ON BEAUVILLE STRUCTURES FOR PSL$(2, q)$

SHELLY GARION

ABSTRACT. We characterize Beauville surfaces of unmixed type with group either PSL$(2, p^e)$ or PGL$(2, p^e)$, thus extending previous results of Bauer, Catanese and Grunewald, Fuertes and Jones, and Penegini and the author.

1. INTRODUCTION

1.1. **Beauville structures.** 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 genera 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. A Beauville surface is in particular a minimal surface of general type. Beauville surfaces were introduced by F. Catanese in [4], inspired by a construction of A. Beauville (see [3]).

We have two cases: the *mixed* case where the action of G exchanges the two factors (and then C_1 and C_2 are isomorphic), and the *unmixed* case where G acts diagonally on their product. In the following we shall consider only the unmixed case.

Working out the definition of an unmixed Beauville surface one sees that there is a purely group theoretical criterion which characterizes the groups of unmixed Beauville surfaces: the existence of what in [2] is called 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 in G which satisfy

(i) $a_1b_1c_1 = 1$ and $a_2b_2c_2 = 1$,

(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

$$\Sigma(a_i, b_i, c_i) := \bigcup_{g\in G} \bigcup_{j=1}^{\infty} \{ga_i^j g^{-1}, gb_i^j g^{-1}, gc_i^j g^{-1}\} \text{ for } i = 1, 2.$$

Moreover, $\tau_i := (\mathrm{ord}(a_i), \mathrm{ord}(b_i), \mathrm{ord}(c_i))$ is called the *type* of (a_i, b_i, c_i) (for $i = 1, 2$), and a type which satisfies the condition $\frac{1}{\mathrm{ord}(a_i)} + \frac{1}{\mathrm{ord}(b_i)} + \frac{1}{\mathrm{ord}(c_i)} < 1$ is called *hyperbolic*.

In this case, we say that G admits an *unmixed Beauville structure of type* (τ_1, τ_2).

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

The author was supported by a European Postdoctoral Fellowship (EPDI) during her stay at the Max-Planck-Institute for Mathematics.

It is known that the following finite almost simple groups admit an unmixed Beauville structure:

(a) The symmetric group S_n, if and only if $n \geq 5$ [2];
(b) The alternating group A_n, if and only if $n \geq 6$ [2, 11];
(c) $\mathrm{PSL}(2,q)$, where $q = p^e$ is a prime power, if and only if $q \geq 7$ [2, 10, 12];
(d) Suzuki groups $\mathrm{Sz}(q)$, where $q = 2^{2e+1}$, and Ree groups $R(q)$, where $q = 3^{2e+1}$ [12];
(e) Some other finite simple groups $G(q)$ of Lie type of low Lie rank, such as $\mathrm{PSL}(3,q)$ and $\mathrm{PSU}(3,q)$, provided that $q = p^e$ is large enough [10].

Moreover, in [10] it is proved that if (r_1,s_1,t_1) and (r_2,s_2,t_2) are two hyperbolic types, then almost all alternating groups A_n admit an unmixed Beauville structure of type $\big((r_1,s_1,t_1),(r_2,s_2,t_2)\big)$. This was previously conjectured by Bauer, Catanese and Grunewald in [2].

Analogously for $\mathrm{PSL}(2,q)$, where $q = p^e$ is a prime power, the aim of this paper is to generalize the results given in [10, 12], and characterize the possible types of an unmixed Beauville structure for the group $\mathrm{PSL}(2,q)$.

The question of which finite groups admit an unmixed Beauville structure is deeply related to the question of which finite groups are quotients of certain triangle groups. 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 $\Delta(\mathrm{ord}(a_i),\mathrm{ord}(b_i),\mathrm{ord}(c_i))$ for $i = 1,2$ with torsion-free kernel. Therefore, we shall now recall some results regarding finite quotients of triangle groups. Note that it is condition *(iii)* of Definition 1.1 which makes the existence of an unmixed Beauville structure for G a more delicate issue.

1.2. **Triangle groups and their finite quotients.** Starting with three positive integers r,s,t, consider the group $\Delta(r,s,t)$ presented by the generators and relations

$$\Delta(r,s,t) = \langle x,y : x^r = y^s = (xy)^t = 1\rangle,$$

known as a *triangle group*.

The triple (r,s,t) is *hyperbolic* if $\frac{1}{r}+\frac{1}{s}+\frac{1}{t} < 1$. In this case, the corresponding triangle group $\Delta(r,s,t)$ is also called *hyperbolic*. Hyperbolic triangle groups are infinite. It is therefore interesting to study their finite quotients, particularly the simple ones therein.

Among all hyperbolic triples (r,s,t), the triple $(2,3,7)$ attains the smallest positive value of $1-\big(\frac{1}{r}+\frac{1}{s}+\frac{1}{t}\big)$. Therefore, the study of the group $\Delta(2,3,7)$, known as the *Hurwitz triangle group*, and its finite quotients, known as *Hurwitz groups*, has attracted much attention, see for example [6] for a historical survey, and [7, 22] and the references therein for the current state of the art.

It was shown by Conder [5] (following Higman) that the alternating group A_n is a Hurwitz group if $n \geq 168$. Concerning the group $\mathrm{PSL}(2,p^e)$, Macbeath [16] has shown that it is a Hurwitz group if and only if either $e = 1$ and $p \equiv 0,\pm 1 \pmod 7$, or $e = 3$ and $p \equiv \pm 2,\pm 3 \pmod 7$.

We thus see different behaviors for the different families of simple groups. Namely, any large enough alternating group is a Hurwitz group, whereas for

PSL$(2,p^e)$, the prime p determines a unique exponent e such that PSL$(2,p^e)$ is a Hurwitz group.

