[1]

BEAUVILLE SURFACES WITHOUT REAL STRUCTURES, I.

INGRID BAUER- FABRIZIO CATANESE - FRITZ GRUNEWALD

Abstract. Inspired by a construction by Arnaud Beauville of a surface of general type with $K^2 = 8,\ p_g = 0$, the second author defined the Beauville surfaces as the surfaces which are rigid, i.e., they have no nontrivial deformation, and admit un unramified covering which is isomorphic to a product of curves of genus at least 2.

In this case the moduli space of surfaces homeomorphic to the given surface consists either of a unique real point, or of a pair of complex conjugate points corresponding to complex conjugate surfaces. It may also happen that a Beauville surface is biholomorphic to its complex conjugate surface, neverless it fails to admit a real structure.

First aim of this note is to provide series of concrete examples of the second situation, respectively of the third.

Second aim is to introduce a wider audience, especially group theorists, to the problem of classification of such surfaces, especially with regard to the problem of existence of real structures on them.

Contents

[1]Universität Bayreuth[2]- Universität Düsseldorf

The research of the authors was performed in the realm of the SCHWERPUNKT "Globale Methode in der komplexen Geometrie", and of the EAGER EEC Project.

Date: August 2 , 2004.

1. Introduction

In [Bea] (see p. 159) A. Beauville constructed a new surface of general type with $K^2 = 8$, $p_g = 0$ as a quotient of the product of two Fermat curves of degree 5 by the action of the group $(\mathbb{Z}/5\mathbb{Z})^2$. Inspired by this construction, in the article [Cat00], dedicated to the geometrical properties of varieties which admit an unramified covering biholomorphic to a product of curves, the following definition was given

Definition 1.1. *A Beauville surface is a compact complex surface S which*

1) is rigid , i.e., it has no nontrivial deformation,

2) is isogenous to a higher product, i.e., it admits an unramified covering which is isomorphic (i.e., biholomorphic) to the product of two curves C_1, C_2 of genera ≥ 2.

It was proven in [Cat00] (cf. also [Cat03]) that any surface S isogenous to a higher product has a unique minimal realization as a quotient $S = (C_1 \times C_2)/G$, where G is a finite group acting freely and with the property that no element acts trivially on one of the two factors C_i. Moreover, any other smooth surface X with the same topological Euler number as S, and with isomorphic fundamental group, is diffeomorphic to S, and either X or the conjugate surface $\bar{X}$ belongs to an irreducible family of surfaces containing S as element.

Therefore, in the case that S is a Beauville surface, either X is isomorphic to S, or X is isomorphic to $\bar{S}$.

In order to reduce the description of Beauville surfaces to some group theoretic statement, we need to recall that surfaces isogenous to a higher product belong to two types:

- S is of **unmixed type** if the action of G does not mix the two factors, i.e., it is the product action of respective actions of G on C_1, resp. C_2. We set then $G^0 := G$.
- S is of **mixed type**, i.e., C_1 is isomorphic to C_2, and the subgroup G^0 of transformations in G which do not mix the factors has index precisely 2 in G.

It is obvious from the above definition that every Beauville surface of mixed type has an unramified double covering which is a Beauville surface of unmixed type.

The rigidity property of the Beauville surface is equivalent to the fact that $C_i/G \cong \mathbb{P}^1$ and that the projection $C_i \to C_i/G \cong \mathbb{P}^1$ is branched in three points. Therefore the datum of a Beauville surface of unmixed type is determined, once we look at the monodromy of each covering of $\mathbb{P}^1$, by the datum of a finite group $G = G^0$ together with two respective systems of generators, (a, c)

and (a', c'), which satisfy a further property (*), ensuring that the product action of G on $C \times C'$ is free, where $C := C_1$, $C' := C_2$ are the corresponding curves with an action of G associated to the monodromies determined by (a, c), resp. (a', c').

Define b, b' by the properties $abc = a'b'c' = 1$, let Σ be the union of the conjugates of the cyclic subgroups generated by a, b, c respectively, and define Σ' analogously: then property (*) is the following

$$(*)\ \Sigma \cap \Sigma' = \{1_G\}.$$

In the mixed case, one requires instead that the two systems of generators be related by an automorphism ϕ of G^0 which should satisfy the further conditions:

- ϕ^2 is an inner automorphism, i.e., there is an element $\tau \in G^0$ such that $\phi^2 = \mathrm{Int}_\tau$,
- $\Sigma \cap \phi(\Sigma) = \{1_{G^0}\}$,
- there is no $g \in G^0$ such that $\phi(g)\tau g \in \Sigma$,
- moreover $\phi(\tau) = \tau$ and indeed the elements in the trivial coset of G^0 are transformations of $C \times C$ of the form
$$g(x, y) = (g(x), \phi(g)(y))$$
while transformations in the nontrivial coset are transformations of the form
$$\tau' g(x, y) = (\phi(g)(y), \tau g(x)).$$

Remark 1.2. *The choice of τ is not unique, we can always replace τ by $\phi(g)\tau g$, where $g \in G^0$ is arbitrary, and accordingly replace ϕ by $\phi \circ \mathrm{Int}_g$.*

Observe however that, in the case where G^0 has only inner automorphisms, certainly we cannot find any Beauville surface of mixed type, since the second of the above properties will obviously be violated.

In this paper we use the above definition of Beauville surfaces of unmixed and mixed type to create group-theoretic data which will allow us to treat the following problems:

1. The biholomorphism problem for Beauville surfaces

We introduce sets of structures $\mathbb{U}(G)$ and $\mathbb{M}(G)$ for every finite group G together with groups $\mathrm{A}_{\mathbb{U}}(G)$, $\mathrm{A}_{\mathbb{M}}(G)$ acting on them. We call $\mathbb{U}(G)$ the set of unmixed Beauville structures and $\mathbb{M}(G)$ the set of mixed Beauville structures on G. Using constructions from [Cat00] and [Cat03] we associate an unmixed Beauville surface $S(v)$ to every $v \in \mathbb{U}(G)$ and a mixed Beauville surface $S(u)$ to every $u \in \mathbb{M}(G)$. The minimal Galois representation of every Beauville surface yields a surface $S(v)$ in the unmixed case, respectively a surface $S(u)$ in the mixed case. We then show that $S(v)$ is biholomorphic to $S(v')$ $(v, v' \in \mathbb{U}(G))$ if and only if v lies in the $\mathrm{A}_{\mathbb{U}}(G)$ orbit of v'. We also establish the analogous result in the mixed case.

2. Existence and classification problem for Beauville surfaces

The existence problem now asks for finite groups G such that $\mathbb{U}(G)$ or $\mathbb{M}(G)$ is not empty. So far only abelian groups G were known with $\mathbb{U}(G) \neq \emptyset$. We give many more examples of groups G with $\mathbb{U}(G) \neq \emptyset$. In the mixed case it is not immediately clear that the requirements for the corresponding structures can be met. In fact no examples were known previously. We give here a group theoretic construction which produces finite groups G with $\mathbb{M}(G) \neq \emptyset$.

The classification problem has two meanings. First of all we might like to find all groups G with $\mathbb{U}(G) \neq \emptyset$ or $\mathbb{M}(G) \neq \emptyset$. In [Cat03] all finite abelian groups G are found with $\mathbb{U}(G) \neq \emptyset$ (we give a proof of this fact in Section 3, Theorem 3.4). We show here amongst other things that a group G with $\mathbb{U}(G) \neq \emptyset$ cannot be a non-trivial quotient of one of the non hyperbolic triangle groups.

Our examples however show that this classification problem might be hopeless. In fact we show in Section 3.2 that every finite group G of exponent n with $G.C.D.(n, 6) = 1$, which is generated by 2 elements and which has $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ as abelianization has $\mathbb{U}(G) \neq \emptyset$. Even if, by Zelmanov's solution of the restricted Burnside problem, there is for every n a maximal such group, the number of groups involved here is vast. We also show

Theorem 1.3. *Let G be one of the groups $\mathbf{SL}(2, \mathbb{F}_p)$ or $\mathbf{PSL}(2, \mathbb{F}_p)$ where $\mathbb{F}_p$ is the prime field with p elements and where the prime p is distinct from $2, 3, 5$. Then there is an unmixed Beauville surface with group G.*

A finer classification entails the determination of all orbits of Beauville structures for a fixed group G or for an interesting series of groups. We do not address this problem here.

3. Is S biholomorphic to $\bar{S}$?

We give here examples of Beauville surfaces S such that the complex conjugate surface $\bar{S}$ is not biholomorphic to S. Note that $\bar{S}$ is the same differentiable manifold as S, but with complex structure $-J$ instead of J. To do this we introduce involutions $\iota : \mathbb{U}(G) \to \mathbb{U}(G)$ and $\iota : \mathbb{M}(G) \to \mathbb{M}(G)$. We prove that $S(v)$ $(v \in \mathbb{U}(G))$ is biholomorphic to $\overline{S(v)}$ if and only if v is in the $\mathrm{A}_{\mathbb{U}}(G)$ orbit of $\iota(v)$. We also show the analogous result in the mixed case. We use this to produce the following explicit example:

Theorem 1.4. *Let G be the symmetric group $\mathcal{S}_n$ in $n \geq 8$ letters, let $S(n)$ be the unmixed Beauville surface corresponding to the choice of $a := (5, 4, 1)(2, 6)$, $c := (1, 2, 3)(4, 5, \dots, n)$, and of $a' := \sigma^{-1}$, $c' := \tau\sigma^2$, where $\tau := (1, 2)$ and $\sigma := (1, 2, \dots, n)$.*

Then $S(n)$ is not biholomorhic to $\overline{S(n)}$ provided that $n \equiv 2 \bmod 3$.

We shall now give the construction of a mixed Beauville surface with the same property. We shall first describe the group G and its subgroup G^0.

Let H be nontrivial group. Let $\Theta : H \times H \to H \times H$ be the automorphism defined by $\Theta(g, h) := (h, g)$ $(g, h \in H)$. We consider the semidirect product

$$G := H_{[4]} := (H \times H) \rtimes \mathbb{Z}/4\mathbb{Z} \tag{1}$$

where the generator 1 of $\mathbb{Z}/4\mathbb{Z}$ acts through Θ on $H \times H$. Since Θ^2 is the identity we find

$$G^0 := H_{[2]} := H \times H \times 2\mathbb{Z}/4\mathbb{Z} \cong H \times H \times \mathbb{Z}/2\mathbb{Z} \tag{2}$$

as a subgroup of index 2 in $H_{[4]}$.

Theorem 1.5. *Let p be a prime with $p \equiv 3$ mod 4 and $p \equiv 1$ mod 5 and consider the group $H := \mathbf{SL}(2, \mathbb{F}_p)$. Let S be the mixed Beauville surface corresponding to the data $G := H_{[4]}$, $G^0 := H_{[2]}$ and to a certain system of generators (a, c) of $H_{[2]}$ with $\mathrm{ord}(a) = 20$, $\mathrm{ord}(c) = 30$, $\mathrm{ord}(a^{-1}c^{-1}) = 5p$.*

Then S is not biholomorhic to $\overline{S}$.

Different types of examples of rigid surfaces S which are not isomorphic to $\bar{S}$ have been constructed in [K-K02], using Hirzebruch type examples of ball quotients.

4. Is S real?

A surface S is said to be real if there exists a biholomorphism $\sigma : S \to \bar{S}$ with the property that $\sigma^2 = \mathrm{Id}$. In this case we say that S has a real structure. We translate this problem into group theory and obtain the following examples.

Theorem 1.6. *Let $p > 5$ be a prime with $p \equiv 1$ mod 4, $p \not\equiv 2, 4$ mod 5, $p \not\equiv 5$ mod 13 and $p \not\equiv 4$ mod 11. Set $n := 3p+1$. Then there is an unmixed Beauville surface S with group $\mathcal{A}_n$ which is biholomorphic to the complex conjugate surface $\bar{S}$ but is not real.*

Further examples of real and non real Beauville surfaces will be given in the sequel to this paper.

Acknowledgement: We thank Benjamin Klopsch for help with the alternating groups.

2. Triangular curves and group actions

In this section we recall the construction of triangular curves as given in [Cat00], [Cat03]. They are the building blocks for the Beauville surfaces of both unmixed and mixed type. We add some group-theoretic observations which will help with the classification problems of Beauville surfaces which were mentioned above and which will be studied later.

We need the following group theoretic notation. Let G be a group and let M, N be two sets equipped with an action (from the left) of G. We say that a map $\sigma : M \to N$ is *G-twisted-equivariant* if there is an automorphism $\psi : G \to G$ of G with

$$\sigma(gP) = \psi(g)\sigma(P) \quad \text{for all } g \in G, P \in M. \tag{3}$$

Let now G be a finite group and (a, c) a pair of elements of G. We define

$$\Sigma(a, c) := \bigcup_{g \in G} \bigcup_{i=0}^{\infty} \{ga^i g^{-1}, gc^i g^{-1}, g(ac)^i g^{-1}\} \tag{4}$$

to be the union of the G-conjugates of the cyclic groups generated by a, c and ac. Moreover set

$$\mu(a,c) := \frac{1}{\mathrm{ord}(a)} + \frac{1}{\mathrm{ord}(c)} + \frac{1}{\mathrm{ord}(ac)}, \tag{5}$$

where $\mathrm{ord}(a)$ stands for the order of the element $a \in G$. We furthermore call

$$(\mathrm{ord}(a), \mathrm{ord}(c), \mathrm{ord}(ac)) \tag{6}$$

the *type* of the pair (a,c) and define

$$\nu(a,c) := \mathrm{ord}(a)\mathrm{ord}(c)\mathrm{ord}(ac). \tag{7}$$

We consider here finite groups G having a pair (a,c) of generators. Setting $(r,s,t) := (\mathrm{ord}(a), \mathrm{ord}(c), \mathrm{ord}(ac))$, such a group is a quotient of the triangle group

$$T(r,s,t) := \langle x, y \mid x^r = y^s = (xy)^t = 1 \rangle. \tag{8}$$

We define

$$\mathbb{T}(G) := \{(a,c) \in G \times G \mid \langle a, c \rangle = G\}. \tag{9}$$

Given $(a,c) \in \mathbb{T}(G)$ we shall consider the *triangular triple* $(a,b,c) := (a, a^{-1}c^{-1}, c)$ attached to (a,c). Clearly the automorphism group $\mathrm{Aut}(G)$ of G acts diagonally on $\mathbb{T}(G)$. If $\mathbb{T}(G) \neq \emptyset$ then this action is faithful. We define additionally the following permutations of $\mathbb{T}(G)$:

$$\sigma_0 : (a,c) \mapsto (a,c),\ \sigma_1 : (a,c) \mapsto (a^{-1}c^{-1}, a),\ \sigma_2 : (a,c) \mapsto (c, a^{-1}c^{-1}), \tag{10}$$

$$\sigma_3 : (a,c) \mapsto (c,a),\ \sigma_4 : (a,c) \mapsto (c^{-1}a^{-1}, c),\ \sigma_5 : (a,c) \mapsto (a, c^{-1}a^{-1}). \tag{11}$$

Observe that the set $\mathbb{T}(G)$ is in bijection with the set of triples $\mathbb{T}_{\mathrm{tr}}(G) := \{(a,b,c) | abc = 1\}$. By looking at those triples we see that σ_0 is the identity, σ_1 is the 3-cycle $(a,b,c) \to (b,c,a)$, σ_3 is the permutation $(a,b,c) \to (c, c^{-1}bc, a)$, while $\sigma_2 = \sigma_1^2$ and $\sigma_1\sigma_3 = \sigma_4,\ \sigma_1^2\sigma_3 = \sigma_5$. We see therefore that we have the relations:

$$\sigma_1^3 = \sigma_3^2 = \sigma_0,\ \sigma_2 = \sigma_1^2,\ \sigma_1\sigma_3 = \sigma_4,\ \sigma_1^2\sigma_3 = \sigma_5, \tag{12}$$

$$(\sigma_1\sigma_3)^2 = \sigma_4^2 = \mathrm{Int}_{c^{-1}} \circ \sigma_0. \tag{13}$$

Let us write

$$\mathrm{A}_{\mathbb{T}}(G) := \langle \mathrm{Aut}(G), \sigma_1, \dots, \sigma_5 \rangle \tag{14}$$

for the permutation group generated by these operations. The above equations show that we have a homomorphism of the symmetric group $\mathcal{S}_3$ into $\mathrm{A}_{\mathbb{T}}(G)/\mathrm{Int(G)}$ and that $\mathrm{Aut}(G)$ is a normal subgroup of index ≤ 6 in $\mathrm{A}_{\mathbb{T}}(G)$, with quotient a subgroup of $\mathcal{S}_3$. In particular, every element $\rho \in \mathrm{A}_{\mathbb{T}}(G)$ can be written as

$$\rho = \psi \circ \sigma_i \tag{15}$$

for an automorphism ψ of G and an element σ_i from the above list.

We also define

$$\mathrm{I}_{\mathbb{T}}(G) := \langle \mathrm{Int}(G), \sigma_1, \dots, \sigma_5 \rangle \tag{16}$$

where $\mathrm{Int}(G)$ the (normal) subgroup of $\mathrm{A}_{\mathbb{T}}(G)$ consisting of the inner automorphisms.

