$ and $t_1,t_2\neq p$.
Let (A_1,B_1,C_1) be as in Case (2). By the assumption of the theorem, in this case, t_1 and t_2 are *good G-orders*. Hence by Lemma 3.17, there exist $A_2,B_2,C_2\in G$ of respective orders p,p,t_2 such that A_2 is G-conjugate to B_2, $A_2B_2C_2=1$ and $\langle A_2,B_2\rangle=G$. Again, we denote $A'_2=XA_2X^{-1}$, $B'_2=XB_2X^{-1}$ and $C'_2=XC_2X^{-1}$. Then also $A'_2B'_2C'_2=1$ and $\langle A'_2,B'_2\rangle=G$. By Proposition 4.3,

$$\text{either } \Sigma(A_1,B_1)\cap\Sigma(A_2,B_2)=\{1\} \text{ or } \Sigma(A_1,B_1)\cap\Sigma(A'_2,B'_2)=\{1\}.$$

Moreover, since p, t_1 and t_2 are pairwise coprime, then by Lemma 4.2,

$$\Sigma(A_1,B_1)\cap\Sigma(C_2)=\{1\},\ \Sigma(A_1,B_1)\cap\Sigma(C'_2)=\{1\},$$
$$\Sigma(C_1)\cap\Sigma(A_2,B_2)=\{1\},\ \Sigma(C_1)\cap\Sigma(A'_2,B'_2)=\{1\},$$
$$\Sigma(C_1)\cap\Sigma(C_2)=\{1\},\ \Sigma(C_1)\cap\Sigma(C'_2)=\{1\}.$$

Therefore, either $\Sigma(A_1,B_1,C_1)\cap\Sigma(A_2,B_2,C_2)=\{1\}$ or $\Sigma(A_1,B_1,C_1)\cap\Sigma(A'_2,B'_2,C'_2)=\{1\}$.

We conclude that in these three cases, either $\big((A_1,B_1,C_1),(A_2,B_2,C_2)\big)$ or $\big((A_1,B_1,C_1),(A'_2,B'_2,C'_2)\big)$ is an unmixed Beauville structure of type (τ_1,τ_2).

The conditions are necessary. Assume that the group $G=\mathrm{PSL}_2(q)$ admits an unmixed Beauville structure of type (τ_1,τ_2), where $\tau_i=(r_i,s_i,t_i)$ for $i=1,2$. Then there exist A_1,B_1,C_1,A_2,B_2,C_2 in G of orders r_1,s_1,t_1,r_2,s_2,t_2 respectively, such that $A_1B_1C_1=1=A_2B_2C_2$ and $\langle A_1,B_1\rangle=G=\langle A_2,B_2\rangle$, implying that G is a quotient of the triangle groups T_{r_1,s_1,t_1} and T_{r_2,s_2,t_2} with torsion-free kernel, and so condition *(i)* is necessary.

Moreover, $\Sigma(A_1,B_1,C_1)\cap\Sigma(A_2,B_2,C_2)=\{1\}$, and so by Lemma 4.2, if $p=2$ or e is odd, then each of r_1,s_1,t_1 is necessarily coprime to each of r_2,s_2,t_2, implying that $r_1s_1t_1$ is coprime to $r_2s_2t_2$.

If p is odd and e is even then, by Lemma 4.2, $\gcd(r_1, r_2) = 1$ or p, $\gcd(r_1, s_2) = 1$ or p, $\gcd(r_1, t_2) = 1$ or p, $\gcd(s_1, r_2) = 1$ or p, $\gcd(s_1, s_2) = 1$ or p, $\gcd(s_1, t_2) = 1$ or p, $\gcd(t_1, r_2) = 1$ or p, $\gcd(t_1, s_2) = 1$ or p, and $\gcd(t_1, t_2) = 1$ or p. Moreover, it is not possible that $r_1 = s_1 = t_1 = p$ (respectively $r_2 = s_2 = t_2 = p$), since in this case $e = 1$, by Theorem 3.2. Thus, $g = \gcd(r_1 s_1 t_1, r_2 s_2 t_2) \in \{1, p, p^2\}$.

If moreover, $q = p^e > 9$, p divides g and $\tau_i = (p, p, t_i)$ $(i \in \{1, 2\})$ then $t_i \neq p$ and the condition that $\Sigma(A_1, B_1, C_1) \cap \Sigma(A_2, B_2, C_2) = \{1\}$ implies that A_i is G-conjugate to B_i, by Proposition 4.3. We now deduce from Corollary 3.16 that t_i is a *good G-order.*

If $q = 9$ then it follows from a careful observation of the possible G-triples in Table 6 and Remark 3.18 that necessarily $g = 1$.