More generally, Higman had already conjectured in the late 1960s that every hyperbolic triangle group has all but finitely many alternating groups as quotients. This was eventually proved by Everitt [9]. Later, Liebeck and Shalev [15] gave an alternative proof based on probabilistic group theory.

Langer and Rosenberger [13] and Levin and Rosenberger [14] had generalized the above result of Macbeath, and determined, for a given prime power $q = p^e$, all the triples (r,s,t) such that PSL$(2,q)$ is a quotient of $\Delta(r,s,t)$, with torsion-free kernel. It follows that if (r,s,t) is hyperbolic, then for almost all primes p, there is precisely one group of the form PSL$(2,p^e)$ or PGL$(2,p^e)$ which is a homomorphic image of $\Delta(r,s,t)$ with torsion-free kernel.

This result will be described in detail is Section 2.1. We note that it can also be obtained by using other techniques. Firstly, Marion [17] has recently provided a proof for the case where r,s,t are primes relying on probabilistic group theoretical methods. Secondly, it also follows from the representation theoretic arguments of Vincent and Zalesski [24]. Such methods can be used for dealing with other families of finite simple groups of Lie type, see for example [18, 19, 21, 24].

1.3. **Organization.** This paper is organized as follows. Section 2 presents the main Theorems in detail. In Section 3 we present some of the basic properties of the groups PSL$(2,q)$ and PGL$(2,q)$ that are needed later for the proofs. The proofs themselves are presented in Section 4.

Acknowledgement. I would like to thank Ingrid Bauer, Fabrizio Catanese and Fritz Grunewald for introducing me to the fascinating world of Beauville structures and for many useful discussions. I am very thankful to Alexandre Zalesski for his interesting comments. I am grateful to Claude Marion for kindly providing me with his recent preprints, and to Matteo Penegini for many interesting discussions and for his remarks on this manuscript.

2. Main Theorems

2.1. Which triangle groups surject onto PSL$(2,q)$?

Notation 2.1. For a prime p and $n \in \mathbb{N}$ such that $\gcd(n,p) = 1$, define

(i) $\mu_{\mathrm{PGL}}(p,n) = \min\{f > 0 \,:\, p^f \equiv \pm 1 \pmod n\}$;

(ii) $\mu_{\mathrm{PSL}}(p,n) = \begin{cases} \min\{f > 0 \,:\, p^f \equiv \pm 1 \pmod n\} & \text{if } n \text{ is odd} \\ \min\{f > 0 \,:\, p^f \equiv \pm 1 \pmod{2n}\} & \text{if } n \text{ is even} \end{cases}$;

(iii) We also set $\mu_{\mathrm{PGL}}(p,p) = 1$ and $\mu_{\mathrm{PSL}}(p,p) = 1$.

Note that $\mu_{\mathrm{PGL}}(p,n)$ (respectively $\mu_{\mathrm{PSL}}(p,n)$) is equal to the minimal integer e such that PGL$(2,p^e)$ (respectively PSL$(2,p^e)$) contains an element of order n.

Notation 2.2. For a prime p and integers $n_1,\dots,n_k$, such that each of them is either relatively prime to p or equal to p, define

(i) $\mu_{\mathrm{PGL}}(p;n_1,\dots,n_k) = \mathrm{lcm}\big(\mu_{\mathrm{PGL}}(p,n_1),\dots,\mu_{\mathrm{PGL}}(p,n_k)\big)$.

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

Note that $\mu_{\mathrm{PGL}}(p; n_1, \ldots, n_k)$ (respectively $\mu_{\mathrm{PSL}}(p; n_1, \ldots, n_k)$) is equal to the minimal integer e such that $\mathrm{PGL}(2, p^e)$ (respectively $\mathrm{PSL}(2, p^e)$) contains k elements of orders $n_1, \ldots, n_k$.

When q is odd, one needs to distinguish triples (r, s, t) of orders of elements that generate $\mathrm{PSL}(2, q)$ from the ones that generate $\mathrm{PGL}(2, q)$. The latter triples are called *irregular* (see [16, §9] and [13, Lemma 3.5]), and contain exactly two orders of elements in $\mathrm{PGL}(2, q) \setminus \mathrm{PSL}(2, q)$ and one order of an element in $\mathrm{PSL}(2, q)$. More precisely, they are defined as follows.

Definition 2.3. Let p be an odd prime, and let (r, s, t) be a hyperbolic triple such that each of r, s, t is either relatively prime to p or equal to p. We say that (r, s, t) is *irregular* if there is a permutation (r', s', t') of (r, s, t) such that one of the following cases occurs.

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 $\frac{e}{2}$.

The following theorems summarize the results in [13, Theorems 4.1 and 4.2] and [14, Theorems 1 and 2].