By an operation from $\mathrm{A}_{\mathbb{T}}(G)$ we may always ensure that a pair $(a,c) \in \mathbb{T}(G)$ satisfies

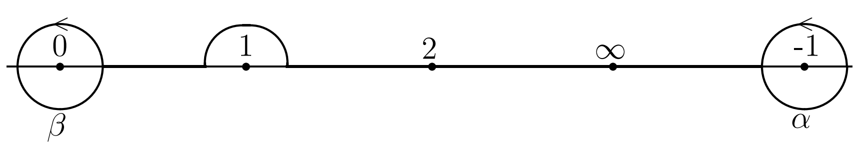
$$\mathrm{ord}(a) \le \mathrm{ord}(b) = \mathrm{ord}(a^{-1}c^{-1}) \le \mathrm{ord}(c)$$

in which case we call the pair *normalised*. We call (a,c) *strict*, if all inequalities are strict, *critical* if all the three orders are equal, and *subcritical* otherwise.

We shall attach now a complex curve $C(a,c)$ to every pair $(a,c) \in \mathbb{T}(G)$. It will be constructed as a ramified covering of $\mathbb{P}^1_{\mathbb{C}}$. Consider the set $B \subset \mathbb{P}^1_{\mathbb{C}}$ consisting of three real points $B := \{-1,0,1\}$. We choose ∞ as a base point in $\mathbb{P}^1_{\mathbb{C}} - B$, and we take the following generators α, β, γ of $\pi_1(\mathbb{P}^1_{\mathbb{C}} - B, \infty)$:

- α goes from ∞ to $-1-\epsilon$ along the real line, passing through -2, then makes a full turn counterclockwise around the circumference with centre -1 and radius ϵ, then goes back to 2 along the same way on the real line.
- γ goes from ∞ to $1+\epsilon$ along the real line, then makes a full turn counterclockwise around the circumference with centre $+1$ and radius ϵ, then goes back to ∞ along the same way on the real line.
- β goes from ∞ to $1+\epsilon$ along the real line, makes a half turn counterclockwise around the circumference with centre $+1$ and radius ϵ, reaching $1-\epsilon$, then proceeds along the real line reaching $+\epsilon$, makes a full turn counterclockwise around the circumference with centre 0 and radius ϵ, goes back to $1-\epsilon$ along the same way on the real line, makes again a half turn clockwise around the circumference with centre $+1$ and radius ϵ, reaching $1+\epsilon$, finally it proceeds along the real line returning to ∞.

A graphical picture of α, β, is:



Writing α, β, γ for the corresponding elements of $\pi_1(\mathbb{P}^1_{\mathbb{C}} - B, \infty)$ we find

$$\pi_1(\mathbb{P}^1_{\mathbb{C}} - B, \infty) = \langle \alpha, \beta, \gamma \mid \alpha\beta\gamma = 1 \rangle$$

and α, γ are free generators of $\pi_1(\mathbb{P}^1_{\mathbb{C}} - B, \infty)$.

Let now G be a finite group and $(a,c) \in \mathbb{T}(G)$. Observe that by Riemann's existence theorem the elements a, $b = a^{-1}c^{-1}$, c, once we fixed a basis of the fundamental group of $\mathbb{P}^1_{\mathbb{C}} - \{-1,0,1\}$ as above, give rise to a surjective homomorphism

$$\pi_1(\mathbb{P}^1_{\mathbb{C}} - B, \infty) \to G, \qquad \alpha \mapsto a,\ \gamma \mapsto c \tag{17}$$

and to a Galois covering $\lambda : C \to \mathbb{P}^1_{\mathbb{C}}$ ramified only in $\{-1, 0, 1\}$ with ramification indices equal to the orders of a, b, c and with group G (beware, this means that these data yield a well determined action of G on $C(a, c)$).

We call this covering a *triangular covering.* We embed G into $\mathcal{S}_G$ as the transitive subgroup of left translations. The monodromy homomorphism [1]

$$m_\lambda : \pi_1(\mathbb{P}^1_{\mathbb{C}} - B, \infty) \to \mathcal{S}_G$$

maps onto the embedded subgroup G and is the same as the homomorphism (17).

Note that by Hurwitz's formula we have

$$g(C(a, c)) = 1 + \frac{1 - \mu(a, c)}{2}\ |G| \tag{18}$$

for the genus $g(C(a, c))$ of the curve $C(a, c)$.

Let now (a, c), $(a', c') \in \mathbb{T}(G)$. A *twisted covering isomorphism* from the Galois covering $\lambda : C(a, c) \to \mathbb{P}^1_{\mathbb{C}}$ to the Galois covering $\lambda' : C(a', c') \to \mathbb{P}^1_{\mathbb{C}}$ is a pair (σ, δ) of biholomorphic maps $\sigma : C(a, c) \to C(a', c')$ and $\delta : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ with $\delta(B) = B$ such that the diagram

$$\begin{array}{ccc} C(a,c) & \xrightarrow{\sigma} & C(a',c') \\ \Big\downarrow \lambda & & \Big\downarrow \lambda' \\ \mathbb{P}^1_{\mathbb{C}} & \xrightarrow{\delta} & \mathbb{P}^1_{\mathbb{C}}. \end{array} \tag{19}$$

is commutative. We shall moreover say that we have a *strict covering isomorphism* if moreover the map δ is the identity.

Consider now G as acting on $C(a, c)$ as a group of covering transformations over λ, and conjugate a transformation $g \in G$ by σ: since $\sigma \circ g \circ \sigma^{-1}$ is a covering transformation of $C(a', c')$, we obtain in this way an automorphism ψ of G (attached to the biholomorphic equivalence (σ, δ)) such that

$$\sigma(gP) = \psi(g)\sigma(P) \quad \text{for all } g \in G, P \in C(a, c).$$

That is, the map $\sigma : C(a, c) \to C(a', c')$ is G-twisted-equivariant.

Remark 2.1. *We claim that ψ is the identity if we have a strict covering isomorphism. The converse does not necessarily hold, as it is shown by the example of $G = \mathbb{Z}/3\mathbb{Z}$ as a quotient of $T(3, 3, 3)$, where all the three elements α, β, γ have the same image $= 1$ mod 3 (see the following considerations).*

In order to understand the equivalence relation induced by the covering isomorphisms on the set $\mathbb{T}(G)$ of triangle structures, recall the following well known facts from the theory of ramified coverings (see [Mi]):

A) The monodromy homomorphism is only determined by the choice of a base point ∞' lying over ∞; a different choice alters the monodromy up to composition with an inner automorphism (corresponding to a transformation carrying one base point to the other).

[1] Actually, with the usual conventions the monodromy is an antihomomorphism; there are two ways to remedy this problem, here we shall do it by considering the composition of paths $\gamma \circ \delta$ as the path obtained by following first δ and then γ .

B) The map δ induces isomorphisms

$$\delta_* : \pi_1(\mathbb{P}^1_{\mathbb{C}} \setminus B, \infty) \to \pi_1(\mathbb{P}^1_{\mathbb{C}} \setminus B, \delta(\infty)) \to \pi_1(\mathbb{P}^1_{\mathbb{C}} \setminus B, \infty)$$

the second being induced by the choice of a path from ∞ to $\delta(\infty)$.

Since the stabiliser of a chosen base point lying over ∞ under the monodromy action is equal to the kernel of the monodromy homomorphism m_λ, the class of monodromy homomorphisms corresponding to the covering $C(a', c')$ is obtained from the one of the given μ (corresponding to $C(a, c)$) by composing with $(\delta_*)^{-1}$. In particular, we may set $a'' := \mu(\delta_*)^{-1}(\alpha)$, and $c'' := \mu(\delta_*)^{-1}(\gamma)$. It follows also that ψ is gotten from the natural isomorphism of $\pi_1(\mathbb{P}^1_{\mathbb{C}} \setminus B, \infty)/ker\mu \to \pi_1(\mathbb{P}^1_{\mathbb{C}} \setminus B, \infty)/ker(\mu \circ (\delta_*)^{-1})$ induced by (δ_*), and the obvious identifications of these quotient groups with G (in more concrete terms, ψ sends $a'' \to a'$, $c'' \to c'$).

C) The above shows that if the isomorphism is strict, then ψ is the identity. The converse does not hold since ψ can be the identity, without δ_* being the identity.

Proposition 2.2. *Let G be a finite group and (a, c), $(a', c') \in \mathbb{T}(G)$. The following are equivalent:*

(i-t) there is a twisted covering isomorphism from $\lambda : C(a, c) \to \mathbb{P}^1_{\mathbb{C}}$ to the Galois covering $\lambda' : C(a', c') \to \mathbb{P}^1_{\mathbb{C}}$,

(ii-t) there is a G-twisted-equivariant biholomorphic map $\sigma : C(a, c) \to C(a', c')$,

(iii-t) (a, c) is in the $\mathrm{A}_{\mathbb{T}}(G)$-orbit of (a', c').

Respectively, the following are equivalent:

(i-s) there is a strict covering isomorphism from $\lambda : C(a, c) \to \mathbb{P}^1_{\mathbb{C}}$ to the Galois covering $\lambda' : C(a', c') \to \mathbb{P}^1_{\mathbb{C}}$,

(ii-s) there is a G-equivariant biholomorphic map $\sigma : C(a, c) \to C(a', c')$,

(iii-s) (a, c) is in the $\mathrm{I}_{\mathbb{T}}(G)$-orbit of (a', c').

Proof. The equivalence of (i) and (ii) follows directly from the definition. In view of A) we only consider triangle structures up to action of $\mathrm{Int}(G)$. We have seen that two triangle structures yield coverings which are twisted covering isomorphic if and only if there is an automorphism δ of $(\mathbb{P}^1_{\mathbb{C}} - B)$ and an automorphism $\psi \in \mathrm{Aut}(G)$ such that $\psi \circ \mu = \mu' \circ \delta_*$.

In particular, $a'' := \mu(\delta_*)^{-1}(\alpha)$, $c'' := \mu(\delta_*)^{-1}(\gamma)$ are ψ equivalent to a', c', and it suffices to show that they are obtained from (a, c) by one of the transformations σ_i. Observe however that the group of projectivities $\mathrm{Aut}(\mathbb{P}^1_{\mathbb{C}} - B)$ is isomorphic to the group of permutations of B, by the fundamental theorem on projectivities.

We see immediately the action of an element of order two: namely, consider the projectivity $z \to -z$: this leaves the base point ∞ fixed, as well as the point 0, and acts by sending $\alpha \to \gamma$, $\gamma \to \alpha$: we obtain in this way the transformation σ_3 on the set of triangle structures.

In order to obtain the transformation σ_1 of order three, it is more convenient, after a projectivity, to assume that the set B consists of the three cubic roots of unity. Setting $\omega = \exp(2\pi i/3)$ and $B = \{1, \omega, \omega^2\}$, one sees immediately that σ_1 is induced by the automorphism $z \to \omega z$, which leaves again the base point ∞ fixed and cyclically permutes α, β, γ.

Q.E.D.

To be able to treat questions of reality we define

$$\iota(a, c) := (a^{-1}, c^{-1}) \tag{20}$$

for $(a, c) \in \mathbb{T}(G)$ and call it the *conjugate* of (a, c). Note that we have $\iota(a, c) \in \mathbb{T}(G)$ and also $\Sigma(\iota(a, c)) = \Sigma(a, c)$, $\mu(\iota(a, c)) = \mu(a, c)$. A feature built into our construction is:

Proposition 2.3. *Let G be a finite group and $(a, c) \in \mathbb{T}(G)$ then*

$$C(\iota(a, c)) = \overline{C(a, c)}. \tag{21}$$

Proof. For the proof note that by construction the complex conjugates of the paths α, γ used in the construction of the triangular curves $C(a, c)$ satisfy $\bar{\alpha} = \alpha^{-1}$, $\bar{\gamma} = \gamma^{-1}$. *Q.E.D.*

We now remind the reader of the operations $\sigma_0, \dots, \sigma_5$ defined in 10, 11. For later use we observe:

Lemma 2.4. *Let G be a finite group and $(a, c) \in \mathbb{T}(G)$. Let $\rho = \psi \circ \sigma_i \in \mathrm{A}_{\mathbb{T}}(G)$.*

(i) In case $i = 0$, $\rho(a, c) = \iota(a, c)$ if and only if $\psi(a) = a^{-1}$ and $\psi(c) = c^{-1}$.

(ii) In case $i = 1$, $\rho(a, c) = \iota(a, c)$ if and only if $\psi(a) = c^{-1}$ and $\psi(c) = ac$.

(iii) In case $i = 2$, $\rho(a, c) = \iota(a, c)$ if and only if $\psi(a) = ac$ and $\psi(c) = a^{-1}$.

(iv) In case $i = 3$, $\rho(a, c) = \iota(a, c)$ if and only if $\psi(a) = c^{-1}$ and $\psi(c) = a^{-1}$.

(v) In case $i = 4$, $\rho(a, c) = \iota(a, c)$ if and only if $\psi(a) = ac$ and $\psi(c) = c^{-1}$.

(vi) In case $i = 5$, $\rho(a, c) = \iota(a, c)$ if and only if $\psi(a) = a^{-1}$ and $\psi(c) = ac$.

Using the notation of the lemma we assume that $\rho(a, c) = \psi \circ \sigma_i(a, c) = \iota(a, c)$ and get the formulae

$(\psi \circ \sigma_0)^2(a, c) = (a, c)$, $(\psi \circ \sigma_1)^2(a, c) = (c^{-1}ac, c)$, $(\psi \circ \sigma_2)^2(a, c) = (a, aca^{-1})$,
$(\psi \circ \sigma_3)^2(a, c) = (a, c)$, $(\psi \circ \sigma_4)^2(a, c) = (c^{-1}ac, c)$, $(\psi \circ \sigma_5)^2(a, c) = (a, aca^{-1})$,
for the square of ρ on (a, c).

3. The unmixed case

In this section we shall translate the problem of existence and classification of Beauville surfaces S of unmixed type into purely group-theoretic problems.

3.1. **Unmixed Beauville surfaces and group actions.** To have the group theoretic background for the construction of Beauville surfaces from [Cat00] we make the following definition.

Definition 3.1. *Let G be a finite group G. We say that a quadruple $v = (a_1, c_1; a_2, c_2)$ of elements of G is an unmixed Beauville structure for G (for short: u-Beauville) if and only if*

(i) the pairs a_1, c_1, and a_2, c_2 both generate G,

(ii) $\Sigma(a_1, c_1) \cap \Sigma(a_2, c_2) = \{1_G\}$.

The group G admits an unmixed Beauville structure if such a quadruple v exists. We write $\mathbb{U}(G)$ for the set of unmixed Beauville structures on G.

We shall need an appropriate notion of equivalence of unmixed Beauville structures. In order to clarify it, let us observe that a Beauville surface has a unique minimal realization ([Cat00], [Cat03]), and that the Galois group of this covering is isomorphic to G. This yields an action of G on the product $C_1 \times C_2$ (whence, two actions of G^0 on both factors) only after we fix an isomorphism of the Galois group with G. In turn, these two actions of G determine a triangular covering up to strict covering isomorphism, so that we can apply Proposition 2.2.

Note that for $(\psi_1, \psi_2) \in \mathrm{I}_{\mathbb{T}}(G)$ and $(a_1, c_1; a_2, c_2) \in \mathbb{U}(G)$ we have $(\psi_1(a_1, c_1); \psi_2(a_2, c_2)) \in \mathbb{U}(G)$. Thus we have a faithful action of $\mathrm{I}_{\mathbb{T}}(G) \times \mathrm{I}_{\mathbb{T}}(G)$ on $\mathbb{U}(G)$. Consider now the group $\mathrm{B}_{\mathbb{U}}(G)$ generated by the action of $\mathrm{I}_{\mathbb{T}}(G) \times \mathrm{I}_{\mathbb{T}}(G)$ and by the diagonal action of $\mathrm{Aut}(G)$ (such that ($\psi \in \mathrm{Aut}(G)$ carries $(a_1, c_1; a_2, c_2) \in \mathbb{U}(G)$ to $(\psi(a_1, c_1); \psi(a_2, c_2)) \in \mathbb{U}(G)$).

We additionally define the following operation

$$\tau((a_1, c_1; a_2, c_2)) := (a_2, c_2; a_1, c_1) \tag{22}$$

on the elements of $\mathbb{U}(G)$ and let

$$\mathrm{A}_{\mathbb{U}}(G) := \langle \mathrm{B}_{\mathbb{U}}(G),\, \tau \rangle \tag{23}$$

be the permutation group generated by these permutations of $\mathbb{U}(G)$. Note that $\mathrm{B}_{\mathbb{U}}(G)$ is a normal subgroup of index ≤ 2 in $\mathrm{A}_{\mathbb{U}}(G)$.

Given an element $v := (a_1, c_1; a_2, c_2) \in \mathbb{U}(G)$ we define now

$$S(v) := C(a_1, c_1) \times C(a_2, c_2)/G. \tag{24}$$

The second condition in our definition of $\mathbb{U}(G)$ ensures that the action of G on the product has no fixed point, hence the covering $C(a_1, c_1) \times C(a_2, c_2) \to S(v)$ is unramified. We call the surface $S(v)$ an *unmixed Beauville surface*. It is obvious that (24) is a *minimal Galois realization* (see [Cat00], [Cat03]) of $S(v)$. Our next result shows that the unmixed Beauville surface $S(v)$ is isogenous to a *higher product* in the terminology of [Cat00].