In fact, if p is odd, e is even and $q = p^e > 9$, then $\mathrm{PSL}_2(q)$ *always* admits unmixed Beauville structures of type $\big((p, p, t_1), (p, p, t_2)\big)$ for certain t_1, t_2. In the following lemma we explicitly construct such a structure.

Lemma 4.5. *Let $3 < q = p^e$ for some odd prime number p and some positive integer e. Then $\mathrm{PSL}_2(q^2)$ admits an unmixed Beauville structure of type $\big((p, p, t_1), (p, p, t_2)\big)$ for certain t_1 dividing $(q^2 - 1)/2$ and t_2 dividing $(q^2 + 1)/2$.*

Proof. As $q > 3$, the following Remark 4.6 shows that there exist some $b, c \in \mathbb{F}_{q^2}$ such that $b^2, c^2 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, $c^2 - 4$ is a square in $\mathbb{F}_{q^2}$ and $b^2 - 4$ is a non-square in $\mathbb{F}_{q^2}$. Let x be a generator of the multiplicative group $\mathbb{F}_{q^2}^*$ and set $d = b/x$.

Define the following matrices

$$A_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},$$

$$g_1 = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}, \quad g_2 = \begin{pmatrix} 1 & 0 \\ d & 1 \end{pmatrix},$$

$$B_1 = g_1 A_1 g_1^{-1} = \begin{pmatrix} -c+1 & 1 \\ -c^2 & c+1 \end{pmatrix}, \quad B_2 = g_2 A_2 g_2^{-1} = \begin{pmatrix} -dx+1 & x \\ -d^2 x & dx+1 \end{pmatrix},$$

$$C_1 = (A_1 B_1)^{-1} = \begin{pmatrix} c+1 & -c-2 \\ c^2 & -c^2-c+1 \end{pmatrix}, \quad C_2 = (A_2 B_2)^{-1} = \begin{pmatrix} dx+1 & -dx^2-2x \\ d^2 x & -d^2x^2-dx+1 \end{pmatrix}.$$

In this case, $|\bar{A_1}| = |\bar{A_2}| = |\bar{B_1}| = |\bar{B_2}| = p$, and we denote by t_1 and t_2 respectively the orders of $\bar{C_1}$ and $\bar{C_2}$. Moreover, $\bar{A_1}$ and $\bar{B_1}$ are conjugate in $\mathrm{PSL}_2(q^2)$, $\bar{A_2}$ and $\bar{B_2}$ are conjugate in $\mathrm{PSL}_2(q^2)$, whereas $\bar{A_1}$ and $\bar{A_2}$ are not conjugate in $\mathrm{PSL}_2(q^2)$ (see Section 3.5). Now, one needs to verify that $\big((\bar{A_1}, \bar{B_1}, \bar{C_1}), (\bar{A_2}, \bar{B_2}, \bar{C_2})\big)$ is an unmixed Beauville structure for $\mathrm{PSL}_2(q^2)$.

(*i*) By the construction, $\bar{A_1}\bar{B_1}\bar{C_1} = 1 = \bar{A_2}\bar{B_2}\bar{C_2}$.

(*ii*) Observe that $\mathrm{tr}(C_1) = 2 - c^2$ and $\mathrm{tr}(C_2) = 2 - d^2x^2 = 2 - b^2$ both belong to $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$, as c^2 and b^2 both belong to $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Hence, neither $\bar{C_1}$ nor $\bar{C_2}$ is conjugate to some element of $\mathrm{PSL}_2(q)$. We now use the methodology described in Section 3.3. Let $i \in \{1, 2\}$. Since $\mathrm{tr}(A_i) = \mathrm{tr}(B_i) = 2$ but $\mathrm{tr}(C_i) \neq \pm 2$, the triple (A_i, B_i, C_i) is not singular, implying that $\langle \bar{A_i}, \bar{B_i} \rangle$ is not a structural subgroup, by [18, Theorem 2].

As t_i is not an order of an element in $\mathrm{PSL}_2(q)$, it follows from Table 6 that if $q^2 > 9$, then either $p > 5$; or $p = 5$ and $t_i \neq 2, 3, 5$; or $p = 3$ and $t_i > 5$. Therefore,

$\langle \bar{A}_i, \bar{B}_i \rangle$ cannot be a small subgroup. In addition, $(\bar{A}_i, \bar{B}_i, \bar{C}_i)$ is not an irregular $\mathrm{PSL}_2(q^2)$-triple. Therefore, $\langle \bar{A}_i, \bar{B}_i \rangle = \mathrm{PSL}_2(q^2)$ for $i \in \{1,2\}$.