Theorem A. [13, 14]. *Let p be a prime and assume that $q = p^e$ is at least 7. Let $r, s, t \in \mathbb{N}$. Then $\mathrm{PSL}(2, q)$ is a quotient of $\Delta(r, s, t)$ with torsion-free kernel if and only if (r, s, t) is hyperbolic and satisfies one of the conditions in the following table:*

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') $\gcd(s' \cdot t', p) = 1$	$\mu_{\mathrm{PSL}}(p; s', t')$	*either at most one of r, s, t is even, or:*
$p \geq 3$	$\gcd(r \cdot s \cdot t, p) = 1$	$\mu_{\mathrm{PSL}}(p; r, s, t)$	*if at least two of r, s, t are even, then none of (α), (β), (γ) occurs*
$p = 2$	-	$\mu_{\mathrm{PSL}}(2; r, s, t)$	-

Theorem B. [13, 14]. *Let p be an odd prime and assume that $q = p^e$ is at least 5. Let $r, s, t \in \mathbb{N}$. Then* PGL$(2, q)$ *is a quotient of $\Delta(r, s, t)$ with torsion-free kernel if and only if (r, s, t) is hyperbolic and satisfies one of the conditions in the following table:*

(r,s,t)	e	*further conditions*
permutation of (p, s', t') $\gcd(s' \cdot t', p) = 1$	$\frac{\mu_{\mathrm{PSL}}(p;s',t')}{2}$	*at least two of* r, s, t *are even,* *and*
$\gcd(r \cdot s \cdot t, p) = 1$	$\frac{\mu_{\mathrm{PSL}}(p;r,s,t)}{2}$	*one of* (α), (β), (γ) *occurs*

The following corollary follows immediately from Theorems A and B.

Corollary C. *Let p be a prime and let (r, s, t) be a hyperbolic triple such that each of r, s, t is either relatively prime to p or equal to p. Then there exist a unique exponent e and a unique $G \in \{\mathrm{PSL}, \mathrm{PGL}\}$ such that $G(2, p^e)$ is a quotient of $\Delta(r, s, t)$ with torsion-free kernel, namely*

(a) PSL$(2, p^e)$ *where $e = \mu_{\mathrm{PSL}}(p; r, s, t)$, if (r, s, t) satisfies the conditions of Theorem A.*

(b) PGL$(2, p^e)$ *where $e = \frac{\mu_{\mathrm{PSL}}(p;r,s,t)}{2}$, if (r, s, t) satisfies the conditions of Theorem B.*

Remark 2.4. For completeness, we list below the results for PSL$(2, q)$ where $q < 7$ and for PGL$(2, q)$ where $q < 5$.

For each group in the table below, we list all the triples $r \le s \le t$ such that $\Delta(r, s, t)$ maps onto it with torsion-free kernel (see also [16, §8]).

group	triple(s)
$\mathrm{PSL}(2,2) \cong S_3$	$(2,2,3)$
$\mathrm{PSL}(2,3) \cong A_4$	$(2,3,3), (3,3,3)$
$\mathrm{PGL}(2,3) \cong S_4$	$(2,3,4), (3,4,4)$
$\mathrm{PSL}(2,4) \cong \mathrm{PSL}(2,5) \cong A_5$	$(2,3,5), (2,5,5), (3,3,5), (3,5,5), (5,5,5)$

2.2. **Beauville Structures for** PSL$(2,q)$ **and** PGL$(2,q)$**.** We present here our result concerning the possible types of unmixed Beauville structures for PSL$(2, q)$.

Theorem D. *Let p be a prime and assume that $q = p^e$ is at least 7. Let (r_1, s_1, t_1) and (r_2, s_2, t_2) be two triples of integers. Then the following conditions are sufficient to guarantee that the group* PSL$(2, q)$ *admits an unmixed Beauville structure of type $\big((r_1, s_1, t_1), (r_2, s_2, t_2)\big)$:*

(i) (r_1, s_1, t_1) *and* (r_2, s_2, t_2) *are hyperbolic.*

(ii) Each of (r_1, s_1, t_1) *and* (r_2, s_2, t_2) *satisfy one of the conditions of Theorem A.*

(iii) $r_1 \cdot s_1 \cdot t_1$ *is relatively prime to* $r_2 \cdot s_2 \cdot t_2$.

These conditions are also necessary if either $p = 2$ or p is odd and e is odd. When p is odd and e is even, conditions (i),(ii) together with the following condition (iii') are necessary.

(iii') $\gcd(r_1 \cdot s_1 \cdot t_1, r_2 \cdot s_2 \cdot t_2)$ *divides* p^2.

Note that Beauville structures for $\mathrm{PSL}(2,p^e)$ of type $\big((p,p,t_1),(p,p,t_2)\big)$ do occur (when p is odd and e is even), hence condition *(iii')* cannot be improved (see Lemma 4.5).

Our next result characterizes the possible unmixed Beauville structures for $\mathrm{PGL}(2,q)$.

Theorem E. *Let p be a prime and assume that $q=p^e$ is at least 5. Let (r_1,s_1,t_1) and (r_2,s_2,t_2) be two triples of integers. Then the group $\mathrm{PGL}(2,q)$ admits an unmixed Beauville structure of type $\big((r_1,s_1,t_1),(r_2,s_2,t_2)\big)$ if and only if the following conditions hold:*

- (*i*) *(r_1,s_1,t_1) and (r_2,s_2,t_2) are hyperbolic.*
- (*ii*) *Each of (r_1,s_1,t_1) and (r_2,s_2,t_2) satisfy one of the conditions of Theorem B.*
- (*iii*) *Each of the numbers*

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

  equals 1 or 2.
- (*iv*) *All even elements in one of the triples divide $q-1$, while all even elements in the other triple divide $q+1$.*
- (*v*) *If one of the triples contains an element $t'=2$, then this triple must contain an even element $r'>2$ and a third element $s'>2$, and moreover:*
  - (a) *If $q\equiv 1 \pmod 4$ and r' divides $q-1$, then Case (β) holds;*
  - (b) *If $q\equiv 1 \pmod 4$ and r' divides $q+1$, then Case (γ) holds;*
  - (c) *If $q\equiv 3 \pmod 4$ and r' divides $q-1$, then Case (γ) holds;*
  - (d) *If $q\equiv 3 \pmod 4$ and r' divides $q+1$, then Case (β) holds.*

3. Preliminaries

In this section we shall describe some well-known properties of the groups $\mathrm{PSL}(2,q)$ and $\mathrm{PGL}(2,q)$ (see for example [20, §6]).