Proposition 3.2. *Let G be a finite, non-trivial group with an unmixed Beauville structure $(a_1, c_1; a_2, c_2) \in \mathbb{U}(G)$. Then $\mu(a_1, c_1) < 1$ and $\mu(a_2, c_2) < 1$. Whence we have: $g(C(a_1, c_1)) \geq 2$ and $g(C(a_2, c_2)) \geq 2$.*

Proof. We may without loss of generality assume that G is not cyclic. Suppose (a_1, c_1) satisfies $\mu(a_1, c_1) > 1$: then the type of (a_1, c_1) is up to permutation amongst the

$$(2, 2, n)\ (n \in \mathbb{N}),\ (2, 3, 3),\ (2, 3, 4),\ (2, 3, 5).$$

In the first case G is a quotient group of the infinite dihedral group and G cannot admitt an unmixed Beauville structure by Lemma 3.7. There are the following isomorphisms of triangular groups

$$T(2, 3, 3) = \mathcal{A}_4,\ T(2, 3, 4) = \mathcal{S}_4,\ T(2, 3, 5) = \mathcal{A}_5,$$

see [Cox], Chapter 4. These groups do not admit an unmixed Beauville structure by Proposition 3.6.

If $\mu(a_1, c_1) = 1$ then the type of (a_1, c_1) is up to permutation amongst the

$$(3, 3, 3),\ (2, 4, 4),\ (2, 3, 6)$$

and G is a finite quotient of one of the wall paper groups and cannot admit an unmixed Beauville structure by the results of Section 6.

The second statement follows now from formula 18 since then $g(C(a_i, c_i))$, for $i = 1, 2$, is an integer strictly greater than 1. *Q.E.D.*

We may now apply results from [Cat00], [Cat03] to prove:

Proposition 3.3. *Let G be a finite group and $v, v' \in \mathbb{U}(G)$. Then $S(v)$ is biholomorphically isomorphic to $S(v')$ if and only if v is in the $\mathrm{A}_{\mathbb{U}}(G)$-orbit of v'.*

Proof. Let $v = (a_1, c_1; a_2, c_2)$, $v' = (a'_1, c'_1; a'_2, c'_2)$. Assume that there is a biholomorphism between two unmixed Beauville surfaces $S(v)$ and $S(v')$. This happens, by Proposition 3.2 of [Cat03], if and only if there is a product biholomorphism (up to a possible interchange of the factors)

$$\sigma : C(a_1, c_1) \times C(a_2, c_2) \to C(a'_1, c'_1) \times C(a'_2, c'_2)$$

of the product surfaces appearing in the minimal Galois realization 24 which normalizes the G-action.

In the notation introduced previously, this means that σ is twisted G-equivariant. That is, there is an automorphism $\psi : G \to G$ with $\sigma(g(x, y)) = \psi(g)(\sigma(x, y))$ for all $g \in G$ and $(x, y) \in C(a_1, c_1) \times C(a_2, c_2)$. Up to replacing one of the two unmixed Beauville structures by an $\mathrm{Aut}(G)$ -equivalent one, we may asume without loss of generality that the map σ is strict G-equivariant.

Note that our surfaces are both isogenous to a higher product by Proposition 3.2. Since σ is of product type it can interchange the factors or not. If it does not, there are biholomorphic maps

$$\sigma_1 : C(a_1, c_1) \to C(a'_1, c'_1), \quad \sigma_2 : C(a_2, c_2) \to C(a'_2, c'_2)$$

such that $\sigma = (\sigma_1, \sigma_2)$. If σ does interchange the factors there are biholomorphic maps

$$\sigma_1 : C(a_1, c_1) \to C(a'_2, c'_2), \quad \sigma_2 : C(a_2, c_2) \to C(a'_1, c'_1)$$

such that $\sigma = (\sigma_1, \sigma_2)$. In both cases we may now use Proposition 2.2 which characterizes strict G-equivariant isomorphisms of triangle coverings. *Q.E.D.*

3.2. **Unmixed Beauville structures on finite groups.** The question arises: which groups admit Beauville structures?

The unmixed case with G abelian is easy to classify, and all examples were essentially given in [Cat00], page 24.

Theorem 3.4. *If $G = G^0$ is abelian, non-trivial and admits an unmixed Beauville structure, then $G \cong (\mathbb{Z}/n\mathbb{Z})^2$, where the integer n is relatively prime to 6. Moreover, the structure is critical for both factors. Conversely, any group $G \cong (\mathbb{Z}/n\mathbb{Z})^2$ admits such a structure.*

Proof. Let $(a,c;a',c')$ be an unmixed Beauville structure on G, set $\Sigma := \Sigma(a,c)$, $\Sigma' := \Sigma(a',c')$ and $b := a^{-1}c^{-1}$, $b' := a'^{-1}c'^{-1}$. Our basic strategy will be to observe that if H is a nontrivial characteristic subgroup of G, and if we show that for each choice of Σ we must have $\Sigma \supset H$, then we obtain a contradiction to $\Sigma \cap \Sigma' = \{1\}$.

Consider the primary decomposition of G,

$$G = \bigoplus_{p \in \{\text{Primes}\}} G_p$$

and observe that since G is 2-generated, then any G_p (which is a characteristic subgroup), is also 2-generated.

Step 1. Let $a = (a_p) \in \bigoplus_{p \in \{\text{Primes}\}} G_p$, and let Σ_p be the set of multiples of a_p, b_p, c_p: then $\Sigma \supset \Sigma_p$. This follows since a_p is a multiple of a.

Step 2. $G_p \cong (\mathbb{Z}/p^m\mathbb{Z})^2$.

Since G_p is 2-generated, otherwise G_p is either cyclic $G_p \cong \mathbb{Z}/p^m\mathbb{Z}$ or $G_p \cong \mathbb{Z}/p^n\mathbb{Z} \oplus \mathbb{Z}/p^m\mathbb{Z}$ with $n < m$. In both cases the subgroup $H_p := \mathrm{Soc}(G_p) := \{x \in G \,|\, px = 0\}$ is characteristic in G and isomorphic to $\mathbb{Z}/p\mathbb{Z}$. But $\Sigma \supset \Sigma_p$, and Σ_p contains generators of G_p, whence it contains a non-trivial element in the socle, thus $\Sigma_p \supset H_p := \mathrm{Soc}(G_p)$, a contradiction.

Step 3. $G_2 = 0$.

Else, by step 2, $G_2 \cong (\mathbb{Z}/2^m\mathbb{Z})^2$, and $H_2 := \mathrm{Soc}(G_2) \cong (\mathbb{Z}/2\mathbb{Z})^2$. But since $\Sigma \supset \Sigma_2$, and Σ_2 contains a basis of G_2, $\Sigma \supset H_2$, a contradiction.

Step 4. $G_3 = 0$.

In this case we have that Σ_3 contains a basis of G_3, whence $\Sigma \cap H_3$ contains at least 6 nonzero elements, likewise for $\Sigma' \cap H_3$, a contradiction since H_3 has only 8 nonzero elements.

Step 5. Whence, $G \cong (\mathbb{Z}/n\mathbb{Z})^2$, and since a, b are generators of G, they are a basis, and without loss of generality a, b are the standard basis e_1, e_2. It follows that all the elements a, b, c, a', b', c' have order exactly n. Write now the elements of G as row vectors, $a' := (x, y), b' := (z, t)$. Then the condition that $\Sigma \cap \Sigma' = \{1\}$ means that any pair of the six vectors yield a basis of G. By using the primary decomposition, we can read out this condition on each primary component: thus it suffices to show that there are solutions in the case where $n = p^m$ is primary.

Step 6. We write up the conditions explicitly, namely, if $n = p^m$ and $U := \mathbb{Z}/n\mathbb{Z}^*$, we want

$$x, y, z, t \in U,\ x - y, x + z, z - t, y + t \in U, x + z - y - t \in U, xt - yz \in U.$$

Again, these conditions only bear on the residue class modulo p, thus we have p^{4m-4} times the number of solutions that we get for $n = p$.

Step 7. Simple counting yields at least $(p-1)(p-2)^2(p-4)$ solutions.

In this case we get $p-1$ times the number of solutions that we get for $x = 1$, and for each choice of $y \neq 0, 1$ $z \neq 0, -1$, $d \neq 0$ we set $t := yz + d :$ the other inequalities are then satisfied if d is different from $z - yz, -yz - y, (1+z)(1-y)$ so that the number of solutions equals at least $(p-1)(p-2)^2(p-4)$. *Q.E.D.*

Remark 3.5. *The computation above shows that the number of biholomorphism classes of unmixed Beauville surfaces with abelian group* $(\mathbb{Z}/n\mathbb{Z})^2$ *is asymptotic to at least* $(1/36)\ n^4$ *(cf.* [Ba-Cat04] *where it is calculated that, for* $n = 5$ *there are exactly two isomorphism classes).*

Proposition 3.6. *No non-abelian group of order* ≤ 128 *admits an unmixed Beauville structure.*

Proof. This result can be obtained by a straightforward computation using the computer algebra system MAGMA or by direct considerations. In fact using the Smallgroups-routine of MAGMA we may list all groups of order ≤ 128 as explicit permutation-groups or given by a polycyclic presentation. Loops which are easily designed can be used to search for appropriate systems of generators. *Q.E.D.*

Another simple result is:

Lemma 3.7. *Let* G *be a non-trivial finite quotient of the infinite dihedral group* $D{:=}\langle x, y \mid x^2, y^2\rangle$ *then* G *does not admit an unmixed Beauville structure.*

Proof. The infinite cyclic subgroup $N_0 := \langle xy\rangle$ is normal in D of index 2, actually D is thus the semidirect product of $N_0 \cong \mathbb{Z}$ through the subgroup of order 2 generated by x. Let $t \in D$ be not contained in N_0. Then there is an integer n such that $t = x(xy)^n$. Since $yty = x(xy)^{n-2}$, the normal subgroup generated by t then contains $(xy)^2$. Hence every normal subgroup N of D not contained in N_0 has index ≤ 4 and thus the quotient D/N cannot admit an unmixed Beauville structure. Let now $N \leq N_0$ be a normal subgroup of D. The quotient D/N is a finite dihedral group. Let (a, c) be a pair of generators for D/N. It is easy to see that one of the elements a, c, ac lies in the (cyclic) image of N_0 in D/N and generates it. Thus condition (*) is contradicted. *Q.E.D.*

Proposition 3.8. *The following groups admit an unmixed Beauville structure:*

1. the alternating groups $\mathcal{A}_n$ *for large* n*,*

2. the symmetric groups $\mathcal{S}_n$ *for* $n \in \mathbb{N}$ *with* $n \geq 8$ *and* $n \equiv 2 \bmod 3$*,*

3. the groups $\mathbf{SL}(2, \mathbb{F}_p)$ *and* $\mathbf{PSL}(2, \mathbb{F}_p)$ *for every prime* p *distinct from* $2, 3, 5$.

Proof. 1. Fix two triples (n_1, n_2, n_3), $(m_1, m_2, m_3) \in \mathbb{N}^3$ such that neither $T(n_1, n_2, n_3)$ nor $T(m_1, m_2, m_3)$ is one of the non-hyperbolic triangle groups. From [Ev] we infer that, for large enough $n \in \mathbb{N}$, the group $\mathcal{A}_n$ has systems of generators (a_1, c_1) of type (n_1, n_2, n_3) and (a_2, c_2) of type (m_1, m_2, m_3). Adding the additional property that $\gcd(n_1n_2n_3, m_1m_2m_3) = 1$ we find that $(a_1, c_1; a_2, c_2)$ is an unmixed Beauville structure on $\mathcal{A}_n$.

By going through the proofs of [Ev] the minimal choice of such an $n \in \mathbb{N}$ can be made effective.

2. This follows directly from the first Proposition of Section 5.1.

3. Let p be a prime with the property that no prime $q \geq 5$ divides $p^2 - 1$. Then $(p, 1)$ is a primitive solution of an equation

$$y^2 - x^3 = \pm 2^n 3^m \tag{25}$$

with $n, m \in \mathbb{N}$ chosen appropriately. It is known that the collection of these equations has 98 primitive solutions (as n, m vary). A table of them is contained in [BK] Table 4, page 125. From this we see that $p = 2, 3, 5, 7, 17$ are the only primes with the property that no prime $q \geq 5$ divides $p^2 - 1$. Notice that a theorem of C.L. Siegel implies directly that there are only finitely many such primes. A special case of this theorem says that any of the equation (25) has only finitely many solutions in $\mathbb{Z}[1/2, 1/3]$.

If p is a prime with $p \neq 2, 3, 5, 7, 17$ we use the system of generators from (42) which is of type $(4, 6, p)$ together with one of the system of generators from (44) or (46) to conclude the result for $\mathbf{SL}(2, \mathbb{F}_p)$. The groups $\mathbf{PSL}(2, \mathbb{F}_p)$ can be treated by reduction of these systems of generators, observing that the two generators belonging to different systems have coprime orders.

For the primes $p = 7, 17$ appropriate systems of generators can be easily found by a computer calculation.

Q.E.D.

From the third item of the above proposition we immediately obtain a *proof of Theorem 1.3.*

Remark 3.9. *The various systems of generators given in Section 5 for the alternating groups $\mathcal{A}_n$ and for $\mathbf{SL}(2, \mathbb{F}_p)$, $\mathbf{PSL}(2, \mathbb{F}_p)$ can be grouped together in many ways to construct unmixed Beauville structures on these groups. We in turn obtain Beauville surfaces of unmixed type for which the two curves appearing in the minimal Galois realization have different genus.*

We shall describe now some groups of a completely different nature admitting an unmixed Beauville structure. For $n \in \mathbb{N}$ define:

(26)
$$C[n] := \langle x, y \mid x^n = y^n = (xy)^n = (xy^{-1})^n = (xy^{-2})^n = (xy^{-1}xy^{-2})^n = 1 \rangle$$

Proposition 3.10. *Let $n \in \mathbb{N}$ be given with G.C.D.$(n, 6) = 1$. Let further $N \leq C[n]'$ be a normal subgroup of finite index where $C[n]'$ is the commutator subgroup of $C[n]$. Then $C[n]/N$ admits an unmixed Beauville structure.*

Proof. An unmixed Beauville structure for $C[n]/N$ is given by

$$(a_1, c_1; a_2, c_2) = (x, y; xy^{-1}, xy^{-2}).$$

In fact, let G^{ab} be the abelianization of G. Then Σ and Σ' map injectively into G^{ab}, and their images do not meet inside G^{ab}, as verified in [Cat00], lemma 3.21.

Q.E.D.

Amongst the quotients $C[n]/N$ ($N \leq C[n]'$) are all finite groups G of exponent n having $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ as abelianization. The Proposition can hence be used to construct finite p-groups ($p \geq 5$) admitting an unmixed Beauville structure.

3.3. **Questions of reality.** We shall also translate into group theoretic conditions the two questions concerning an unmixed Beauville surface mentioned in the introduction:

- Is S biholomorphic to the complex conjugate surface $\bar{S}$?
- Is S real, i.e. does there exist such a biholomorphism σ with the property that $\sigma^2 = \mathrm{Id}$?

Let G be a finite group and $v = (a_1, c_1; a_2, c_2) \in \mathbb{U}(G)$. In analogy with (20) we define

$$\iota(v) := (a_1^{-1}, c_1^{-1}; a_2^{-1}, c_2^{-1}) \tag{27}$$

and infer from Proposition 2.3:

$$S(\iota(v)) = \overline{S(v)}. \tag{28}$$

From Proposition 3.3 we get

Proposition 3.11. *Let G be a finite group with an unmixed Beauville structure $v = (a_1, c_1; a_2, c_2) \in \mathbb{U}(G)$. Then*

1. $S(v)$ biholomorphic to $\overline{S(v)}$ if and only if $\iota(v)$ is in the $\mathrm{A}_{\mathbb{U}}(G)$ orbit of v,

2. $S(v)$ is real if and only if there is a $\rho \in \mathrm{A}_{\mathbb{U}}(G)$ with $\rho(v) = \iota(v)$ and moreover $\rho(\iota(v)) = v$.

Remark 3.12. *The above observations immediately imply that unmixed Beauville surfaces S with abelian group G always have a real structure, since $g \to -g$ is an automorphism (of order 2).*

We observe the following:

Corollary 3.13. *Let G be a finite group with an unmixed Beauville structure $v = (a_1, c_1; a_2, c_2) \in \mathbb{U}(G)$. Assume that the sets $\{\mathrm{ord}(a_1), \mathrm{ord}(c_1), \mathrm{ord}(a_1c_1)\}$ and $\{\mathrm{ord}(a_2), \mathrm{ord}(c_2), \mathrm{ord}(a_2c_2)\}$ are distinct. Assume further that both (a_1, c_1) and (a_2, c_2) are strict. Then $S(v)$ is biholomorphically isomorphic to $\overline{S(v)}$ if and only if the following holds:*

There are inner automorphisms ϕ_1, ϕ_2 of G and an automorphism $\psi \in Aut(G)$ such that, setting $\psi_j := \psi \circ \phi_j$, we have $\psi_1(a_1) = a_1^{-1}$, $\psi_1(c_1) = c_1^{-1}$, and $\psi_2(a_2) = {a_2}^{-1}$, $\psi_2(c_2) = {c_2}^{-1}$.

In particular $S(v)$ is isomorphic to $\overline{S(v)}$ if and only if $S(v)$ has a real structure.