(iii) The characteristic polynomial of C_1 is $\lambda^2 - (2-c^2)+1$, and its discriminant equals $c^2(c^2-4)$, which is a square in $\mathbb{F}_{q^2}$, thus $\bar{C}_1$ is split and so t_1 divides $(q^2-1)/2$. Similarly, the characteristic polynomial of C_2 is $\lambda^2-(2-b^2)+1$, and its discriminant equals $b^2(b^2-4)$, which is a non-square in $\mathbb{F}_{q^2}$, thus $\bar{C}_2$ is non-split and so t_2 divides $(q^2+1)/2$. By Lemma 4.2, $\Sigma(\bar{A}_1, \bar{B}_1, \bar{C}_1) \cap \Sigma(\bar{A}_2, \bar{B}_2, \bar{C}_2) = \{1\}$, since t_1 and t_2 are coprime, $\bar{A}_1$ and $\bar{A}_2$ are not conjugate in $\mathrm{PSL}_2(q^2)$, and so also $\bar{B}_1$ and $\bar{B}_2$ are not conjugate in $\mathrm{PSL}_2(q^2)$.

□

Remark 4.6. Recall that if q is odd then an element in $\mathrm{PSL}_2(q)$ is non-split if and only if the characteristic polynomial $P(\lambda) := \lambda^2 - \alpha\lambda + 1$ of its pre-image $A \in \mathrm{SL}_2(q)$ (where $\alpha = \mathrm{tr}(A)$) has no distinct roots in $\mathbb{F}_q$, or equivalently, the discriminant $\alpha^2 - 4$ is a non-square in $\mathbb{F}_q$. Thus, by [18, Lemma 2], $\#\{b \in \mathbb{F}_q : b^2 - 4 \text{ is a non-square}\} = (q-1)/2$ and $\#\{c \in \mathbb{F}_q : c^2 - 4 \text{ is a square}\} = (q+1)/2$.

Therefore, $\#\{c \in \mathbb{F}_{q^2} : c^2-4 \text{ is a square}\} = (q^2+1)/2$, and $\#\{b \in \mathbb{F}_{q^2} : b^2-4 \text{ is a non-square}\} = (q^2-1)/2$. In addition, $\#\{c \in \mathbb{F}_{q^2} : c^2 \in \mathbb{F}_q\} = 2q-1$, and if $c^2 \in \mathbb{F}_q$ then also $c^2 - 4 \in \mathbb{F}_q$ is a square in $\mathbb{F}_{q^2}$. Hence,

$$\#\{c \in \mathbb{F}_{q^2} : c^2 \notin \mathbb{F}_q,\ c^2 - 4 \text{ is a square}\} = (q^2+1)/2 - (2q-1) = (q^2-4q+3)/2,$$

and

$$\#\{b \in \mathbb{F}_{q^2} : b^2 \notin \mathbb{F}_q,\ b^2 - 4 \text{ is a non-square}\} = (q^2-1)/2.$$

4.4. **Proof of Theorem 2.**

The conditions are necessary. Assume that the group $G_1 = \mathrm{PGL}_2(q)$ admits an unmixed Beauville structure of type $\big((r_1,s_1,t_1),(r_2,t_2,s_2)\big)$. Then there exist A_1,B_1,C_1,A_2,B_2,C_2 in G_1 of orders r_1,s_1,t_1,r_2,s_2,t_2 respectively, such that $A_1B_1C_1 = 1 = A_2B_2C_2$ and $\langle A_1, B_1 \rangle = G_1 = \langle A_2, B_2 \rangle$, implying that G_1 is a quotient of the triangle groups T_{r_1,s_1,t_1} and T_{r_2,s_2,t_2} with torsion-free kernel, and so condition *(i)* is necessary.

Therefore, we may assume that (r_1,s_1,t_1) and (r_2,s_2,t_2) are hyperbolic triples, and moreover they are *irregular w.r.t* q^2 (see §3.3).

If, for example, $\gcd(r_1,r_2) > 2$, then Lemma 4.4 implies that $\Sigma(A_1) \cap \Sigma(A_2)$ is non-trivial, contradicting $\Sigma(A_1,B_1,C_1) \cap \Sigma(A_2,B_2,C_2) = \{1\}$. Hence, condition *(ii)* is necessary.