3.1. **Definition.** Let K be a field. Recall that $\mathrm{GL}(2,K)$ is the group of invertible 2×2 matrices over K, and $\mathrm{SL}(2,K)$ is the subgroup of $\mathrm{GL}(2,K)$ comprising the matrices with determinant 1. Then $\mathrm{PGL}(2,K)$ and $\mathrm{PSL}(2,K)$ are the quotients of $\mathrm{GL}(2,K)$ and $\mathrm{SL}(2,K)$ by their respective centers.

Let $q=p^e$, where p is a prime and $e\geq 1$. We denote the finite field of size q by $\mathbb{F}_q$. The algebraic closure of $\mathbb{F}_p$ (which is equal to the algebraic closure of $\mathbb{F}_q$) will be denoted by $\overline{\mathbb{F}}_p$.

For simplicity, we shall denote by $\mathrm{GL}(2,q)$, $\mathrm{SL}(2,q)$, $\mathrm{PGL}(2,q)$ and $\mathrm{PSL}(2,q)$ the groups $\mathrm{GL}(2,\mathbb{F}_q)$, $\mathrm{SL}(2,\mathbb{F}_q)$, $\mathrm{PGL}(2,\mathbb{F}_q)$ and $\mathrm{PSL}(2,\mathbb{F}_q)$, respectively.

When q is even, then one can identify $\mathrm{PSL}(2,q)$ with $\mathrm{SL}(2,q)$ and also with $\mathrm{PGL}(2,q)$, and so its order is $q(q-1)(q+1)$. When q is odd, the orders of $\mathrm{PGL}(2,q)$ and $\mathrm{PSL}(2,q)$ are $q(q-1)(q+1)$ and $\frac{1}{2}q(q-1)(q+1)$ respectively, and therefore we can identify $\mathrm{PSL}(2,q)$ with a normal subgroup of index 2 in $\mathrm{PGL}(2,q)$. Moreover, $\mathrm{PSL}(2,q)$ and $\mathrm{PGL}(2,q)$ can be viewed as subgroups of $\mathrm{PSL}(2,\overline{\mathbb{F}}_p)$. Recall that $\mathrm{PSL}(2,q)$ is simple for $q\neq 2,3$.

3.2. **Group elements.** One can classify the elements of PSL$(2, q)$ according to the possible Jordan forms of their pre-images in SL$(2, q)$. The following table lists the three types of elements, according to whether the characteristic polynomial $P(\lambda) := \lambda^2 - \alpha\lambda + 1$ of the matrix $A \in \mathrm{SL}(2, q)$ (where α is the trace of A) has 0, 1 or 2 distinct roots in $\mathbb{F}_q$.

element type	roots of $P(\lambda)$	canonical form in $\mathrm{SL}(2, \overline{\mathbb{F}}_p)$	order	conjugacy classes
unipotent	1 root	$\begin{pmatrix} \pm 1 & 1 \\ 0 & \pm 1 \end{pmatrix}$ $\alpha = \pm 2$	p	two conjugacy classes in PSL$(2, q)$, which unite in PGL$(2, q)$
split	2 roots	$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ where $a \in \mathbb{F}_q^*$ and $a + a^{-1} = \alpha$	divides $\frac{1}{d}(q-1)$ $d = 1$ for q even $d = 2$ for q odd	for each α: one conjugacy class in PSL$(2, q)$
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 $a + a^q = \alpha$	divides $\frac{1}{d}(q+1)$ $d = 1$ for q even $d = 2$ for q odd	for each α: one conjugacy class in PSL$(2, q)$

Recall that if p is odd and $q = p^e$, then any element in PGL$(2, q)$ is either of order p ("unipotent") or of order dividing $q - 1$ ("split"), or of order dividing $q + 1$ ("non-split"). Moreover, any element which belongs to PGL$(2, q)$ but not to PSL$(2, q)$ has an even order dividing either $q - 1$ but not $\frac{q-1}{2}$ or $q + 1$ but not $\frac{q+1}{2}$.

3.3. **Elements of order 2.** Note that all elements of order 2 in 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 $q \equiv 1 \pmod 4$, and non-split if $p \equiv 3 \pmod 4$.

Moreover, if q is an odd prime power, then PGL$(2, q)$ always contains elements of order 2 which are not contained in PSL$(2, q)$. These elements are split if $q \equiv 3 \pmod 4$, and non-split if $q \equiv 1 \pmod 4$.

Therefore, if q is odd, then an element of order 2 in a hyperbolic irregular triple satisfies exactly one of the following:

	$q \equiv 1 \pmod 4$	$q \equiv 3 \pmod 4$
Case (β)	2 is split	2 is non-split
Case (γ)	2 is non-split	2 is split

4. Beauville Structures for PSL$(2, q)$ and PGL$(2, q)$

In this Section we prove Theorems D and E.

4.1. **Cyclic groups.** The following easy Lemma is needed for the proof of Theorems D and E.

Lemma 4.1. *Let C be a finite cyclic group, and let x and y be non-trivial elements in 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. Denote the orders of x and y by a and b respectively, then, by assumption, $\gcd(a,b) = d \neq 1$, and so one can write $a = a'd$ and $b = b'd$, where $\gcd(a',b') = 1$. Hence, $x^{a'}$ and $y^{b'}$ are of exact order d.