Proof. The first statement follows from our Definition of $\mathrm{A}_{\mathbb{U}}(G)$ and Proposition 3.3. In fact let $\rho \in \mathrm{A}_{\mathbb{U}}(G)$ be such that $\rho(v) = \iota(v)$. We have

$$\rho = (\psi_1 \circ \sigma_i, \psi_2 \circ \sigma_j) \circ \tau^e$$

with ψ_1, ψ_2 as above, $i, j \in \{0, \ldots, 5\}$ and $e \in \{0, 1\}$. Our incompatibility conditions on the orders imply that $e = 0$ and $i = j = 0$ (see Lemma 2.4).

For the second statement note that the conclusion implies that both ψ_1 and ψ_2 have order 2. *Q.E.D.*

Remark 3.14. *If the unmixed Beauville structure v does not have the strong incompatibility properties of the corollary then lemma 2.4 gives the appropriate conditions.*

From our Corollary we immediately get:

Proof of Theorem 1.2. Let $v := (a, c; a', c')$ with $a, c, a', c' \in \mathcal{S}_n$ as in Proposition 5.1. Then v is an unmixed Beauville structure on $\mathcal{S}_n$. The type of (a, c) is $(6, 3(n-3), 3(n-4))$, while the type of (a', c') is $(n, n-1, n)$ or $(n, n-1, (n^2-1)/4)$. Suppose that $S(v)$ is biholomorphic to $\overline{S(v)}$. By Proposition 3.11 (statement 1) $\iota(v)$ is in the $\mathrm{A}_{\mathbb{U}}(\mathcal{S}_n)$ orbit of $S(v)$. The incompatibility of the types of (a, c) and (a', c') makes Corollary 3.13 applicable. This implies that there is a $\psi \in \mathrm{Aut}(\mathcal{S}_n)$ with $\psi(a) = a^{-1}$ and $\psi(c) = c^{-1}$. Since all automorphisms on $\mathcal{S}_n$ $(n \geq 8)$ are inner we obtain a contradiction to Proposition 5.1. *Q.E.D.*

As noted above the unmixed Beauville surfaces S coming from an abelian group G always have a real structure. It is also possible to construct examples from non-abelian groups:

Proposition 3.15. *Let $p \geq 5$ be a prime with $p \equiv 1$ mod 4. Set $n := 3p + 1$. Then there is an unmixed Beauville structure v for the group $\mathcal{A}_n$ such that $S(v)$ is biholomorphic to $\overline{S(v)}$.*

Proof. We use the first and the second system of generators for $\mathcal{A}_n$ from Proposition 5.9. The first is a system of generators (a_1, c_1) of type $(2, 3, 84)$, the second gives (a_2, c_2) of type $(p, 5p, 2p+3)$. Since the orders in the two types are coprime $(a_1, c_1; a_2, c_2)$ is an unmixed Beauville structure on $\mathcal{A}_n$. The existence of the respective elements γ in Proposition 5.9 implies the last assertion. Note that both the elements γ can be chosen to be in $\mathcal{S}_n \setminus \mathcal{A}_n$. *Q.E.D.*

In the further arguments we shall often use the fact that every automorphism of $\mathcal{A}_n$ ($n \neq 6$) is induced by conjugation by an element of $\mathcal{S}_n$ (see [S], page 299).

Proposition 3.16. *The following groups admit unmixed Beauville structures v such that $S(v)$ is not biholomorpically isomorphic to $\overline{S(v)}$:*

1. the symmetric group $\mathcal{S}_n$ for $n \geq 8$ and $n \equiv 2$ mod 3,

2. the alternating group $\mathcal{A}_n$ for $n \geq 16$ and $n \equiv 0$ mod 4, $n \equiv 1$ mod 3, $n \not\equiv 3, 4$ mod 7.

Proof. 1. This is just the example of Section 5.1.

2. We use the system of generators (a_1, c_1) from Proposition 5.9, 1. It has type $(2, 3, 84)$. We then choose $p = 5$ and $q = 11$ and get from Proposition 5.8 a system of generators (a_2, c_2) of type $(11, 5(n-11), n-3)$. Both systems are strict. We set $v := (a_1, c_1; a_2, c_2)$. The congruence conditions $n \not\equiv 3, 4$ mod 7 insure that $\nu(a_1, , c_1)$ is coprime to $\nu(a_2, , c_2)$, hence this is an unmixed Beauville structure. It also satisfies the hypotheses of Corollary 3.13. If $S(v)$ is biholomorpically isomorphic to $\overline{S(v)}$ we obtain an element $\gamma \in \mathcal{S}_n$ with $\gamma a_2 \gamma^{-1} = a_2^{-1}$ and $\gamma c_2 \gamma^{-1} = c_2^{-1}$. This contradicts Proposition 5.8. *Q.E.D.*

Proposition 3.17. *Let $p > 5$ be a prime with $p \equiv 1$ mod 4, $p \not\equiv 2, 4$ mod 5, $p \not\equiv 5$ mod 13 and $p \not\equiv 4$ mod 11. Set $n := 3p + 1$. Then the alternating group $G := \mathcal{A}_n$ admits an unmixed Beauville structure v such that there is an element $\alpha \in \mathrm{A}_{\mathbb{U}}(G)$ with $\alpha(v) = \iota(v)$ but such that there is no element $\beta \in \mathrm{A}_{\mathbb{U}}(G)$ with $\beta(v) = \iota(v)$ and $\beta(\iota(v)) = v$.*

Proof. In order to construct v we use the system of generators (a_1, c_1) from Proposition 5.10. It has type $(3p-2, 3p-1, 3p-1)$. We then use the system of generators (a_2, c_2) from Proposition 5.9, 2. It has type $(p, 5p, 2p+3)$. The second system is strict. We set $v := (a_1, c_1; a_2, c_2)$. The congruence conditions $p \not\equiv 2, 4 \bmod 5$, $p \not\equiv 5 \bmod 13$ and $p \not\equiv 4 \bmod 11$ ensure that $\nu(a_1, , c_1)$ is coprime to $\nu(a_2, , c_2)$, hence v is an unmixed Beauville structure.

We shall first show that there exists $\alpha \in \mathrm{A}_{\mathbb{U}}(\mathcal{A}_n)$ with $\alpha(v) = \iota(v) = (a_1^{-1}, c_1^{-1}; a_2^{-1}, c_2^{-1})$. We choose γ_1 as in Proposition 5.10 and γ_2 as in Proposition 5.9, 2. Let $w \in \mathcal{S}_n$ be a representative of the nontrivial coset of $\mathcal{A}_n$ in $\mathcal{S}_n$. By Propositions 5.10, 5.9 these choices can be made so that $\gamma_1 = \delta_1 w$, $\gamma_2 = \delta_2 w$ with $\delta_1, \delta_2 \in \mathcal{A}_n$. We have now

$$(w^{-1}\delta_1^{-1}\ a_1\ \delta_1 w, w^{-1}\delta_1^{-1}\ c_1^{-1}a_1^{-1}\ \delta_1 w) = (a_1^{-1}, c_1^{-1}), \tag{29}$$

$$(w^{-1}\delta_2^{-1}\ a_2\ \delta_2 w, w^{-1}\delta_2^{-1}\ c_2\ \delta_2 w) = (a_2^{-1}, c_2^{-1}). \tag{30}$$

Recalling the formula for σ_5 (see (11)) the existence of ρ follows from our definition of $\mathrm{A}_{\mathbb{U}}(\mathcal{A}_n)$.

Suppose now that there is a $\beta \in \mathrm{A}_{\mathbb{U}}(G)$ as indicated, then $\beta^2(v) = v$. By construction of v the transformation β cannot interchange (a_1, c_1) and (a_2, c_2). Hence we find $\beta_1, \beta_2 \in \mathrm{A}_{\mathbb{T}}(\mathcal{A}_n)$ with

$$\beta_1(a_1, c_1) = (a_1^{-1}, c_1^{-1}), \quad \beta_1(a_2, c_2) = (a_2^{-1}, c_2^{-1}).$$

from $\beta_1^2(a_1, c_1) = (a_1, c_1)$ and the formulae given immediately after Lemma 2.4 we infer that either $\beta_1 = \psi \circ \sigma_0$ or $\beta_1 = \psi \circ \sigma_3$ for a suitable automorphism ψ of $\mathcal{A}_n$. (Note that a_1 and c_1 cannot commute.) Going back to Lemma 2.4 (i), (iv) we find a contradiction against the statement of Proposition 5.10.*Q.E.D.*

Theorem 1.6 follows immediately from the above Proposition and from Proposition 3.11.

4. The mixed case

In this section we will first fix the algebraic data that are needed for the construction of Beauville surfaces of mixed type. Later on we will use this description to give several examples.

4.1. **Mixed Beauville surfaces and group actions.** This subsection contains the translation between the geometrical data of a mixed Beauville surface and the corresponding algebraic data: finite groups endowed with a mixed Beauville structure. This concept is contained in the following:

Definition 4.1. *Let G be a non-trivial finite group. A mixed Beauville quadruple for G is a quadruple $M = (G^0; a, c; g)$ consisting of a subgroup G^0 of index 2 in G, of elements $a, c \in G^0$ and of an element $g \in G$ such that*

1. *G^0 is generated by a, c,*
2. *$g \notin G^0$,*
3. *for every $\gamma \in G^0$ we have $g\gamma g\gamma \notin \Sigma(a, c)$,*
4. *$\Sigma(a, c) \cap \Sigma(gag^{-1}, gcg^{-1}) = \{1_G\}$.*

From a mixed Beauville quadruple we obtain, by forgetting about the choice of g, a mixed Beauville triple for G, $u = (G^0; a, c)$. The group G is said to admit a mixed Beauville structure if such a quadruple M exists. We let then $\mathbb{M}_4(G)$ be the set of mixed Beauville quadruples on the group G, $\mathbb{M}_3(G)$ be the set of mixed Beauville triples on the group G. These last will also be called mixed Beauville structures.

We shall describe now the correspondence between the data for an unmixed Beauville structure given above and those given in [Cat00] (also described in the introduction). Let $M = (G^0; a, c; g)$ be a mixed Beauville quadruple on a finite group G. Then G^0 is normal in G. By condition (3) the exact sequence

$$1 \to G^0 \to G \to \mathbb{Z}/2\mathbb{Z} \to 1, \tag{31}$$

does not split. Define $\varphi_g : G^0 \to G^0$ to be the automorphism of G^0 induced by conjugation with g, that is $\varphi_g(\gamma) = g\gamma g^{-1}$ for all $\gamma \in G^0$. Suppose φ_g would be an inner automorphism. Then we could find $\delta \in G^0$ with $\varphi_g(\gamma) = \delta\gamma\delta^{-1}$ for all $\gamma \in G^0$. This implies that $\Sigma(gag^{-1}, gcg^{-1}) = \Sigma(a, c)$. Since G is nontrivial condition (4) cannot hold.

Let $\tau := \tau_g := g^2 \in G^0$. We have $\varphi_g(\tau) = \tau$ and $\varphi_g^2 = \mathrm{Int}_\tau$ where Int_τ is the inner automorphism induced by τ. This shows that φ_g is of order 2 in the group of outer automorphisms $\mathrm{Out}(G^0)$ of G^0. Conversely given a non-trivial finite group G^0 together with an an automorphism $\varphi : G^0 \to G^0$ of order 2 in the outer automorphism group allows us to find a group G together with an exact sequence (31).

It is important to observe that the conditions (3), (4) are the ones which guarantee the freeness of the action of G.

We shall describe now the appropriate notion of equivalence for mixed Beauville structures. Let $M = (G^0; a, c; g)$ be a mixed Beauville quadruple for the group G and $\psi : G \to G$ be an automorphism of G: then $\psi(M) := (\psi(G^0); \psi(a), \psi(c); \psi(g))$ is again a mixed Beauville structure on G. Thus we obtain respective actions of $\mathrm{Aut}(G)$ on $\mathbb{M}_4(G)$, $\mathbb{M}_3(G)$. If $M = (G^0; a, c; g)$ is a mixed Beauville quadruple for the group G and $\gamma \in G^0$ then $M_\gamma = (G^0; a, c; \gamma g)$ is also a mixed Beauville quadruple on G.

We can therefore, without loss of generality, only consider mixed Beauville triples (beware, such a triple is obtained from a quadruple satisfying conditions (1)-(4) of the previous definition).

We consider on the set $\mathbb{M}(G) := \mathbb{M}_3(G)$ of mixed Beauville structures the action of the group

$$\mathrm{A}_{\mathbb{M}}(G) :=< \mathrm{Aut}(G),\ \sigma_3, \sigma_4 > . \tag{32}$$

with the understanding that the operations σ_3, σ_4 from (10), (11) are applied to the pair (a, c) of generators of G^0. Note that the operations $\sigma_1, \sigma_2, \sigma_5$ are also in $\mathrm{A}_{\mathbb{M}}(G)$ because of (13).

We will recall now how the above algebraic data give rise to a Beauville surface of mixed type. Let $u := (G^0; a, c; g)$ be a mixed Beauville quadruple on G. Set $\tau_g := g^2$ and $\varphi_g(\gamma) := g\gamma g^{-1}$ for $\gamma \in G^0$. By Riemann's existence theorem as in the previous section the elements a, $b = a^{-1}c^{-1}$, c give rise to a Galois covering $\lambda : C(a, c) \to \mathbb{P}^1_{\mathbb{C}}$ ramified only in $\{-1, 0, 1\}$ with ramification indices equal to the respective orders of a, $b = a^{-1}c^{-1}$, c and with group G^0. We let the group G act on $C(a,c) \times C(a,c)$ by letting

$$\gamma(x,y) = (\gamma x, \varphi_g(\gamma)y), \quad g(x,y) = (y, \tau_g x), \tag{33}$$

for all $\gamma \in G^0$ and $(x,y) \in C(a,c) \times C(a,c)$. These formulae determine an action of G uniquely. By our conditions (3), (4) in the definition of a mixed Beauville quadruple on G the above action of G is fixed point free, yielding a Beauville surface of mixed type

$$S(u) := C(a,c) \times C(a,c)/G. \tag{34}$$

It is obvious that (34) is a *minimal Galois representation* (see [Cat00], [Cat03]) of $S(u)$. From Proposition 3.2 we infer that the mixed Beauville surface $S(u)$ is isogenous to a *higher product* in the terminology of [Cat03].

Observe that a Beauville surface of mixed type $S(u) = C(a,c) \times C(a,c)/G$ has a natural unramified double cover $S^0(u) = (C(a,c) \times C(a,c))/G^0$ which is of unmixed type.

Proposition 4.2. *Let G be a finite group and $u_1, u_2 \in \mathbb{M}(G)$. Then $S(u_1)$ is biholomorphic to $S(u_2)$ if and only if u_1 is in the $\mathrm{A}_{\mathbb{M}}(G)$-orbit of u_2.*

Proof. This Proposition follows (as Proposition 3.3) from [Cat00], [Cat03] (Proposition 3.2).

Let $M = (G_1^0, a_1, c_1; g_1)$, $M' = (G_2^0; a_2, c_2; g_2)$. Assume that the two unmixed Beauville surfaces $S(u)$ and $S(u')$ are biholomorphically isomorphic. This happens, by Proposition 3.2 of [Cat03], if and only if there is a product biholomorphism (up to an interchange of the factors)

$$\sigma : C(a_1, c_1) \times C(a_1, c_1) \to C(a_2, c_2) \times C(a_2, c_2)$$

of the product surfaces. Since σ is of product type it can interchange the factors or not. Hence there are biholomorphic maps

$$\sigma_1, \sigma_2 : C(a_1, c_1) \to C(a_2, c_2)$$

with

$$\sigma(x,y) = (\sigma_1(x), \sigma_2(y)) \qquad \text{for all } x, y \in C(a_1, c_1)$$

in case σ does not interchange the factors and

$$\sigma(x,y) = (\sigma_1(y), \sigma_2(x)) \qquad \text{for all } x, y \in C(a_1, c_1)$$

in case σ does interchange the factors. The map σ normalises the G action if there is an automorphism $\psi : G \to G$ with $\sigma(g(x,y)) = \psi(g)(\sigma(x,y))$ for all $g \in G$ and $(x,y) \in C(a_1, c_1) \times C(a_1, c_1)$.

In both cases we may now use Proposition 2.2 together with some straightforward computations to complete the only if statement of our Proposition.

The reverse statement follows from Proposition 2.2 together with the apropriate considerations. *Q.E.D.*

4.2. **Mixed Beauville structures on finite groups.** To find a group G with a mixed Beauville structure is rather difficult, for instance the subgroup G^0 cannot be abelian:

Theorem 4.3. *If a group G admits a mixed Beauville structure, then the subgroup G^0 is non abelian.*

Proof. By theorem 3.4 we know that G^0 is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$, where n is an odd number not divisible by 3.

In particular, multiplication by 2 is an isomorphism of G^0, thus there is a unique element γ such that $-2\gamma = \tau$. Since $-2\varphi(\gamma) = \varphi(\tau) = \tau = -2\gamma$, it follows that $\varphi(\gamma) = \gamma$, and we have found a solution to the prohibited equation $\varphi(\gamma) + \tau + \gamma \in \Sigma$, since $0 \in \Sigma$. Whence the desired contradiction. *Q.E.D.*

We also report the following fact obtained by computer calculations using MAGMA.