Since (r_1,s_1,t_1) and (r_2,s_2,t_2) are hyperbolic and irregular, both of them must contain at least two even integers, one of which is greater than 2. Hence, we may assume that r_1,r_2 are even and that $r_1,r_2 > 2$. If both r_1,r_2 divide $q-1$ (respectively $q+1$) then both A_1,A_2 are split (respectively non-split) and by Lemma 4.4, $\Sigma(A_1) \cap \Sigma(A_2) \neq \{1\}$, yielding a contradiction.

Hence, we may assume that r_1 divides $q-1$ and r_2 divides $q+1$, and so A_1 is split and A_2 is non-split. If s_1 (respectively t_1) is even and does not divide $q-1$, then it is necessarily an even integer greater than 2, thus it must divide $q+1$, and so B_1 (respectively C_1) is non-split. Lemma 4.4 implies again that $\Sigma(B_1) \cap \Sigma(A_2) \neq \{1\}$ (respectively $\Sigma(C_1) \cap \Sigma(A_2) \neq \{1\}$), yielding a contradiction. Similarly, if s_2 (respectively t_2) is even, then it necessarily divides $q+1$. Hence, condition *(iii)* is necessary.

Moreover, if C_1 (respectively C_2) has order 2, then the above argument shows that it is necessarily split (respectively non-split). By Corollary 3.9, $(r_1, s_1, 2)$ (respectively $(r_2, s_2, 2)$) is a *good involuting triple w.r.t* q (see Definition 1.5), implying that condition *(iv)* is necessary.

The conditions are sufficient. Let (r_1, s_1, t_1) and (r_2, s_2, t_2) be two hyperbolic triples of integers. Assume that $G_1 = \mathrm{PGL}_2(q)$ is a quotient of the triangle groups T_{r_1,s_1,t_1} and T_{r_2,s_2,t_2} with torsion-free kernel. Then one can find elements $A_1, B_1, C_1, A_2, B_2, C_2$ in G_1 of orders $r_1, s_1, t_1, r_2, s_2, t_2$ respectively, such that $A_1B_1C_1 = 1 = A_2B_2C_2$ and $\langle A_1, B_1\rangle = G_1 = \langle A_2, B_2\rangle$, and so conditions *(i)* and *(ii)* of Definition 1.1 are fulfilled.

We may assume that $A_1, A_2, B_1, B_2 \in G_1 \setminus G$ and that $C_1, C_2 \in G$. Hence r_1, r_2, s_1, s_2 are even. Moreover, by Theorem 3.3, (r_1, s_1, t_1) and (r_2, s_2, t_2) are *irregular w.r.t* q^2.

The condition that $\gcd(r_1, r_2) \le 2$ now implies that one of r_1, r_2 divides $q-1$ and the other divides $q+1$. We may assume that $r_1 \mid q-1$ and $r_2 \mid q+1$, and so A_1 is split and A_2 is non-split. Lemma 4.4 now implies that $\Sigma(A_1) \cap \Sigma(A_2) = \{1\}$.

If $s_1 > 2$, then the condition that $s_1 \mid q-1$ implies that B_1 is split. If $s_1 = 2$ then $(r_1, 2, t_1)$ is a *good involuting triple w.r.t* q and so by Corollary 3.9, B_1 is split. Lemma 4.4 implies again that $\Sigma(B_1) \cap \Sigma(A_2) = \{1\}$.

Similarly, if $s_2 > 2$, then the condition that $s_2 \mid q+1$ implies that B_2 is non-split. If $s_2 = 2$ then $(r_2, 2, t_2)$ is a *good involuting triple w.r.t* q and so by Corollary 3.9, B_2 is non-split. Lemma 4.4 implies again that $\Sigma(A_1) \cap \Sigma(B_2) = \{1\}$ and $\Sigma(B_1) \cap \Sigma(B_2) = \{1\}$.

If $t_1 > 2$ is even, then the condition that $t_1 \mid q-1$ implies that C_1 is split, If $t_1 = 2$ then $(r_1, s_1, 2)$ is a *good involuting triple w.r.t* q and so by Corollary 3.9, C_1 is split. Lemma 4.4 implies again that $\Sigma(C_1) \cap \Sigma(A_2) = \{1\}$ and $\Sigma(C_1) \cap \Sigma(B_2) = \{1\}$. If t_1 is odd, then necessarily $\gcd(t_1, r_2) = 1$ and $\gcd(t_1, s_2) = 1$, and Lemma 4.4 implies that $\Sigma(C_1) \cap \Sigma(A_2) = \{1\}$ and $\Sigma(C_1) \cap \Sigma(B_2) = \{1\}$.