Observe that C has only one cyclic subgroup of order d, 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

$$x^{a'k} = z = y^{b'l}.$$

□

4.2. **Elements and conjugacy classes in** $\mathrm{PSL}(2,q)$ **and** $\mathrm{PGL}(2,q)$**.**

Notation 4.2. For a finite group G and $a_1, \dots, a_n \in G$, define

$$\Sigma(a_1, \dots, a_n) = \bigcup_{g \in G} \bigcup_{j=1}^{\infty} \{g a_1^j g^{-1}, \dots, g a_n^j g^{-1}\}.$$

Note that for $n = 3$ this notation coincides with the one given in Definition 1.1*(iii)*.

Observe that for $a_1, \dots, a_n, b_1, \dots, b_m$ the condition

$$\Sigma(a_1, \dots, a_n) \cap \Sigma(b_1, \dots, b_m) = \{1\}$$

is equivalent to the condition that

$$\Sigma(a_i) \cap \Sigma(b_j) = \{1\} \text{ for every } 1 \leq i \leq n, 1 \leq j \leq m.$$

Lemma 4.3. *Let $q = p^e$ be a prime power and let $A_1, A_2 \in \mathrm{PSL}(2,q)$. Then $\Sigma(A_1) \cap \Sigma(A_2) = \{1\}$ if and only if one of the following occurs:*

1. *The orders of A_1 and A_2 are relatively prime;*
2. *p is odd, e is even, $\mathrm{ord}(A_1) = p = \mathrm{ord}(A_2)$ and A_1, A_2 are not conjugate in $\mathrm{PSL}(2,q)$.*

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 different orders, thus

$$\{g_1 A_1^i g_1^{-1}\}_{g_1,i} \cap \{g_2 A_2^j g_2^{-1}\}_{g_2,j} = \{1\},$$

as needed.

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

If there exists some prime $r \neq p$ which divides the orders of A_1 and A_2, then r divides exactly one of $\frac{q-1}{d}$ or $\frac{q+1}{d}$, where $d = 1$ if $p = 2$ and $d = 2$ if p is odd, since $\frac{q-1}{d}$ and $\frac{q+1}{d}$ are relatively prime. Hence, the orders of A_1 and A_2 both divide exactly one of $\frac{q-1}{d}$ or $\frac{q+1}{d}$, and so A_1 and A_2 can be conjugated in $\mathrm{PSL}(2,q)$ to two elements which belong to the same cyclic group (either of order $\frac{q-1}{d}$ or of order $\frac{q+1}{d}$). Lemma 4.1 now implies that there exist some integers i and j such that A_1^i and A_2^j are conjugate in PSL$(2, q)$, and so $\Sigma(A_1) \cap \Sigma(A_2) \neq \{1\}$.

If $\operatorname{ord}(A_1) = p = \operatorname{ord}(A_2)$ then A_1 and A_2 are unipotents, and so, for $k = 1, 2$, A_k can be conjugated in PSL$(2, q)$ to the image of some matrix $A'_k = \begin{pmatrix} 1 & a_k \\ 0 & 1 \end{pmatrix}$, where $a_1, a_2 \in \mathbb{F}_q^*$.

Recall that if $q = 2^e$ then A'_1 and A'_2 are always conjugate in PSL$(2, q)$, and if $q = p^e$ is odd, then A'_1 and A'_2 are conjugate in PSL$(2, q)$ if and only if either both a_1 and a_2 are squares in $\mathbb{F}_q$ or both of them are non-squares.

Note that if p is odd and e is even then all the elements $\{k : 1 \leq k \leq p - 1\}$ are squares in $\mathbb{F}_q$. If p is odd and e is odd, then half of the elements $\{k : 1 \leq k \leq p - 1\}$ are squares in $\mathbb{F}_q$ and half are non-squares.

Therefore, if $q = 2^e$, then A'_1 and A'_2 are necessarily conjugate, and so $\Sigma(A_1) \cap \Sigma(A_2) \neq \{1\}$.

If p is odd and e is even, then for any $1 \leq i, j \leq p - 1$, A_1^i is conjugate to $\begin{pmatrix} 1 & ia_1 \\ 0 & 1 \end{pmatrix}$, which is conjugate to A'_1, and A_2^j is conjugate to $\begin{pmatrix} 1 & ja_2 \\ 0 & 1 \end{pmatrix}$, which is conjugate to A'_2. Hence, $\Sigma(A_1) \cap \Sigma(A_2) \neq \{1\}$ if and only if either both a_1 and a_2 are squares in $\mathbb{F}_q$ or both of them are non-squares, namely, if and only if A'_1 and A'_2 are conjugate.

If p is odd and e is odd, we can choose $1 \leq i, j \leq p - 1$ as follows:

$$i = 1 \text{ if } a_1 \text{ is a square, and } i \text{ is a non-square in } \mathbb{F}_q \text{ otherwise,}$$

$$j = 1 \text{ if } a_2 \text{ is a square, and } j \text{ is a non-square in } \mathbb{F}_q \text{ otherwise,}$$

and so, both A_1^i and A_2^j are conjugate in PSL$(2, q)$ to the image of $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, implying that $\Sigma(A_1) \cap \Sigma(A_2) \neq \{1\}$. □

Lemma 4.4. *Let $q = p^e$ be an odd prime power and let $A_1, A_2 \in$ PGL$(2, q)$. Then $\Sigma(A_1) \cap \Sigma(A_2) = \{1\}$ if and only if one of the following occurs:*

(1) $\gcd(\operatorname{ord}(A_1), \operatorname{ord}(A_2)) = 1$;
(2) *A_1 is split, A_2 is non-split and* $\gcd(\operatorname{ord}(A_1), \operatorname{ord}(A_2)) = 2$;
(3) *A_1 is non-split, A_2 is split and* $\gcd(\operatorname{ord}(A_1), \operatorname{ord}(A_2)) = 2$.