Proposition 4.4. *No group of order* ≤ 512 *admits a mixed Beauville structure.*

We shall describe now a general construction which gives finite groups G with a mixed Beauville structure. Let H be non-trivial group. Let $\Theta : H \times H \to H \times H$ be the automorphism defined by $\Theta(g,h) := (h,g)$ $(g, h \in H)$. We consider the semidirect product

$$H_{[4]} := (H \times H) \rtimes \mathbb{Z}/4\mathbb{Z} \tag{35}$$

where the generator 1 of $\mathbb{Z}/4\mathbb{Z}$ acts through Θ on $H \times H$. Since Θ^2 is the identity we find

$$H_{[2]} := H \times H \times 2\mathbb{Z}/4\mathbb{Z} \cong H \times H \times \mathbb{Z}/2\mathbb{Z} \tag{36}$$

as a subgroup of index 2 in $H_{[4]}$.

Notice that the exact sequence

$$1 \to H_{[2]} \to H_{[4]} \to \mathbb{Z}/2\mathbb{Z} \to 1,$$

does not split because there is no element of order 2 in $H_{[4]}$ which is not already contained in $H_{[2]}$.

We have

Lemma 4.5. *Let H be a non-trivial group and let a_1, c_1, a_2, c_2 be elements of H. Assume that*

1. *the orders of a_1, c_1 are even,*
2. *a_1^2, a_1c_1, c_1^2 generate H,*
3. *a_2, c_2 also generate H,*
4. *$\nu(a_1, c_1)$ is coprime to $\nu(a_2, c_2)$.*

Set $G := H_{[4]}$, $G^0 := H_{[2]}$ as above and $a := (a_1, a_2, 2)$, $c := (c_1, c_2, 2)$. Then $(G^0; a, c)$ is a mixed Beauville structure on G.

If G is a perfect group then the conclusion holds with hypothesis 2 replaced by the following hypothesis

2'. a_1, c_1 generate H.

Proof. We first show that a, c generate $G^0 := H_{[2]}$. Let $L := \langle a, c\rangle$. We view $H \times H$ as the subgroup $H \times H \times \{0\}$ of $H_{[2]}$. The elements a^2, ac, c^2 are in this subgroup. Condition 2 implies that $L \cap (H \times H)$ projects surjectively onto the first factor of $H \times H$. From conditions 1,3, 4 we infer that a_2, c_2 have odd order, and that there is an even number $2m$ such that a_2^{2m}, c_2^{2m} generate H, while $a_1^{2m} = c_1^{2m} = 1$. It follows that $H \times H \leq L$, and it is then obvious that $L = G^0$.

Observe next that

$$(1_H, 1_H, 2) \notin \Sigma(a, c). \tag{37}$$

It would have to be conjugate of a power of a , c or b. Since the orders of a_1, b_1, c_1 are even, we obtain a contradiction. Note in fact that the third component of ac is 0 by construction.

We shall now verify the third condition of our definition of a mixed Beauville structure. Suppose preliminarly that $h = (x, y, z) \in \Sigma(a, c)$ satisfies $\mathrm{ord}(x) = \mathrm{ord}(y)$: then our condition 4 implies that $x = y = 1_H$ and (37) shows $h = 1_{H_{[4]}}$.

Let now $g \in H_{[4]}$, $g \notin H_{[2]}$ and $\gamma \in G^0 = H_{[2]}$ be given. Then $g\gamma = (x, y, \pm 1)$ for appropriate $x, y \in H$. We find

$$(g\gamma)^2 = (xy, yx, 2)$$

and the orders of the first two components of $(g\gamma)^2$ are the same. The remark above shows that $(g\gamma)^2 \in \Sigma(a, c)$ implies $(g\gamma)^2 = 1$.

We come now to the fourth condition of our definition of a mixed Beauville quadruple. Let $g \in H_{[4]}$, $g \notin H_{[2]}$ be given, for instance $(1_H, 1_H, 1)$. Conjugation with g interchanges then the first two components of an element $h \in H_{[4]}$. Our hypothesis 4 implies the result.

So far we have proved the lemma using hypothesis 2. Assume that H is a perfect group (this means that H is generated by commutators). Because of hypothesis 2' the group H is generated by commutators of words in a_1, c_1. Defining L as before we see again that that $L \cap (H \times H)$ projects surjectively onto the first factor of $H \times H$. The rest of the proof is the same.

Q.E.D.

As an application we get

Proposition 4.6. *Let H be one of the following groups:*

1. *the alternating group $\mathcal{A}_n$ for large n,*
2. $\mathbf{SL}(2, \mathbb{F}_p)$ *for $p \neq 2, 3, 5, 17$.*

Then $H_{[4]}$ admits a mixed Beauville structure.

Proof. 1. Fix two triples (n_1, n_2, n_3), $(m_1, m_2, m_3) \in \mathbb{N}^3$ such that neither $T(n_1, n_2, n_3)$ nor $T(m_1, m_2, m_3)$ is one of the non-hyperbolic triangle groups. From [Ev] we infer that, for large enough $n \in \mathbb{N}$, the group $\mathcal{A}_n$ has systems of generators (a_1, c_1) of type (n_1, n_2, n_3) and (a_2, c_2) of type (m_1, m_2, m_3). Adding the additional properties that n_1, n_2 are even and $\gcd(n_1n_2n_3, m_1m_2m_3) = 1$ we find that the $(a_1, c_1; a_2, c_2)$ satisfy the hypotheses 1,2',3,4 of the previous lemma. Since $\mathcal{A}_n$ is, for large n, a simple group the statement follows.

2. The primes $p = 2, 3, 5, 17$ are the only primes with the property that no prime $q \geq 5$ divides $p^2 - 1$. In the other cases we use the system of generators from 42 which is of type $(4, 6, p)$ together with one of the system of generators from 44 or 46 to obtain generators satisfying hypotheses 1,2',3,4 of the previous lemma. Since $\mathbf{SL}(2, \mathbb{F}_p)$ is a perfect group (for $p \neq 2, 3$) the statement follows.

Q.E.D.

4.3. **Questions of reality.** Let G be a finite group and $u = (G^0; a, c) \in \mathbb{M}(G) = \mathbb{M}_3(G)$. In analogy with 20 we define

$$\iota(u) := (G^0; a^{-1}, c^{-1}) \tag{38}$$

and infer from Proposition 2.3:

$$S(\iota(u)) = \overline{S(u)}. \tag{39}$$

From Proposition 3.3 we get

Proposition 4.7. *Let G be a finite group and $u \in \mathbb{M}(G)$ then*

1. $S(u)$ biholomorphic to $\overline{S(u)}$ if and only if $\iota(u)$ lies in the $\mathrm{A}_{\mathbb{M}}(G)$ orbit of u,

2. $S(u)$ real if and only if there exists $\rho \in \mathrm{A}_{\mathbb{M}}(G)$ with $\rho(u) = \iota(u)$ and $\rho(\iota(u)) = u$.

Observe that if a mixed Beauville surface S is isomorphic to its conjugate, then necessarily the same holds for its natural unmixed double cover S^0.

We will now formulate an algebraic condition on $u \in \mathbb{M}(G)$ which will allow us to show easily that the associated Beauville surface $S(u)$ is not isomorphic to $\overline{S(u)}$.

Corollary 4.8. *Let G be a finite group and $u = (G^0; a, c) \in \mathbb{M}(G)$ and assume that (a, c) is a strict system of generators for G^0. Then $S(u) \cong \overline{S(u)}$ if and only if there is an automorphism ψ of G such that $\psi(G^0) = G^0$ and $\psi(a) = a^{-1}$, $\psi(c) = c^{-1}$.*

Proof. This Corollary follows from Proposition 4.7 in the same way as Corollary 3.13 follows from Proposition 3.11.

Q.E.D.

We shall now give a alternative description of the conclusion of Corollary 4.8.

Remark 4.9. *With the assumptions of Corollary 4.8 let $g \in G$ represent the nontrivial coset of G^0 in G. Set $\tau := \tau_g = g^2$ and $\varphi := \varphi_g$. Then $S(u) \cong \overline{S(u)}$ if and only if there is an automorphism β of G^0 such that $\beta(a) = a^{-1}$, $\beta(c) = c^{-1}$, and an element $\gamma \in G^0$ such that $\tau(\beta(\tau^{-1})) = \varphi(\gamma)\gamma$.*

Proof. $S \cong \bar{S}$ if and only if $C_1 \times C_2$ admits an antiholomorphism σ which normalizes the action of G. Since there are biholomorphisms of $C_1 \times C_2$ which exchanges the factors (and lies in G), we may assume that such an antiholomorphism does not exchange the two factors. Being of product type $\sigma = \sigma_1 \times \sigma_2$, it must normalize the product group $G^0 \times G^0$. We get thus a pair of automorphisms β_1, β_2 of G. Since $\beta_1 \times \beta_2$ leaves the subgroup

$\{(\gamma, \varphi(\gamma)) \mid \gamma \in G\}$ invariant , it follows that $\beta_2 = \varphi\beta_1\varphi^{-1}$, and in particular β_2 carries $a' := \varphi(a), c' := \varphi(c)$ to their respective inverses.

Now, $\sigma_1 \times \sigma_2$ normalizes the whole subgroup G if and only if for each $\epsilon \in G^0$ there is $\delta \in G^0$ such that

$$\sigma_1\, \varphi(\epsilon)\sigma_2^{-1} = \varphi(\delta)\sigma_2(\tau\epsilon)\sigma_1^{-1} = \tau\delta.$$

We use now the strictness of the structure: this ensures that both σ_i's are liftings of the standard complex conjugation, whence we easily conclude that there is an element $\gamma \in G^0$ such that $\sigma_2 = \gamma\sigma_1$.

From the second equation we conclude that $\delta = \tau^{-1}\gamma\sigma_1\tau\epsilon\sigma_1^{-1}$, and the first boils then down to $\sigma_1(\varphi(\epsilon))\sigma_1^{-1}\gamma^{-1} = \tau^{-1}(\varphi(\gamma))\gamma\sigma_1\tau(\varphi(\epsilon))\sigma_1^{-1}\gamma^{-1}$.

Since this must hold for all $\epsilon \in G^0$, it is equivalent to require $\sigma_1\tau^{-1}\sigma_1^{-1} = \tau^{-1}(\varphi(\gamma))\gamma$, i.e., $\tau(\beta(\tau^{-1})) = (\varphi(\gamma))\gamma$.

Q.E.D.

We shall now give examples of mixed Beauville structures. In the proofs we shall use that every automorhism of $\mathbf{SL}(2, \mathbb{F}_p)$ (p a prime) is induced by an inner automorphism of the larger group

$$\mathbf{SL}^{\pm 1}(2, \mathbb{F}_p) := \langle \mathbf{SL}(2, \mathbb{F}_p),\ W := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rangle. \tag{40}$$

See the appendix of [Di] for a proof of this fact. We also use the following lemma which is easy to prove.

Lemma 4.10. *1. Let H be a perfect group. Every automorhism $\psi : H_{[4]} \to H_{[4]}$ satisfies $\psi(H \times H \times \{0\}) = H \times H \times \{0\})$.*

2. If H is non-abelian simple finite group, then every automorhism of $H \times H$ is of product type.

3. Let H be $\mathbf{SL}(2, \mathbb{F}_p)$, where p is prime: then every automorhism of $H \times H$ is of product type.

Proof. 1.: $H \times H \times \{0\}$ is the commutator subgroup.

2.: the centralizer $C((x, y))$ of an element (x, y) where $x \neq 1, y \neq 1$ does not map surjectively onto H through either of the two product projections, whence every automorphism leaves invariant the unordered pair of subgroups $\{(H \times \{0\}), (\{0\}) \times H)\}$.

3. follows by the same argument used for 2.

Q.E.D.

We shall apply the above constructions to obtain some concrete examples.

Proposition 4.11. *Let p be a prime with $p \equiv 3$ mod 4 and $p \equiv 1$ mod 5 and consider the group $H := \mathbf{SL}(2, \mathbb{F}_p)$. Then $H_{[4]}$ admits a mixed Beauville structure u such that $\iota(u)$ does not lie in the $\mathrm{A}_{\mathbb{M}}(H_{[4]})$ orbit of u.*

Proof. Set $a_1 := B$, $c_1 := S$ as defined in (42) and a_2, c_2 one of the systems of generators constructed in Proposition 5.13. That is the equations

$$\gamma a_2 \gamma^{-1} = a_2^{-1}, \quad \gamma c_2 \gamma^{-1} = c_2^{-1}$$

are solvable with $\gamma \in \mathbf{SL}(2,\mathbb{F}_p)$ but not with $\gamma \in \mathbf{SL}(2,\mathbb{F}_p)W$. Set $a := (a_1, a_2, 2)$, $c := (c_1, c_2, 2)$. By Lemma 4.5 the triple $u := (H_{[2]}, a, c)$ is a mixed Beauville structure on $H_{[4]}$. The type of (a, c) is $(20, 30, 5p)$, hence it is strict.

Suppose that $\iota(u)$ is in the $\mathrm{A}_{\mathbb{M}}(H_{[4]})$ orbit of u. By Corollary 4.8 we have an automorphism $\psi : H_{[4]} \to H_{[4]}$ with $\psi(H_{[2]}) = H_{[2]}$ with $\psi(a) = a^{-1}$ and $\psi(c) = c^{-1}$. From Lemma 4.10 we get two elements $\gamma_1, \gamma_2 \in \mathbf{SL}^{\pm 1}(2,\mathbb{F}_p)$ with

$$\gamma_1 a_1 \gamma_1^{-1} = a_1^{-1},\ \gamma_1 c_1 \gamma_1^{-1} = c_1^{-1},\ \gamma_2 a_2 \gamma_2^{-1} = a_2^{-1},\ \gamma_2 c_2 \gamma_2^{-1} = c_2^{-1}.$$

Since they come from the automorphism $\psi : H_{[4]} \to H_{[4]}$ they have to lie in the same coset of $\mathbf{SL}(2,\mathbb{F}_p)$ in $\mathbf{SL}^{\pm 1}(2,\mathbb{F}_p)$. This is impossible since $\gamma_1 a_1 \gamma_1^{-1} = a_1^{-1}$, $\gamma_1 c_1 \gamma^{-1} = c_1^{-1}$ is only solvable in the coset $\mathbf{SL}(2,\mathbb{F}_p)W$ as a computation shows. *Q.E.D.*

Proof of Theorem 1.5: We take the mixed Beauville structure from Proposition 4.11 and let S be the corresponding mixed Beauville surface as constructed in Section 4.1. *Q.E.D.*

5. Generating groups by two elements

5.1. **Symmetric groups.** In this section we provide a series of intermediate results which lead to the proof of the above Theorem 1.4. In fact we prove:

Proposition 5.1. *Let $n \in \mathbb{N}$ satisfy $n \geq 8$ and $n \equiv 2$ mod 3, then $\mathcal{S}_n$ has systems of generators (a, c), (a', c') with*

1. $\Sigma(a, c) \cap \Sigma(a', c') = \{1\}$,
2. *there is no $\gamma \in \mathcal{S}_n$ with $\gamma a \gamma^{-1} = a^{-1}$ and $\gamma c \gamma^{-1} = c^{-1}$.*

Lemma 5.2. *Let G be the symmetric group $\mathcal{S}_n$ in $n \geq 7$ letters, let $a := (5, 4, 1)(2, 6)$, $c := (1, 2, 3)(4, 5, 6. \dots, n)$. There is no automorphism of G carrying $a \to a^{-1}$, $c \to c^{-1}$.*

Proof. Since $n \neq 6$, every automorphism of G is an inner one. If there is a permutation g conjugating a to a^{-1}, c to c^{-1}, g would leave each of the sets $\{1, 2, 3\}$, $\{4, 5, \dots, n\}$, $\{1, 4, 5\}$, $\{2, 6\}$ invariant. By looking at their intersections we conclude that g leaves the elements $1, 2, 3, 6$ fixed and that the set $\{4, 5\}$ is invariant.

Since g leaves 1 fixed and conjugates a to a^{-1}, we see moreover that g transposes 4 and 5.

But then g conjugates c to $(1, 2, 3)(5, 4, 6, \dots, n)$ which is a different permutation than c^{-1}. *Q.E.D.*

Lemma 5.3. *The two elements $a := (5, 4, 1)(2, 6)$, $c := (1, 2, 3)(4, 5, 6, \dots, n)$ generate the symmetric group $\mathcal{S}_n$ if $n \geq 7$ and $n \neq 0$ mod 3.*

Proof. Let G be the subgroup generated by a, c. Then G is generated also by s, α, T, γ where $s := (2, 6)$, $\alpha := (5, 4, 1)$, $T := (1, 2, 3)$, $\gamma := (4, 5, 6, \dots n)$,since these elements are powers of a, c and 3 and $n - 3$ are relatively prime.

Since G contains a transposition, it suffices to show that it is doubly transitive.