Similarly, if $t_2 > 2$ is even, then the condition that $t_2 \mid q+1$ implies that C_2 is non-split, and if $t_2 = 2$ then $(r_2, s_2, 2)$ is a *good involuting triple w.r.t* q and so by Corollary 3.9, C_2 is non-split. Lemma 4.4 implies again that $\Sigma(A_1) \cap \Sigma(C_2) = \{1\}$ and $\Sigma(B_1) \cap \Sigma(C_2) = \{1\}$. If t_2 is odd, then necessarily $\gcd(r_1, t_2) = 1$ and $\gcd(s_1, t_2) = 1$, and Lemma 4.4 implies that $\Sigma(A_1) \cap \Sigma(C_2) = \{1\}$ and $\Sigma(B_1) \cap \Sigma(C_2) = \{1\}$. Moreover, either $\gcd(t_1, t_2) = 1$, or $\gcd(t_1, t_2) = 2$ and C_1 is split while C_2 is non-split, and so, by Lemma 4.4, $\Sigma(C_1) \cap \Sigma(C_2) = \{1\}$.

To conclude, $\Sigma(A_1, B_1, C_1) \cap \Sigma(A_2, B_2, C_2) = \{1\}$, hence condition *(iii)* of Definition 1.1 is fulfilled.

References

[1] I. Bauer, F. Catanese, F. Grunewald, *Beauville surfaces without real structures*, Geometric methods in algebra and number theory, Progr. Math., vol. **235**, Birkhäuser Boston, (2005), 1–42.

[2] I. Bauer, F. Catanese, F. Grunewald, *Chebycheff and Belyi polynomials, dessins d'enfants, Beauville surfaces and group theory*, Mediterr. J. Math. **3**, **no.2**, (2006), 121–146.

[3] A. Beauville, *Surfaces algébriques complexes*, Astérisque **54**, Paris (1978).

[4] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. **24** (1997), no. 3–4, 235–265.

[5] F. Catanese, *Fibred surfaces, varieties isogenous to a product and related moduli spaces*, Amer. J. Math. **122**, (2000), 1–44.

[6] L.E. Dickson, *Linear groups with an exposition of the Galois field theory* (Teubner, 1901).

[7] B. Fairbairn, K. Magaard, C. Parker, *Generation of finite simple groups with an application to groups acting on Beauville surfaces*, to appear in Proc. London Math. Soc.
[8] Y. Fuertes, G. González-Diez, *On Beauville structures on the groups* S_n *and* A_n, Math. Z. **264** (2010), 959–968.
[9] Y. Fuertes, G. González-Diez, A. Jaikin-Zapirain, *On Beauville surfaces*, Groups Geom. Dyn. **5** (2011), 107–119.
[10] Y. Fuertes, G. Jones, *Beauville surfaces and finite groups*, J. Algebra **340** (2011), 13–27.
[11] S. Garion, M. Larsen, A. Lubotzky, *Beauville surfaces and finite simple groups*, J. Reine Angew. Math. **666** (2012), 225–243.
[12] S. Garion, M. Penegini, *New Beauville surfaces and finite simple groups*, to appear in Manuscripta Math.
[13] D. Gorenstein, *Finite groups*, Chelsea Publishing Co., New York, 1980.
[14] R. Guralnick, G. Malle, *Simple groups admit Beauville structures*, to appear in J. London Math. Soc.
[15] U. Langer, G. Rosenberger, *Erzeugende endlicher projektiver linearer Gruppen*, Results Math. **15** (1989), no. 1-2, 119–148.
[16] F. Levin, G. Rosenberger, *Generators of finite projective linear groups. II.*, Results Math. **17** (1990), no. 1-2, 120–127.
[17] M.W. Liebeck, A. Shalev, *Fuchsian groups, coverings of Riemann surfaces, subgroup growth, random quotients and random walks*, J. Algebra **276** (2004), 552–601.
[18] A.M. Macbeath, *Generators of the linear fractional groups*, Number Theory (Proc. Sympos. Pure Math., Vol. XII, Houston, Tex., 1967), Amer. Math. Soc., Providence, R.I. (1969), 14–32.
[19] C. Marion, *Triangle groups and* $\mathrm{PSL}_2(q)$, J. Group Theory **12** (2009), 689–708.
[20] M. Suzuki, *Group Theory I*, Springer-Verlag, Berlin, 1982.

Max-Planck-Institute for Mathematics, D-53111 Bonn, Germany
Current address: Fachbereich Mathematik und Informatik, Universität Münster, Einsteinstrasse 62, D-48149 Münster, Germany
E-mail address: shelly.garion@uni-muenster.de