Proof. If $\gcd(\operatorname{ord}(A_1), \operatorname{ord}(A_2)) = 1$ then every two non-trivial powers A_1^i and A_2^j have different orders, thus $\Sigma(A_1) \cap \Sigma(A_2) = \{1\}$, as needed.

If A_1 is split and A_2 is non-split, then necessarily $\gcd(\operatorname{ord}(A_1), \operatorname{ord}(A_2)) \leq 2$, 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 conjugated in PGL$(2, q)$, implying that $\Sigma(A_1) \cap \Sigma(A_2) = \{1\}$ as needed.

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

If $\mathrm{ord}(A_1) = p = \mathrm{ord}(A_2)$, then A_1 and A_2 are unipotents, and so they can be conjugated in $\mathrm{PGL}(2,q)$ to the image of the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, implying that $\Sigma(A_1) \cap \Sigma(A_2) \neq \{1\}$.

Otherwise, $\gcd(\mathrm{ord}(A_1), \mathrm{ord}(A_2)) = r$, where $r > 2$ and $(r,p) = 1$, and so r divides exactly one of $q-1$ or $q+1$, since $\gcd(q-1, q+1) = 2$, implying that $\mathrm{ord}(A_1)$ and $\mathrm{ord}(A_2)$ both divide exactly one of $q-1$ or $q+1$. Hence, A_1 and A_2 can be conjugated in $\mathrm{PGL}(2,q)$ to two elements which belong to the same cyclic group (either of order $q-1$ or of order $q+1$). Lemma 4.1 now implies that there exist some integers i and j such that A_1^i and A_2^j are conjugate in $\mathrm{PGL}(2,q)$, and so $\Sigma(A_1) \cap \Sigma(A_2) \neq \{1\}$. □

4.3. **Proof of Theorem D.**

The conditions are sufficient. Let (r_1, s_1, t_1) and (r_2, s_2, t_2) be two triples of integers. Assume that $\mathrm{PSL}(2,q)$ is a quotient of the triangle groups $\Delta(r_1, s_1, t_1)$ and $\Delta(r_2, s_2, t_2)$ with torsion-free kernel. Then one can find elements $A_1, B_1, C_1, A_2, B_2, C_2 \in \mathrm{PSL}(2,q)$ of orders $r_1, s_1, t_1, r_2, s_2, t_2$ respectively, such that $A_1B_1C_1 = I = A_2B_2C_2$ and $\langle A_1, B_1 \rangle = \mathrm{PSL}(2,q) = \langle A_2, B_2 \rangle$, and so conditions *(i)* and *(ii)* of Definition 1.1 are fulfilled. Moreover, the condition that $r_1 \cdot s_1 \cdot t_1$ is relatively prime to $r_2 \cdot s_2 \cdot t_2$ implies that each of r_1, s_1, t_1 is relatively prime to each of r_2, s_2, t_2, and so by Lemma 4.3, $\Sigma(A_1, B_1, C_1) \cap \Sigma(A_2, B_2, C_2) = \{1\}$, hence condition *(iii)* of Definition 1.1 is fulfilled. Therefore, $\mathrm{PSL}(2,q)$ admits an unmixed Beauville structure of type $\big((r_1, s_1, t_1), (r_2, t_2, s_2)\big)$.

The conditions are necessary. Assume that the group $\mathrm{PSL}(2,q)$ admits an unmixed Beauville structure of type $\big((r_1, s_1, t_1), (r_2, t_2, s_2)\big)$. Then there exist $A_1, B_1, C_1, A_2, B_2, C_2 \in \mathrm{PSL}(2,q)$ of orders $r_1, s_1, t_1, r_2, s_2, t_2$ respectively, such that $A_1B_1C_1 = I = A_2B_2C_2$ and $\langle A_1, B_1 \rangle = \mathrm{PSL}(2,q) = \langle A_2, B_2 \rangle$, implying that $\mathrm{PSL}(2,q)$ is a quotient of the triangle groups $\Delta(r_1, s_1, t_1)$ and $\Delta(r_2, s_2, t_2)$ with torsion-free kernel, and so conditions *(i)* and *(ii)* are necessary.

Moreover, $\Sigma(A_1, B_1, C_1) \cap \Sigma(A_2, B_2, C_2) = \{1\}$, and so by Lemma 4.3, if either $p = 2$ or p is odd and e is odd, then each of r_1, s_1, t_1 is necessarily relatively prime to each of r_2, s_2, t_2, implying that $r_1 \cdot s_1 \cdot t_1$ is relatively prime to $r_2 \cdot s_2 \cdot t_2$.

If p is odd and e is even then, by Lemma 4.3, $\gcd(r_1, r_2) = 1$ 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 $(r_1, s_1, t_1) = (p,p,p) = (r_2, s_2, t_2)$, since in this case $e = 1$ (by Theorem A). Thus, $\gcd(r_1 \cdot s_1 \cdot t_1, r_2 \cdot s_2 \cdot t_2)$ divides p^2.

The following Lemma shows that in case p odd and e even, the condition that $\gcd(r_1 \cdot s_1 \cdot t_1, r_2 \cdot s_2 \cdot t_2)$ divides p^2 cannot be improved.

Lemma 4.5. *Let p be an odd prime and let $q = p^e$. Then the group $\mathrm{PSL}(2,q^2)$ admits an unmixed Beauville structure of type $\big((p,p,t_1),(p,p,t_2)\big)$ where $t_1 \mid \frac{q^2-1}{2}$ and $t_2 \mid \frac{q^2+1}{2}$.*

Proof. Observe that the set

$$D := \{a^2 - 4 : a \in \mathbb{F}_{q^2}, a^2 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q\}$$

contains both squares and non-squares in $\mathbb{F}_{q^2}$. Hence, there exist $b, c \in \mathbb{F}_{q^2}$ such that $b^2, c^2 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, $c^2 - 4$ is a square and $b^2 - 4$ is a non-square.