The transitivity of G being obvious, since the supports of the cyclic permutations s, α, T, γ have the whole set $\{1, 2, \dots n\}$ as union, let us consider the subgroup $H \subset G$ which stabilizes $\{3\}$. H contains s, α, γ and again these are cyclic permutations such that their supports have as union the set $\{1, 2, 4, 5 \dots n\}$. Thus G is doubly transitive, whence $G = \mathcal{S}_n$. *Q.E.D.*

Remark 5.4.
- *Since* 3 *does not divide* n*, it follows that* $\mathrm{ord}(c) = 3(n-3)$*, while* $\mathrm{ord}(a) = 6$.
- *We calculate now* $\mathrm{ord}(b)$*, recalling that* $abc = 1$*, whence* b *is the inverse of* ca*. Since* $ca = (1, 6, 3)(4, 2, 7, \dots n)$ *we have* $\mathrm{ord}(b) = \mathrm{lcm}(3, n-4)$.
- *Recalling that* $a' := \sigma^{-1}$*,* $c' := \tau\sigma^2$*, where* $\tau := (1, 2)$ *and* $\sigma := (1, 2, \dots, n)$*, it follows immediately that* a', c' *generate the whole symmetric group.*
- *We have* $\mathrm{ord}(b') = \mathrm{ord}(c'a') = \mathrm{ord}(\tau\sigma) = \mathrm{ord}((2, 3, \dots n)) = n-1$, $\mathrm{ord}(a') = \mathrm{ord}(\sigma) = n$.
- *If* n *is even,* $n = 2m$*, then* $c' = (1, 2)(1, 3, 5, \dots 2m-1)(2, 4, 6, \dots 2m)$ *is the cyclical permutation* $c' = (2, 4, \dots, 2m, 1, 3, \dots, 2m-1)$ *and* $\mathrm{ord}(c') = n$.
- *If* n *is odd,* $n = 2m+1$*, then* $c' = (1, 2)(1, 3, 5, \dots 2m+1, 2, 4, 6, \dots 2m)(1, 3, 5, \dots 2m+1)(2, 4, 6, \dots 2m)$ *and thus* $\mathrm{ord}(c') = m(m+1)$.

Proposition 5.5. *Let* $a, b, c,\ a', b', c'$ *be as above then*

$$\Sigma(a, c) \cap \Sigma(a', c') = \{1\}.$$

Proof. We say that a permutation has type $(d_1 \leq \dots \leq d_k)$, with $d_i \geq 2\ \forall\ i$, if its cycle decomposition consists of k cycles of respective lengths $d_1, \dots d_k$. We say that the type is monochromatic if all the d_i's are equal, and dichromatic if the number of distinct d_i's is exactly two. Two permutations are conjugate to each other iff their types are the same. We say that a type $(p_1 \leq \dots \leq p_r)$ is derived from $(d_1 \leq \dots \leq d_k)$ if it is the type of a power of a permutation of type $(d_1 \leq \dots \leq d_k)$.

Therefore we observe that the types of $\Sigma(a, c)$ are those derived from $(2, 3)$, $(3, n-3)$, $(3, n-4)$, while those of $\Sigma(a', c')$ are those derived from $(n), (n-1)$ for n even, and also from $(m, m+1)$ in case where $n = 2m+1$ is odd.

We use then the following lemma whose proof is straightforward

Lemma 5.6. *Let* g *be a permutation of type* (d_1, d_2).
Then the type of g^h *is the reshuffle of* h_1*-times* d_1/h_1 *and* h_2*-times* d_2/h_2*, where* $h_i := \gcd(d_i, h)$*. Here, reshuffling means throwing away all the numbers equal to* 1 *and arranging the others in increasing order.*

In particular, if the type of g^h *is dichromatic,* (d_1, d_2) *are automatically determined. If moreover* d_1*,* d_2 *are relatively prime and the type of* g^h *is monochromatic, then it is derived from type* d_1 *or from type* d_2.

For the types in $\Sigma(a', c')$, we get types derived from (n), $(n-1)$, or $(\frac{1}{2}(n-1), \frac{1}{2}(n+1))$. The latter come from relatively prime numbers, whence they can never equal a type in $\Sigma(a, c)$, derived from the pairs $(2, 3)$, $(3, n-4)$ and $(3, n-3$. The monochromatic types in $\Sigma(a, c)$ can only be derived by (3), (2), $(n-4)$, $(n-3)$, since we are assuming that 3 does neither divide n nor $n-1$.

Q.E.D.

5.2. **Alternating groups.** In this section we shall construct certain systems of generators of the alternating groups $\mathcal{A}_n$ ($n \in \mathbb{N}$). Our principal tool is the theorem of Jordan, see [Wie]. This result says that $\langle a, c\rangle = \mathcal{A}_n$ for any pair $a, c \in \mathcal{A}_n$ which satifies

- the group $H := \langle a, c\rangle$ acts primitively on $\{1, \dots, n\}$,
- the group H contains a q-cycle for a prime $q \leq n - 3$.

A further result that we shall need is:

Lemma 5.7. *For $n \in \mathbb{N}$ with $n \geq 12$ let $U \leq \mathcal{A}_n$ be a doubly transitive group. If U contains a double-transposition then $U = \mathcal{A}_n$.*

Proof. The degree $m(\sigma)$ of a permutation $\sigma \in \mathcal{A}_n$ is the number of elements moved by σ. Let $\sigma \in U$ be a double-transposition. We have $m(\sigma) = 4$. Let m now be the minimal degree taken over all non-trivial elements of U. Since U is also primitive we may apply a result of de Séguier (see [Wie], page 43) which says that if $m > 3$ (in our situation we would have m=4) then

$$n < \frac{m^2}{4}\log\frac{m}{2} + m\left(\log\frac{m}{2} + \frac{3}{2}\right). \tag{41}$$

For $m = 4$ the right-hand side of 41 is roughly 11.5. Our assumptions imply that $m = 3$. We then apply Jordan's theorem to reach the desired conclusion.

Q.E.D.

We shall start now to construct the systems of generators required for the constructions of Beauville surfaces. We treat permutations as maps which act from the left on the set of reference. We also use the notation $g^\gamma := \gamma g \gamma^{-1}$ for the conjugate of an element g.

Proposition 5.8. *Let $n \in \mathbb{N}$ be even with $n \geq 16$ and let $3 \leq p \leq q \leq n-3$ be primes with $n - q \not\equiv 0$ mod p. Then there is a system (a, c) of generators for $\mathcal{A}_n$ of type $(q, p(n-q), n-p+2)$ such that there is no $\gamma \in \mathcal{S}_n$ with $\gamma a \gamma^{-1} = a^{-1}$ and $\gamma c \gamma^{-1} = c^{-1}$.*

Proof. Set $k := n - q$ and define

$$a := (1, 2, \dots, q),\ c := (q + 1, q + 2, \dots, q + k - 1, 1)(q + k, p, p - 1, \dots, 2).$$

We compute

$$ca = (1, q + k, p, p + 1, \dots, q + k - 1)$$

and the statement about the type is clear. We show that there is no $\gamma \in \mathcal{S}_n$ with the above properties. Otherwise, γ would leave invariant the three sets corresponding to the non trivial orbits of a, respectively c, and in particular we would have $\gamma(1) = 1$, $\gamma(\{2, \dots, p\}) = \{2, \dots, p\}$. But then $\gamma(2) \neq q$, a contradiction. We set $U := \langle a, c\rangle$ and show that $U = \mathcal{A}_n$.

Obviously U is transitive. The stabiliser V of $q+k$ in U contains the elements a, c^p. It is clear that the subgroup generated by these two elements is transitive on $\{1, \dots, n\} \setminus \{q + k\}$, hence U is doubly transitive. The group U contains the q-cycle a, whence we infer by Jordan's theorem that $U = \mathcal{A}_n$. *Q.E.D.*

For the applications in the previous sections we need:

Proposition 5.9. *1. Let $n \in \mathbb{N}$ satisfy $n \geq 16$ with $n \equiv 0 \mod 4$ and $n \equiv 1 \mod 3$. There is a pair (a, c) of generators of $\mathcal{A}_n$ of type $(2, 3, 84)$ and an element $\gamma \in \mathcal{S}_n \setminus \mathcal{A}_n$ with $\gamma a \gamma^{-1} = a^{-1}$ and $\gamma c \gamma^{-1} = c^{-1}$.*

2. Let p be a prime with $p > 5$. Set $n := 3p + 1$. There is a pair (a, c) of generators of $\mathcal{A}_n$ of type $(p, 5p, 2p + 3)$ and $\gamma \in \mathcal{S}_n$ with $\gamma a \gamma^{-1} = a^{-1}$ and $\gamma c \gamma^{-1} = c^{-1}$. If $p \equiv 1$ mod 4 then γ can be chosen in $\mathcal{S}_n \setminus \mathcal{A}_n$, if $p \equiv 3$ mod 4 then γ can be chosen in $\mathcal{A}_n$.

Proof. 1. We take as set of reference $\{0, \ldots, n - 1\}$ instead of $\{1, \ldots, n\}$ and set

$$\gamma := (0)(1) \prod_{i=1}^{\frac{n-4}{6}} (6i - 2, 6i + 1) \cdot (2, 3) \cdot \prod_{i=1}^{\frac{n-4}{6}} (6i - 1, 6i + 3)(6i, 6i + 2),$$

$$a := (0, 1) \cdot \prod_{i=1}^{\frac{n-4}{6}} (6i-2, 6i+1) \cdot \prod_{i=1}^{\frac{n-4}{6}} (6i-4, 6i-1) \cdot \prod_{i=1}^{\frac{n-4}{6}} (6i-4, 6i-1)^{\gamma} \cdot (n-2, n-4),$$

$$c := (0) \prod_{i=1}^{\frac{n-1}{3}} (3i - 2, 3i - 1, 3i).$$

Observe that

$$\prod_{i=1}^{\frac{n-4}{6}} (6i - 4, 6i - 1)^{\gamma} = \prod_{i=2}^{\frac{n-4}{6}} (6i - 6, 6i + 3) \cdot (3, 9).$$

We have now

$$ca = (0, 2, 6, 13, 11, 9, 1) \cdot (3, 7, 5) \cdot \prod_{i=1}^{\frac{n-16}{6}} (6i-2, 6i+2, 6i+6, 6i+13, 6i+11, 6i+9)$$
$$\cdot (n - 1, n - 12, n - 8, n - 4) \cdot (n - 2, n - 6)$$

We have $\mathrm{ord}(a) = 2$, $\mathrm{ord}(c) = 3$, $\mathrm{ord}(ca) = 84$ and $\gamma a \gamma^{-1} = a^{-1}$ and $\gamma c \gamma^{-1} = c^{-1}$. To apply the theorem of Jordan we note that $(ca)^{12}$ is a 7-cycle. It remains to show that $H := \langle a, c \rangle$ acts primitively. In figure 1 we exhibit the orbits of a and c. In the right hand picture we connect two elements of $\{0, \ldots, n - 1\}$ if they are in the orbit of a, in the left hand picture similarly for c.

Figure 1 makes it obvious that H acts transitively. Since $(ca)^{12}$ is a 7-cycle, the second condition of Jordan's theorem is fullfilled. Let H_0 be the stabiliser of 0. Then c and $(ca)^7$ are contained in H_0. In Figure 2 we show the orbits of the two elements c and $(ca)^7$. The notation is the same as in Figure 1. A glance at Figure 2 shows that H_0 is transitive on $\{1, \ldots, n - 1\}$. We infer that H is doubly transitive. Again by Theorem 9.6 of [Wie] the group H is primitive.

2. Again we take as set of reference $\{0, \ldots, n-1\}$ instead of $\{1, \ldots, n\}$ and set

$$\gamma := (0)(1)(p + 1, 2p + 1) \cdot \prod_{i=1}^{\frac{p-1}{2}} (1 + i, p + 1 - i) \cdot \prod_{i=1}^{p-1} (p + 1 + i, 3p + 1 - i),$$

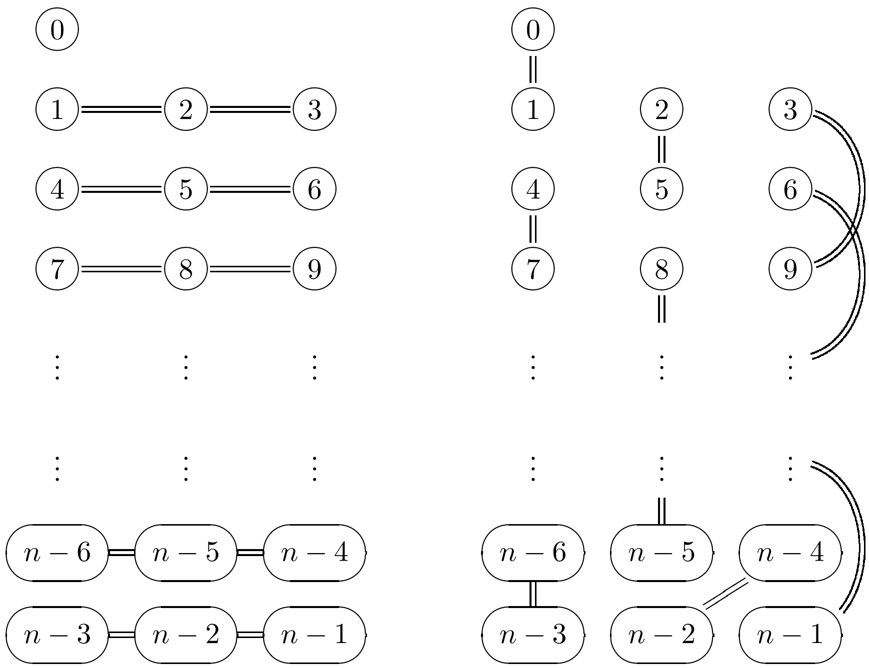


FIGURE 1. The orbits of c, a

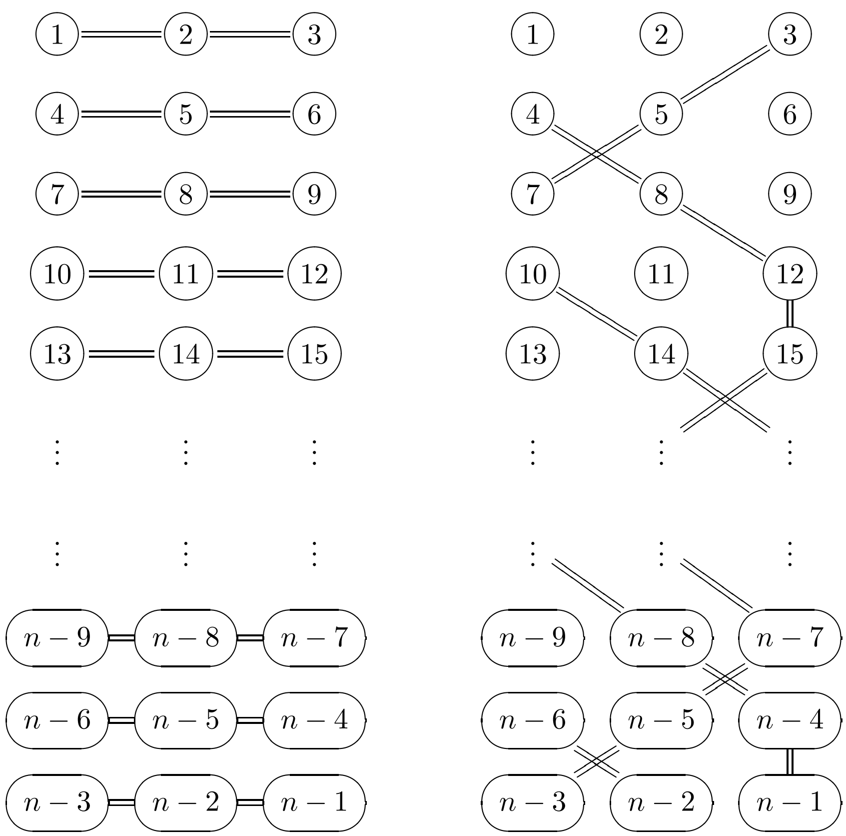


FIGURE 2. The orbits of c and $(ca)^7$

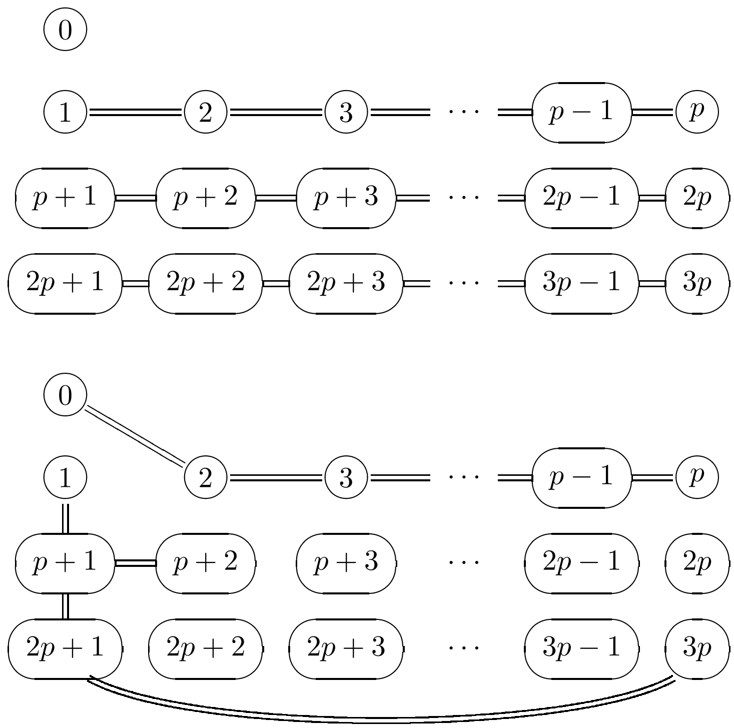


FIGURE 3. The orbits of a und c

$$a := (0)(1, 2, \ldots, p)(p + 1, p + 2, \ldots, 2p)(2p + 1, 2p + 2, \ldots, 3p),$$
$$c := (0, p, p - 1, p - 2, \ldots, 3, 2)(1, p + 1, 3p, p + 2, 2p + 1).$$

We have

$$ca := (2)(3) \ldots (p-1)(0, p, p+1, 2p+1, 2p+2, \ldots, 3p-1, p+2, p+3, \ldots 2p, 3p, 1).$$

From this definition we see that $\mathrm{ord}(a) = p$, $\mathrm{ord}(c) = 5p$ and $\mathrm{ord}(ca) = 2p+3$. The formulae $\gamma a \gamma^{-1} = a^{-1}$ and $\gamma c \gamma^{-1} = c^{-1}$ are also clear.