Let x be a generator of the multiplicative group $\mathbb{F}_{q^2}^*$ and let $d = b/x$.

Define the following matrices

$$A_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},$$
$$g_1 = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}, \quad g_2 = \begin{pmatrix} 1 & 0 \\ d & 1 \end{pmatrix},$$
$$B_1 = gA_1g^{-1} = \begin{pmatrix} -c+1 & 1 \\ -c^2 & c+1 \end{pmatrix}, \quad B_2 = gA_1g^{-1} = \begin{pmatrix} -dx+1 & x \\ -d^2x & dx+1 \end{pmatrix},$$
$$C_1 = (A_1B_1)^{-1} = \begin{pmatrix} c+1 & -c-2 \\ c^2 & -c^2-c+1 \end{pmatrix}, \quad C_2 = (A_2B_2)^{-1} = \begin{pmatrix} dx+1 & -dx^2-2x \\ d^2x & -d^2x^2-dx+1 \end{pmatrix}.$$

Now, one needs to verify that $\big((\bar{A}_1, \bar{B}_1, \bar{C}_1), (\bar{A}_2, \bar{B}_2, \bar{C}_2)\big)$, where $\bar{A}_1, \bar{B}_1, \bar{C}_1$, $\bar{A}_2, \bar{B}_2, \bar{C}_2$ are the images of A_1, B_1, C_1, A_2, B_2, C_2 in PSL$(2, q^2)$, is an unmixed Beauville structure for PSL$(2, q^2)$.

(i) $A_1B_1C_1 = 1 = A_2B_2C_2$ and so $\bar{A}_1\bar{B}_1\bar{C}_1 = 1 = \bar{A}_2\bar{B}_2\bar{C}_2$.

(ii) $\operatorname{tr} C_1 = 2 - c^2$ and $\operatorname{tr} C_2 = 2 - d^2x^2$ both belong to $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$, as c^2 and $b^2 = d^2x^2$ both belong to $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Hence, $\bar{C}_1$ and $\bar{C}_2$ do not belong to PSL$(2, q)$. Moreover, $\bar{A}_1$ and $\bar{B}_1$ do not commute and $\bar{A}_2$ and $\bar{B}_2$ do not commute. Therefore by [16, Theorem 4], $\langle \bar{A}_1, \bar{B}_1 \rangle = \mathrm{PSL}(2, q^2) = \langle \bar{A}_2, \bar{B}_2 \rangle$.

(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 its order divides $\frac{q^2-1}{2}$. 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 its order divides $\frac{q^2+1}{2}$.

By Lemma 4.3, $\Sigma(\bar{A}_1, \bar{B}_1, \bar{C}_1) \cap \Sigma(\bar{A}_2, \bar{B}_2, \bar{C}_2) = \{1\}$, since the orders of $\bar{C}_1$ and $\bar{C}_2$ are relatively prime, and $\bar{A}_1$ and $\bar{A}_2$ are not conjugate in PSL$(2, q^2)$.

□

4.4. **Proof of Theorem E.**

The conditions are necessary. Assume that the group 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 $A_1, B_1, C_1, A_2, B_2, C_2 \in \mathrm{PGL}(2, q)$ of orders $r_1, s_1, t_1, r_2, s_2, t_2$ respectively, such that $A_1B_1C_1 = I = A_2B_2C_2$ and $\langle A_1, B_1 \rangle = \mathrm{PGL}(2, q) = \langle A_2, B_2 \rangle$, implying that PGL$(2, q)$ is a quotient of the triangle groups $\Delta(r_1, s_1, t_1)$ and $\Delta(r_2, s_2, t_2)$ with torsion-free kernel, and so conditions *(i)* and *(ii)* are necessary.

Therefore, we may assume that (r_1, s_1, t_1) and (r_2, s_2, t_2) are hyperbolic and irregular, namely that they satisfy one of the Cases (α), (β), (γ) of Definition 2.3.

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 *(iii)* is necessary.

Since (r_1, s_1, t_1) and (r_2, s_2, t_2) are hyperbolic and irregular, then both of them must contain at least two even numbers, 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 $q-1$ (resp. $q+1$) then both A_1, A_2 are split (resp. 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 one of s_1, t_1 is even and not divides $q-1$, then it is necessarily an even integer greater than 2, thus it must divide $q+1$, and so either B_1 or C_1 is non-split. Lemma 4.4 now implies again that either $\Sigma(B_1) \cap \Sigma(A_2) \neq \{1\}$ or $\Sigma(C_1) \cap \Sigma(A_2) \neq \{1\}$, yielding a contradiction. Hence, condition *(iv)* is necessary.

Moreover, if either B_1 or C_1 has order 2, then the above argument shows that it is necessarily split. Hence, by §3.3, if $q \equiv 1 \pmod 4$, then Case (β) holds, and if $q \equiv 3 \pmod 4$, then Case (γ) holds. Similarly, if either B_2 or C_2 has order 2, then the above argument shows that it is necessarily non-split. Hence, by §3.3, if $q \equiv 1 \pmod 4$, then Case (γ) holds, and if $q \equiv 3 \pmod 4$, then Case (β) holds. Hence, condition *(v)* is necessary.