We verify the conditions of Jordan's theorem. First of all c^5 is a p-cycle. It remains to show that $H := \langle a, c \rangle$ acts primitively. In Figure 3, above, we exhibit the orbits of a, respectively the orbits of c below. From this it is obvious that H acts transitively.

Let now $\Delta_1 \cup \Delta_2 \cup \ldots \cup \Delta_k = \{0, 1, \ldots, 3p\}$ be a block-decomposition for H with $0 \in \Delta_1$. Note that the natural number k satisfies $|\Delta_i|k = 3p+1$ for all i. Since a is in the stabiliser of 0 we have $|\Delta_1| \in \{1, p+1, 2p+1, 3p+1\}$. Since $|\Delta_1|$ divides $3p+1$, we infer that H acts primitively. *Q.E.D.*

Further systems of generators are needed:

Proposition 5.10. *Let $n = 2k$ be an even natural number with $n \geq 16$. Then there is a system of generators (a, c) of $\mathcal{A}_n$ of type $(2k-3, 2k-2, 2k-2)$ and $\gamma \in \mathcal{S}_n$ such that*

$$\gamma a \gamma^{-1} = a^{-1}, \quad \gamma c \gamma^{-1} = ac.$$

If k is even then γ can be chosen in $\mathcal{S}_n \setminus \mathcal{A}_n$, if k is odd then γ can be chosen in $\mathcal{A}_n$. The system of generators (a, c) has the further property that there is no $\delta \in \mathcal{S}_n$ with

$$\delta a \delta^{-1} = a^{-1} \text{ and } \delta c \delta^{-1} = c^{-1} \quad \text{or} \quad \delta a \delta^{-1} = c^{-1} \text{ and } \delta c \delta^{-1} = a^{-1}.$$

Proof. We set

$$a := (1, 2, \dots, 2k-4, 2k-3),$$

$$d := (1,2,3)(2k-3, 2k-4, 2k-5)(k-1, 2k-1)(2k-2, k-2, 2k, k)$$

and

$$\alpha := (1, 2k-3)(2, 2k-4)(3, 2k-5)\dots(k-2, k)\cdot(2k-2, 2k).$$

The following are clear:

- d^6 is a double-transposition,
- α is in $\mathcal{A}_n$ if k is odd, and in $\mathcal{S}_n \setminus \mathcal{A}_n$ if k is even,
- $\alpha a \alpha^{-1} = a^{-1}$ and $\alpha d \alpha^{-1} = d$,
- there is no $\delta \in \mathcal{S}_n$ with $\delta a \delta^{-1} = a$ and $\delta d \delta^{-1} = d^{-1}$.

For the last item note that a has $\{2k-2, 2k-1, 2k\}$ as its set of fixed points. A δ with the above property would have to stabilise this set. The element d interchanges $k-1$ and $2k-1$ hence both these elements have to be fixed by δ. The condition $\delta a \delta^{-1} = a$ implies then that δ acts as the identity on $\{1, 2, \dots, 2k-3\}$, in particular as the identity on the subset $\{1,2,3\}$, contradicting $\delta d \delta^{-1} = d^{-1}$. Set

$$c := da^{k-2} = (1, 2k-1, k-1, 2k-4, k-3, 2k-3, 2k, k,$$

$$2, 2k-2, k-2, 2k-5, k-4, 2k-6, k-5, 2k-7, \dots, 5, k+3, 4, k+2)(3, k+1).$$

Note that $\mathrm{ord}(c) = 2k-2$. We find

$$\alpha c \alpha^{-1} = \alpha d a^{k-2} \alpha^{-1} = d a^{-k+2} = c a^{-2k+4} = ca,$$

whence also $ord(ca) = 2k-2$. Set now $\gamma := a\alpha$, so that γ clearly satisfies the required properties.

Set $U := \langle a, c \rangle$. We shall now show that $U = \mathcal{A}_n$. Clearly, U is a transitive group. Let $V \leq U$ the stabiliser of $2k-1$. The subgroup V contains

$$a,\ d^2,\ da^{k-2}da^{4-k}d.$$

From the definitions it is clear that these elements generate a group which is transitive on $\{1, \dots, 2k\} \setminus \{2k-1\}$. Hence U is doubly transitive and contains a double transposition. From Lemma 5.7 we infer that $U = \mathcal{A}_n$.

The last property follows from the above items since in the first case we would have $a \to a^{-1}, d \to (Int_a)^{-(k-2)}(d^{-1})$, and composing with $Int_{\alpha \cdot a^{k-2}}$ we contradict the third item.

Whereas, in the second case, just observe that a and c have different order.

Q.E.D.

5.3. **SL(2) and PSL(2) over finite fields.** In this section we give systems of generators consisting of two elements of the respective groups $\mathbf{SL}(2, \mathbb{F}_p)$ and $\mathbf{PSL}(2, \mathbb{F}_p)$ which will allow us to construct certain Beauville structures on them.

If p is a prime we denote by $\mathbb{F}_p$, $\mathbb{F}_{p^2}$ the fields with p, respectively p^2 elements and by $\mathbb{F}_p^*$, $\mathbb{F}_{p^2}^*$ the corresponding multiplicative groups. We let

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p} : \mathbb{F}_{p^2}^* \to \mathbb{F}_p^*$$

be the norm map. We also introduce the matrices

$$B := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \; S := \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \; T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \; W := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{42}$$

in $\mathbf{GL}(2, \mathbb{F}_p)$. For $\lambda \in \mathbb{F}_p$ with $\lambda \neq 0$ and $k \in \mathbb{F}_p$ we define

$$D(\lambda) := \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \quad M(k) := \begin{pmatrix} 0 & 1 \\ -1 & k \end{pmatrix}.$$

We have

$$B^4 = S^6 = W^2 = 1, \; T = BS, \; WBW^{-1} = B^{-1}, \; WSW^{-1} = S^{-1}.$$

The matrices (B, S) form a system of generators of $\mathbf{SL}(2, \mathbb{F}_p)$ of type $(4, 6, p)$. Their images in $\mathbf{PSL}(2, \mathbb{F}_p)$ form a system of generators of type $(2, 3, p)$.

Proposition 5.11. *Let p be an odd prime and let $q \geq 5$ be a prime with $q|p-1$ and let $\lambda \in \mathbb{F}_p^*$ be of order q: then $\lambda + \lambda^{-1} - 2 \neq 0$, $\lambda^2 + \lambda^{-2} - 2 \neq 0$ and $\lambda + \lambda^{-1} - \lambda^2 - \lambda^{-2} \neq 0$. Set*

$$g := \begin{pmatrix} 1 & b \\ 1 & d \end{pmatrix} \quad \text{with } b := \frac{\lambda + \lambda^{-1} - \lambda^2 - \lambda^{-2}}{\lambda^2 + \lambda^{-2} - 2}, \; d := \frac{\lambda + \lambda^{-1} - 2}{\lambda^2 + \lambda^{-2} - 2}. \tag{43}$$

Then

$$D(\lambda), \quad gD(\lambda)g^{-1} \tag{44}$$

form a system of generators of $\mathbf{SL}(2, \mathbb{F}_p)$ of type (q, q, q). Set further

$$e(\lambda) := \frac{2 - \lambda - \lambda^{-1}}{\lambda + \lambda^{-1} - \lambda^2 - \lambda^{-2}}. \tag{45}$$

There exists $\gamma \in \mathbf{SL}(2, \mathbb{F}_p)$ with $\gamma D(\lambda)\gamma^{-1} = D(\lambda)^{-1}$ and $\gamma g D(\lambda) g^{-1}\gamma^{-1} = gD(\lambda)^{-1}g^{-1}$ if and only if $e(\lambda)$ is a square in $\mathbb{F}_p$. There is $\gamma \in \mathbf{SL}(2, \mathbb{F}_p)W$ satisfying these conditions if and only if $-e(\lambda)$ is a square in $\mathbb{F}_p$.

Proof. Let us prove that $\lambda + \lambda^{-1} - 2 = 0$ leads to a contradiction. In fact, multiplying by λ we find $(\lambda - 1)^2 = 0$ which is impossible since λ has order q. The other two cases are treated similarly.

We see immediately that the determinant of g is equal to 1, furthermore an easy computation shows that the trace of $h := D(\lambda)gD(\lambda)g^{-1}$ is $\lambda + \lambda^{-1}$, hence h has also order q. Notice further that the subgroup H generated by $D(\lambda)$ and $gD(\lambda)g^{-1}$ cannot be solvable because these two elements have no common fixpoint in the action on $\mathbb{P}^1_{\mathbb{F}_p}$. From the list of isomorphism classes of subgroups of $\mathbf{PSL}(2, \mathbb{F}_p)$ given in [Hu] (Hauptsatz 8.27, page 213). we find that H has to be $\mathbf{SL}(2, \mathbb{F}_p)$ if $q \neq 5$. For $q = 5$ these simple arguments with subgroup orders leave the possibility that H be isomorphic to the binary icosahedral group $2 \cdot \mathcal{A}_5 \leq \mathbf{SL}(2, \mathbb{F}_p)$. But this group does not have a system of generators of type $(5, 5, 5)$, as it is easily seen by computer calculation.

The assertion about the simultaneous conjugacy of $D(\lambda)$, $D(\lambda)^{-1}$ and $gD(\lambda)g^{-1}$, $gD(\lambda)^{-1}g^{-1}$ follows by a straightforward computation. In fact we just take a matrix X with indeterminate entries and write down the 9 equations resulting from $XD(\lambda) = D(\lambda)^{-1}X$ and $XgD(\lambda)g^{-1} = gD(\lambda)^{-1}g^{-1}X$, $\mathrm{Det}(X) = \pm 1$ and the statement follows by a small manipulation of them.

Q.E.D.

Proposition 5.12. *Let p, q be odd primes such that $q \geq 5$ and $q|p+1$. Let $\lambda \in \mathbb{F}_{p^2}^*$ be of order q (thus $N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\lambda) = 1$). Consider its trace $k := \lambda + \lambda^{-1} \in \mathbb{F}_p$: then there exists $g \in \mathbf{SL}(2, \mathbb{F}_p)$ such that*

$$M(k), \quad gM(k)g^{-1} \tag{46}$$

form a system of generators of type (q, q, q).

Proof. Choose k as indicated and notice that $k \neq 1$, $k \neq 2$, as we already saw.

Let us now change our perspective and let $R := \mathbb{Z}[r, s, t]$ treating $r = k$ as a variable. Set

$$x := \begin{pmatrix} 0 & 1 \\ -1 & r \end{pmatrix}, \ g := \begin{pmatrix} 1 & s \\ t & 1+st \end{pmatrix}, \ y := gxg^{-1}, \ z := x \cdot y \in \mathbf{SL}(2, R).$$

The reduction into $\mathbf{SL}(2, \mathbb{F}_p)$ of x and of y have order q for any choice of s, t and $r = k$. We want $z = xy$ also to have order q. This happens if the trace of the reduction into $\mathbf{SL}(2, \mathbb{F}_p)$ of z is equal to k. This follows from $\mathrm{Tr}(z) = r$ which is equivalent to the equation

$$-s^2t^2 + s^2tr - s^2 - st^2r + str^2 - 2st - t^2 + r^2 - r - 2 = 0. \tag{47}$$

We write $C_{p,k}$ for the plane affine curve obtained from (47) by setting $r = k$ and reducing modulo p. Furthermore let $\mathbb{P}C_{p,k}$ be the projective closure of $C_{p,k}$ (with respect to s, t) and $\mathbb{P}C_{p,k}^\infty$ its set of points at infinity.

These are immediately seen to be the two points with $s = 0, t = 1$, respectively $t = 0, s = 1$, and in these two points at ∞ the curve has two ordinary double points.

By a computation using a Gröbner-routine over $\mathbb{Z}$ (possible in MAGMA or SINGULAR) one can also verify that the affine curve $C_{p,k}$ is smooth for every $p \geq 11$.

To check this fact we projectivise (47), compute derivatives and analise the ideal in R generated by these homogeneous polynomials. In this step we use $k \neq 1$, $k \neq 2$.

Let now $\tilde{C}_{p,k} \to \mathbb{P}C_{p,k}$ be a non-singular model of $\mathbb{P}C_{p,k}$. We conclude from the above analysis of the singularities of $\mathbb{P}C_{p,k}$ and from Bézout's theorem that the non-singular curve $\tilde{C}_{p,k}$ is absolutely irreducible and has genus 1. We may then apply the Hasse-Weil estimate (cf. e.g. the textbook [Har], V 1.10, page 368) to obtain:

$$||\tilde{C}_{p,k}(\mathbb{F}_p)| - p - 1| \leq 2\sqrt{p}$$

and since there are at most two $\mathbb{F}_p$-points over every singular point of $\mathbb{P}C_{p,k}$ we get at worst

$$||C_{p,k}(\mathbb{F}_p)| - p + 3| \leq 2\sqrt{p}.$$

Hence we have $C_{p,k}(\mathbb{F}_p) \neq \emptyset$ for $p \geq 11$.

Let now (s, t) be in $C_{p,k}(\mathbb{F}_p)$ and x, y, z the correspondinding matrices defined above. Notice that all 3 of them have order q. It can be checked, again by a Gröbner-routine over $\mathbb{Z}$ that we have $y \neq \pm x$ and $y \neq \pm x^{-1}$. Assume that $q > 5$. A glance at the sugroups of $\mathbf{PSL}(2, \mathbb{F}_p)$ ([Hu]) shows that the subgroup generated by x, y could only be cyclic which is impossible by the remarks just made. If $q = 5$ we conclude by observing again that $2 \cdot \mathcal{A}_5 \leq \mathbf{SL}(2, \mathbb{F}_p)$ does not have a system of generators of type $(5, 5, 5)$.

Q.E.D.

In order to use Proposition 5.11 effectively for our problems we would have to show that the invariant e from (45) takes both square and nonsquare values as λ varies over all elements of order q. This leads to a difficult problem about exponential sums which we could not resolve. In case $q = 5$ we found the following way to treat the problem by a simple trick.

Proposition 5.13. *Let p be a prime with $p \equiv 3$ mod 4 and $p \equiv 1$ mod 5. Then the group $\mathbf{SL}(2, \mathbb{F}_p)$ has a system of generators (a, c) of type $(5, 5, 5)$ such that the equations*

$$\gamma a \gamma^{-1} = a^{-1}, \quad \gamma c \gamma^{-1} = c^{-1} \tag{48}$$

are solvable with $\gamma \in \mathbf{SL}(2, \mathbb{F}_p)$ but not with $\gamma \in \mathbf{SL}(2, \mathbb{F}_p)W$. The same group has another system of generators (a, c) such that (48) is solvable in $\mathbf{SL}(2, \mathbb{F}_p)W$ but not in $\mathbf{SL}(2, \mathbb{F}_p)$.

Proof. Take $\lambda \in \mathbb{F}_p$ with $\lambda^5 = 1$, $\lambda \neq 1$ and consider the system of generators given in (44). Since $p \equiv 3$ mod 4 the number -1 is not a square in $\mathbb{F}_p$. Suppose that the invariant $e(\lambda)$ is a square in $\mathbb{F}_p$ whence(48) is solvable in $\mathbf{SL}(2, \mathbb{F}_p)$ and not in $\mathbf{SL}(2, \mathbb{F}_p)W$ (see Proposition 5.11). Then we are done. Suppose instead that the invariant $e(\lambda)$ is not a square in $\mathbb{F}_p$. We replace λ by λ^2 and find by a small computation that $e(\lambda) = -e(\lambda^2)$ up to squares. In this place we use $\lambda^5 = 1$,whence $(\lambda^2)^2 = \lambda^{-1}$ and the denominator simply changes sign as we replace λ by λ^2. Notice also that

$$2 - \lambda - \lambda^{-1} = -(\mu - \mu^{-1})^2 \qquad (\mu^2 = \lambda)$$

is never a square. We infer that $e(\lambda^2)$ is a square and proceed as before.

The second statement is proved similarly. *Q.E.D.*

5.4. **Other groups and more generators.** In this subsection we report on computer experiments related to the existence of unmixed or mixed Beauville structures on finite groups. We also try to formulate some conjectures concerning these questions.

We have paid special attention to unmixed Beauville structures on finite nonabelian simple groups.

The smallest of these groups is $\mathcal{A}_5 \cong \mathbf{PSL}(2, \mathbb{F}_5)$. This group cannot have an unmixed Beauville structure. On the one hand it has only elements of orders $1, 2, 3, 5$. It is not solvable hence it cannot be a quotient group of one of the euclidean triangle groups (see Section 6). This implies that any normalised system of generators has type $(n, m, 5)$ with $n, m \in \{2, 3, 5\}$. Finally we note that, by Sylow's theorem, all subgroups of order 5 are conjugate.

There are 47 finite simple nonabelian groups of order ≤ 50000. By computer calculations we have found unmixed Beauville structures on all of them with the exception of $\mathcal{A}_5$. This and the results of Section 3.2 leads us to:

Conjecture 1: *All finite simple nonabelian groups except $\mathcal{A}_5$ admit an unmixed Beauville structure.*

We have also checked this conjecture for some bigger simple groups like the Mathieu groups $\mathbf{M}12$, $\mathbf{M}22$ and also matrix groups of size bigger then 2. Furthermore we have proved:

Proposition 5.14. *Let p be an odd prime: then the Suzuki group $\mathbf{Suz}(2^p)$ has an unmixed Beauville structure.*

In the proof, which is not included here, we use in an essential way that the Suzuki groups $\mathbf{Suz}(2^p)$ are minimally simple, that is have only solvable proper subgroups. For the Suzuki groups see [HuB].