The conditions are sufficient. Let (r_1, s_1, t_1) and (r_2, s_2, t_2) be two triples of integers. Assume that $\mathrm{PGL}(2, q)$ is a quotient of the triangle groups $\Delta(r_1, s_1, t_1)$ and $\Delta(r_2, s_2, t_2)$ with torsion-free kernel. Then one can find elements $A_1, B_1, C_1, A_2, B_2, C_2 \in \mathrm{PGL}(2, q)$ of orders $r_1, s_1, t_1, r_2, s_2, t_2$ respectively, such that $A_1 B_1 C_1 = I = A_2 B_2 C_2$ and $\langle A_1, B_1 \rangle = \mathrm{PGL}(2, q) = \langle A_2, B_2 \rangle$, and so conditions *(i)* and *(ii)* of Definition 1.1 are fulfilled.

Since, by Theorem B, (r_1, s_1, t_1) and (r_2, s_2, t_2) are hyperbolic and irregular, they must contain at least two even numbers. Hence, we may assume that r_1, r_2, s_1, s_2 are even, that $r_1, r_2 > 2$, that $\mu_{\mathrm{PSL}}(p, r_1)$ and $\mu_{\mathrm{PSL}}(p, r_2)$ do not divide $\frac{e}{2}$, and that $\mu_{\mathrm{PSL}}(p, t_1)$ and $\mu_{\mathrm{PSL}}(p, t_2)$ both divide $\frac{e}{2}$.

The condition that $\gcd(r_1, r_2) \leq 2$ 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 is greater than 2, then the condition that $s_1 \mid q-1$ implies that B_1 is split, and if $s_1 = 2$ then Case (γ) holds, and so $q \equiv 3 \pmod 4$, thus again B_1 is split. Lemma 4.4 implies again that $\Sigma(B_1) \cap \Sigma(A_2) = \{1\}$.

If s_2 is greater than 2, then the condition that $s_2 \mid q+1$ implies that B_2 is non-split, and if $s_2 = 2$ then Case (γ) holds, and so $q \equiv 1 \pmod 4$, thus again 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 is even and greater than 2, then the condition that $t_1 \mid q-1$ implies that C_1 is split, and if $t_1 = 2$ then Case (β) holds, and so $q \equiv 1 \pmod 4$, thus again 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 is even and greater than 2, then the condition that $t_2 \mid q+1$ implies that C_2 is non-split, and if $t_2 = 2$ then Case (β) holds, and so $q \equiv 3 \pmod 4$, thus again 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, *Some new surfaces with $p_g = q = 0$*. Proceeding of the Fano Conference. Torino (2002), 123–142.

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

[3] A. Beauville, *Surfaces Algébriques Complex.* Astérisque **54**, Paris (1978).

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

[5] M.D.E. Conder, *Generators for alternating and symmetric groups*, J. London Math. Soc. **22** (1980) 75–86.

[6] M.D.E. Conder, *Hurwitz groups: a brief survey*, Bull. Amer. Math. Soc. **23** (1990) 359-370.

[7] M.D.E. Conder, *An update on Hurwitz groups*, Groups, Complexity and Cryptology **02** (2010) No. 1.

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

[9] B. Everitt, *Alternating quotients of Fuchsian groups*, J. Algebra **223** (2000) 457–476.

[10] S. Garion, M. Penegini, *New Beauville surfaces, moduli spaces and finite groups*, preprint availiable at arXiv:0910.5402.

[11] Y. Fuertes, G. González-Diez, *On Beauville structures on the groups S_n and A_n*, preprint.

[12] Y. Fuertes, G. Jones, *Beauville surfaces and finite groups*, preprint availiable at arXiv:0910.5489.

[13] U. Langer, G. Rosenberger, *Erzeugende endlicher projektiver linearer Gruppen*, Results Math. **15** (1989), no. 1-2, 119–148.

[14] F. Levin, G. Rosenberger, *Generators of finite projective linear groups. II.*, Results Math. **17** (1990), no. 1-2, 120–127.

[15] M.W. Liebeck, A. Shalev, *Fuchsian groups, coverings of Riemann surfaces, subgroup growth, random quotients and random walks.* J. Algebra **276** (2004) 552–601.

[16] 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.

[17] C. Marion, *Triangle groups and* $\mathrm{PSL}_2(q)$, J. Group Theory **12** (2009), 689–708.

[18] C. Marion, *On triangle generation of finite groups of Lie type*, to appear in J. Group Theory.

[19] L. Di Martino, M.C. Tamburini, A.E. Zalesskii. *On Hurwitz groups of low rank*, Comm. Algebra **28** (2000), no. 11, 5383–5404.

[20] M. Suzuki, *Group Theory I*, Springer-Verlag, Berlin, 1982.

[21] M.C. Tamburini, M. Vsemirnov, *Irreducible* $(2,3,7)$*-subgroups of* $\mathrm{PGL}_n(F)$ *for* $n \leq 7$, J. Algebra **300** No. 1 (2006), 339–362,

[22] M.C. Tamburini, M. Vsemirnov, *Hurwitz groups and Hurwitz generation*, Handbook of Algebra, vol. 4, edited by M. Hazewinkel, Elsevier (2006), 385–426.

[23] M.C. Tamburini, A.E. Zalesskii. *Classical groups in dimension* 5 *which are Hurwitz*, Finite groups 2003, 363–371, Walter de Gruyter, Berlin, 2004.

[24] R. Vincent and A. E. Zalesski, *Non-Hurwitz classical groups*, LMS J. Comput. Math. **10** (2007), 21–82.

Shelly Garion, Max-Planck-Institute for Mathematics, D-53111 Bonn, Germany

E-mail address: shellyg@mpim-bonn.mpg.de