Let us call a type $(r, s, t) \in \mathbb{N}$ *hyperbolic* if

$$\frac{1}{r} + \frac{1}{s} + \frac{1}{t} < 1.$$

In this case the triangle group $T(r, s, t)$ is hyperbolic. From our studies also the following looks suggestive:

Conjecture 2: *Let (r, s, t), (r', s', t') be two hyperbolic types. Then almost all alternating groups $\mathcal{A}_n$ have an unmixed Beauville structure $v = (a_1, c_1; a_2, c_2)$ where (a_1, c_1) has type (r, s, t) and (a_2, c_2) has type (r', s', t').*

Let us call an unmixed Beauville structure $v = (a_1, c_1; a_2, c_2)$ on the finite group G *strongly real* if there are $\delta_1, \delta_2 \in G$ and $\psi \in \mathrm{Aut}(G)$ with

$$(\delta_1\psi(a_1)\delta_1^{-1}, \delta_1\psi(c_1)\delta_1^{-1}; \delta_2\psi(a_2)\delta_2^{-1}, \delta_2\psi(c_2)\delta_2^{-1}) = (a_1^{-1}, c_1^{-1}; a_2^{-1}, c_2^{-1}). \tag{49}$$

If the unmixed Beauville structure v is strongly real then the associated surface $S(v)$ is real.

There are 18 finite simple nonabelian groups of order ≤ 15000. By computer calculations we have found strongly unmixed Beauville structures on all of them with the exceptions of $\mathcal{A}_5$, $\mathbf{PSL}(2, \mathbb{F}_7)$, $\mathcal{A}_6$, $\mathcal{A}_7$, $\mathbf{PSL}(3, \mathbb{F}_3)$, $\mathbf{U}(3, 3)$ and the Mathieu group $\mathbf{M}11$. The alternating group $\mathcal{A}_8$ however has such a structure. This and the results of Section 3.3 leads us to:

Conjecture 3: *All but finitely many finite simple groups have a strongly real unmixed Beauville structure.*

Conjectures 1,2,3 are variations of a conjecture of Higman saying that every hyperbolic triangle group surjects onto almost all alternating groups. This conjecture was resolved positively in [Ev] where a related discussion can be found.

We were unable to find finite 2- or 3-groups having an unmixed Beauville structure. For $p \geq 5$ our construction (26) gives plenty of examples of p-groups having an unmixed Beauville structure.

Finally we report now on two general facts that we have found during our investigations. These are useful in the quest of finding Beauville structures on finte groups.

Using the methods used the proofs of Propositions 5.11, 5.12 the following can be proved:

Proposition 5.15. *Let p be an odd prime.*

1. Let $q_2 > q_1 \geq 5$ be primes with $q_1 q_2 | p-1$ and let $\lambda_1, \lambda_2 \in \mathbb{F}_p^*$ be of respective orders q_1 and q_2. Then there is an element $g \in \mathbf{SL}(2, \mathbb{F}_p)$ such that

$$D(\lambda_1), \quad gD(\lambda_2)g^{-1} \tag{50}$$

form a system of generators of type $(q_1, q_2, q_1 q_2)$.

2. Let $q_2 > q_1 \geq 5$ be primes with $q_1 q_2 | p+1$ and let $\lambda_{1,2} \in \mathbb{F}_{p^2}^*$ with $N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\lambda_{1,2}) = 1$ be of respective orders q_1 and q_2. Then their traces $k_{1,2} := \lambda_{1,2} + \lambda_{1,2}^{-1}$ are in $\mathbb{F}_p$ and there is an element $g \in \mathbf{SL}(2, \mathbb{F}_p)$ such that

$$M(k_1), \quad gM(k_2)g^{-1} \tag{51}$$

form a system of generators of type $(q_1, q_2, q_1 q_2)$.

Surfaces S which are not real but still are biholomorphic to their conjugate $\bar{S}$ are somewhat difficult to find. Our Theorem 1.6 gives examples using the alternating groups. We also have found:

Proposition 5.16. *Let p be an odd prime and assume that there is a prime $q \geq 7$ dividing $p+1$ such that q is not a square modulo p : then there is an unmixed Beauville surface S with group $G = \mathbf{SL}(2, \mathbb{F}_p)$ which is biholomorphic to the complex conjugate surface $\bar{S}$ but is not real.*

For the proof we turn the conditions into polynomial equations and polynomial inequalities (as in Propositions 5.11, 5.12) and then use arithmetic algebraic geometry over finite fields (in a more subtle way) as before. We do not include this here.

Remark 5.17. *First examples of primes p satisfying the conditions of Proposition 5.16 are $p = 13$ with $q = 7$, $p = 37$ with $q = 19$ and $p = 41$ with $q = 7$. Let p, q be odd primes. The law of quadratic reciprocity implies that the conditions of Proposition 5.16 are equivalent to $q \equiv 3$ mod 4, $p \equiv 1$ mod 4 and $p \equiv -1$ mod q. Dirichlet's theorem on primes in arithmetic progressions implies that there are infinitely many such pairs (p, q).*

6. The wall paper groups

In this section we analyse the finite quotients of the triangular groups

$$T(3,3,3), \qquad T(2,4,4), \qquad T(2,3,6).$$

and we will show that they do not admit any unmixed Beauville structure. We shall give two proofs of this fact, a "geometric" one, and the other in the taste of combinatorial group theory.

These are groups of motions of the euclidean plane, in fact in the classical classification they are the groups **p3**, **p4**, **p6**. Each of them contains a normal subgroup N isomorphic to $\mathbb{Z}^2$ with finite quotient.

In fact, let T be such a triangle group: then T admits a maximal surjective homomorphism onto a cyclic group C_d of order d. Here, d is respectively equal to $3, 4, 6$, and the three generators map to elements of C_d whose order equals their order in T.

It follows that the covering corresponding to T is the universal cover of the compact Riemann surface E corresponding to the surjection onto C_d, and one sees immediately two things:

1) E is an elliptic curve because $\mu(a, c) = 1$

2) E has multiplication by the group $\mu_d \cong \mathbb{Z}/d\mathbb{Z}$ of d-roots of unity.

Letting $\omega = exp(2/3\pi i)$, we see that

- $T(3, 3, 3)$ is the group of affine transformations of $\mathbb{C}$ of the form
$$g(z) = \omega^j z + \eta \text{ , for } j \in \mathbb{Z}/3\mathbb{Z}, \eta \in \Lambda_\omega := \mathbb{Z} \oplus \mathbb{Z}\omega$$
- $T(2, 4, 4)$ is the group of affine transformations of $\mathbb{C}$ of the form
$$g(z) = i^j z + \eta \text{ , for } j \in \mathbb{Z}/4\mathbb{Z}, \eta \in \Lambda_i := \mathbb{Z} \oplus \mathbb{Z}i$$
- $T(2, 3, 6)$ is the group of affine transformations of $\mathbb{C}$ of the form
$$g(z) = (-\omega)^j z + \eta \text{ , for } j \in \mathbb{Z}/6\mathbb{Z}, \eta \in \Lambda_\omega := \mathbb{Z} \oplus \mathbb{Z}\omega.$$

Remark 6.1. *Using the above affine representation, we see that N is the normal subgroup of translations, i.e. of the transformations which have no fixed point on $\mathbb{C}$.*

Moreover, if an element $g \in T - N$, then the linear part of g is in $\mu_d - \{1\}$, and g has a unique fixed point p_g in $\mathbb{C}$. An immediate calculation shows that indeed this fixed point p_g lies in the lattice Λ, and we obtain in this way that the conjugacy classes of elements $g \in T - N$ are exactly given by their linear parts, so they are in bijection with the elements of $\mu_d - \{1\}$.

Let now $G = T/M$ be a non trivial finite quotient group of T: then G admits a maximal surjective homomorphism onto a cyclic group C' of order d, where $d \in \{2, 3, 4, 6\}$. Assume that there is an element $g \in T - N$ which lies in the kernel of the composite homomorphism: then the whole conjugacy class of g is in the kernel. Since all transformations in the N - coset of g are in the conjugacy class, it follows that N is in the kernel and G is cyclic, whence isomorphic to C'.

In the case where C' is isomorphic to C, we get that G is a semidirect product $G = K \rtimes C$, where $K = N/N \cap M$, and the action of C on K is induced by the one of C on N. We have thus shown:

Proposition 6.2. *Let G be a non trivial finite quotient of a triangle group $T = T(3, 3, 3)$, or $T(2, 4, 4)$, or $T(2, 3, 6)$. Then there is a maximal surjective homomorphism of G onto a cyclic group C_d of order $d \leq 6$.*

If moreover G is not isomorphic to C, then $d = 3$ for $T(3, 3, 3)$, for $T(2, 4, 4)$ $d = 4$, $d = 6$ for $T(2, 3, 6)$, and G is a semidirect product $G = K \rtimes C$, where the action of C is induced by the one of C on N. In particular, let a_1, c_1 and a_2, c_2 by two systems of generators of G: then $|\Sigma(a_1, c_1) \cap \Sigma(a_2, c_2)| \neq \emptyset$.

Proof. Just observe that two elements which have the same image in $C - \{0\}$ belong to the same conjugacy class by our previous remarks. The rest follows rightaway. *Q.E.D.*

We give now an alternative proof by purely group theoretical arguments.

In case of $T(3,3,3)$ we have an isomorphism of finitely presented groups

$$\langle a,c \,|\, a^3, c^3, (ac)^3\rangle \cong \langle x,y,r \,|\, [x,y], r^3, rxr^{-1} = y, ryr^{-1} = x^{-1}y^{-1}\rangle$$

given by $x = ca^{-1}$, $y = cac$, $r = a$. We set $N_3 := \langle x, y\rangle$. The second presentation shows that $\Gamma(3,3,3)$ is isomorphic to the split extension of $N_3 \cong \mathbb{Z}^2$ by the cyclic group (of order 3) generated by r. We have

Proposition 6.3. *Let L be a normal subgroup of finite index in $T(3,3,3)$. If $L \neq T(3,3,3)$ then $L \leq N_3$ and $G := T(3,3,3)/L$ is isomorphic to the split extension of a finite abelian group N by a cyclic group of order 3. The only possible*

types for a two generator system of G are (up to permutation) $(3,3,3)$ and $(3,3,l)$ for some divisor l of $|N|$. Let a_1, c_1 and a_2, c_2 by two systems of generators of G then $|\Sigma(a_1,c_1) \cap \Sigma(a_2,c_2)| \geq 3$.

Proof. An obvious computation shows that the normal closure of any element $g = ur$ $(u \in N_3)$ contains N_3 and hence is equal to $T(3,3,3)$. This proves the first statement. Let now $L \leq N_3$ and let a_1, a_2 generate $G = T(3,3,3)/L$ then at least one of the cosets a_1, a_2 must contain an element of the form $g = ur^{\pm 1}$ $(u \in N_3)$. By rearrangement both cosets contain an element of this type. A computation shows that every element has order exactly 3 in $T(3,3,3)$. This shows he statement about the types. Let $g = ur^{\pm 1}$ be as above and let S be the union of the conjugates of the cyclic group generated by g in $\Gamma(3,3,3)$. It is clear that S contains either xr or r or both these elements. *Q.E.D.*

In case of $T(2,4,4)$ we have an isomorphism of finitely presented groups

$$\langle a,c \,|\, a^2, c^4, (ac)^4\rangle \cong \langle x,y,r \,|\, [x,y], r^4, rxr^{-1} = y, ryr^{-1} = y^{-1}\rangle$$

given by $x = ac^2$, $y = cac$, $r = c$. We set $N_4 := \langle x, y\rangle$. The second presentation shows that $\Gamma(2,4,4)$ is isomorphic to the split extension of $N_4 \cong \mathbb{Z}^2$ by the cyclic group (of order 4) generated by r. We have

Proposition 6.4. *Let L be a normal subgroup of finite index in $T(2,4,4)$. If the index of L in $T(2,4,4)$ is ≥ 16 then $L \leq N_4$ and $G := T(2,4,4)/L$ is isomorphic to the split extension of a finite abelian group N by a cyclic group of order 4. The only possible types for a two generator system of G are (up to permutation) $(2,4,4)$ and $(4,4,l)$ for some divisor l of $|N|$. Let a_1, c_1 and a_2, c_2 by two systems of generators of G then $|\Sigma(a_1,c_1) \cap \Sigma(a_2,c_2)| \geq 2$.*

The proof is analogous to the first Proposition of this section.

In case of $T(2,3,6)$ we have an isomorphism of finitely presented groups

$$\langle a,c \,|\, a^2, c^3, (ac)^6\rangle \cong \langle x,y,r \,|\, [x,y], r^6, rxr^{-1} = y^{-1}x, ryr^{-1} = x\rangle$$

given by $x = cac^{-1}a$, $y = c^{-1}aca$, $r = ac$. We set $N_6 := \langle x, y\rangle$. The second presentation shows that $\Gamma(2,3,6)$ is isomorphic to the split extension of $N_6 \cong \mathbb{Z}^2$ by the cyclic group (of order 6) generated by r. We have

Proposition 6.5. *Let L be a normal subgroup of finite index in $\Gamma(2,3,6)$. If the index of L in $T(2,3,6)$ is ≥ 24 then $L \leq N_6$ and $G := \Gamma(2,3,6)/L$ is isomorphic to the split extension of a finite abelian group N by a cyclic group of order 6. The only possible types for a two generator system of G are (up* *to permutation)* $(2,3,6)$ *and* $(6,6,l)$ *for some divisor* l *of* $|N|$*. Let* a_1, c_1 *and* a_2, c_2 *by two systems of generators of* G *then* $|\Sigma(a_1, c_1) \cap \Sigma(a_2, c_2)| \geq 2$*.*

Again the proof is analogous to the first Proposition of this section.

References

[Ba-Cat04] I. Bauer, F. Catanese, '*Some new surfaces with* $p_g = q = 0$, math.AG/0310150, to appear in the Proceedings of the Fano Conference (Torino 2002), U.M.I. FANO special Volume.

[BPV84] W. Barth, C. Peters and A. Van de Ven, "*Compact Complex Surfaces*", Ergebnisse der Mathematik und ihrer Grenzgebiete, Folge 3, B.4, Springer-Verlag, (1984), 304 pp..

[Bea] A. Beauville, "*Surfaces algébriques complexes*" Asterisque *54* Soc. Math. France (1978).

[BK] B.J. Birch, W. Kuyk, "*Modular Functions of One Variable IV*", Springer LNM **476**, Springer Verlag, Berlin-Heidelberg-New York, (1975)

[Cat00] F. Catanese, "*Fibred surfaces, varieties isogenous to a product and related moduli spaces.*", Amer. J. Math. 122 (2000), no.1, 1–44.

[Cat03] F. Catanese, "*Moduli Spaces of Surfaces and Real Structures*", Ann. Math. 158 (2003), no.2, 577-592.

[Cox] H.S.M. Coxeter, W.O.J. Moser, "*Generators and Relations for discrete Groups*", Ergebnisse der Mathematik **14**, Springer Verlag, Berlin-Heidelberg-New York (1965)

[Di] J. Dieudonné, "*On the automorphisms of the classical groups*", Memoirs of the American Math. Soc. **2**, (1949)

[Ev] B. Everitt, "*Alternating quotients of Fuchsien groups*", Journal of Algebra **223**, 457–476 (2000)

[Har] R. Hartshorne, "*Algebraic Geometry* ", Graduate Texts in Mathematics**52**, Springer Verlag, Berlin-Heidelberg-New York (1977)

[Hu] B. Huppert, "*Endliche Gruppen I*", Grundlehren der mathematischen Wissenschaften **134**, Springer Verlag, Berlin-Heidelberg-New York (1967)

[HuB] B. Huppert, N. Blackburn, "*Finite Groups III*", Grundlehren der mathematischen Wissenschaften **243**, Springer Verlag, Berlin-Heidelberg-New York (1982)

[K-K02] V. Kharlamov and V. Kulikov, "*On real structures of rigid surfaces ,* " Izv. Ross. Akad. Nauk Ser. Mat. 66 (2002), no. 1, 133–152.

[Mi] Miranda, R. "*Algebraic Curves and Riemann Surfaces*", Graduate Studies in Math., AMS (1995)

[S] M. Suzuki, "*Group Theory I*", Grundlehren der mathematischen Wissenschaften **247**, Springer Verlag, Berlin-Heidelberg-New York (1980)

[Wie] Wielandt, H. "*Finite Permutation Groups*", Academic Press (1964)

Authors' addresses:

Pr. D. Ingrid Bauer and Prof. Dr. Fabrizio Catanese
Lehrstuhl Mathematik VIII
Universität Bayreuth, NWII
D-95440 Bayreuth, Germany

e-mail:
Ingrid.Bauer@uni-bayreuth.de
Fabrizio.Catanese@uni-bayreuth.de

Prof. Dr. Fritz Grunewald
Mathematisches Institut der
Heinrich-Heine-Universität Düsseldorf

Universitätsstr. 1 D-40225 Düsseldorf, Germany
e-mail:
grunewald@math.uni-duesseldorf.de