Arbitrarily large Galois orbits of non-homeomorphic surfaces

Gabino González-Diez Gareth A. Jones
David Torres-Teigell

April 12, 2018

Abstract

We construct orbits of the absolute Galois group, of explicit unbounded size, consisting of surfaces with mutually non-isomorphic fundamental groups. These are Beauville surfaces with Beauville group $PGL_2(p)$.

2010 Mathematics Subject Classification: 14J25 (primary); 11R52, 14J29 and 20G40 (secondary).

1 Introduction

If X is a projective variety defined over the field $\overline{\mathbb{Q}}$ of algebraic numbers, then it is natural to ask which topological properties it shares with its Galois conjugates X^σ, obtained by applying elements σ of the absolute Galois group $\mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$ to the coefficients of the polynomials defining X. In dimension 1 the answer is straightforward: two Galois conjugate curves have the same genus, and are therefore homeomorphic, so they share all their topological properties; for this and other Galois invariants, in the context of Grothendieck's theory of *dessins d'enfants*, see [18].

More generally, by Hodge theory (see [16, 26] for instance) the dimensions of the cohomology groups $H^i(X,\mathbb{C})$ of a complex projective variety X can be expressed in terms of the Hodge numbers $h^{p,q}(X) = \dim H^q(X,\Omega^p)$, where Ω^p is the sheaf of holomorphic p-differential forms on X. By Serre's GAGA principle [20] these numbers $h^{p,q}$ are invariant under Galois conjugation. It follows that in dimension 2, for instance, many of the standard topological invariants of a complex projective surface X are also Galois invariants. These include

- the Betti numbers $b_i = \dim H_i(X)$,
- the Euler characteristic or Euler number $e = \sum_{i=0}^{4}(-1)^i b_i$,
- the irregularity $q = h^{0,1} = h^{1,0}$,

- the geometric genus $p_g = h^{0,2} = h^{2,0}$,
- the arithmetic genus $p_a = p_g - q$,
- the holomorphic Euler characteristic $\chi = p_g - q + 1$,
- the signature (of the second cohomology group) $\tau = 4\chi - e$, and
- the Chern numbers $c_2 = e$ and $c_1^2 = K^2 = 12\chi - e$.

(see e.g. [26, Th. 6.33]). Nevertheless, in 1964 Serre [21] constructed examples of Galois conjugate pairs of complex projective varieties, including surfaces, which have non-isomorphic fundamental groups, and are therefore not homeomorphic to each other. Since then, further examples of conjugate but non-homeomorphic varieties have been found: see [1, 2, 12, 9, 19, 5, 23, 13] for instance.

A Beauville surface is an example of a complex surface which is isogenous to a higher product, that is, it has the form $S = (C_1 \times C_2)/G$ where each C_i is a curve of genus $g_i > 1$, and G is a finite group acting freely on the product (see §2 for the full definition). Various rigidity properties of Beauville surfaces have been proved by Catanese [8] and by Bauer, Catanese and Grunewald [3, 4, 5], including the following (see [15, Theorem 4.1] for a proof by the first and third authors using uniformisation theory):

Proposition 1. *If $S = (C_1 \times C_2)/G$ and $S' = (C_1' \times C_2')/G'$ are Beauville surfaces with $\pi_1 S \cong \pi_1 S'$ then $G \cong G'$ and, possibly after transposing factors, each C_i is isomorphic to either C_i' or its complex conjugate curve $\overline{C_i'}$.* □

In particular, the conclusions of Proposition 1 apply if S and S' are homeomorphic to each other. Since Beauville surfaces are defined over $\overline{\mathbb{Q}}$, this result (or more precisely its contrapositive) suggests that these surfaces should provide further examples of non-homeomorphic Galois conjugate varieties. Indeed, for this purpose one can use any Beauville surface $S = (C_1 \times C_2)/G$ where $g_1 \neq g_2$ and there is some $\sigma \in \mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$ such that C_1^σ is not isomorphic to C_1 or $\overline{C}_1$.

In [25] Streit developed a method for determining the Galois orbits and fields of definition of certain curves with large automorphism groups, such as the Macbeath-Hurwitz curves. In [15], the first and third authors used generating triples for the groups $G = PSL_2(p)$, where p is prime, together with Streit's method, to construct arbitrarily large Galois orbits of mutually non-homeomorphic Beauville surfaces. Specifically, for any integer $n > 6$ dividing $(p \pm 1)/2$, they constructed an orbit of at least $\varphi(n)/2$ such surfaces, where φ is Euler's function. Now the most convenient necessary and sufficient condition for two pairs of triples in a group G to give isomorphic Beauville surfaces depends on a rather delicate relationship between the actions of inner and outer automorphisms of G. In this particular case, the existence of a non-trivial outer automorphism of $PSL_2(p)$ (induced by conjugation in $PGL_2(p)$) makes it difficult to determine the precise size of this orbit. Here we use a similar construction, based instead on the groups $G = PGL_2(p)$ which have no outer automorphisms, to give exact values for the (unbounded) sizes of certain Galois

orbits of mutually non-homeomorphic Beauville surfaces (see Theorem 2 in §6). As a particular case, we have following result:

Theorem 1. *For each prime $p \equiv 19$ mod (24), there is an orbit of* Gal $\overline{\mathbb{Q}}/\mathbb{Q}$ *consisting of $\varphi(m)/4$ Beauville surfaces with Beauville group $PGL_2(p)$, where $m = (p^2-1)/2$, and with mutually non-isomorphic fundamental groups.* □

Of course, the surfaces in each such orbit are mutually non-homeomorphic. By Dirichlet's Theorem, there are infinitely many primes $p \equiv 19$ mod (24). The corresponding orbit-lengths $\varphi(m)/4$ are unbounded above, since there are only finitely many integers m with a given value of $\varphi(m)$.

It is worth noting that the mutually non-isomorphic fundamental groups in Theorems 1 and 2 have isomorphic profinite completions (cf. Serre's examples in [21]). We recall that the profinite completion of a group Γ is the projective limit $\widehat{\Gamma} = \varprojlim \Gamma/\Gamma_i$, where Γ_i ranges over the finite index normal subgroups of Γ and the quotient groups are endowed with the obvious epimorphisms $\Gamma/\Gamma_i \to \Gamma/\Gamma_j$ whenever $\Gamma_i < \Gamma_j$. In the particular case in which $\Gamma = \pi_1 X$ is the fundamental group of a non-singular complex projective variety X, elementary covering space theory shows that, if $\widetilde{X}$ denotes the holomorphic universal cover of X, then Γ acts freely and properly discontinuously on $\widetilde{X}$, so that X can be viewed as $X = \widetilde{X}/\Gamma$ and its unramified finite Galois coverings as $X_i = \widetilde{X}/\Gamma_i$. Therefore $\widehat{\Gamma}$ can be seen as

$$\widehat{\Gamma} = \widehat{\pi_1 X} = \varprojlim \mathrm{Aut}(X_i/X),$$

where $X_i \to X$ ranges over the unramified finite Galois coverings of X by (necessarily) projective varieties X_i and the covering groups $\mathrm{Aut}(X_i/X)$ are understood to be related by the natural epimorphisms $\mathrm{Aut}(X_i/X) \to \mathrm{Aut}(X_j/X)$, whenever $X_i \to X$ factors through the coverings $X_i \to X_j$ and $X_j \to X$. Thus, for any Galois element σ one clearly has

$$\widehat{\pi_1 X} = \varprojlim \mathrm{Aut}(X_i/X) \cong \varprojlim \mathrm{Aut}(X_i^\sigma/X^\sigma) = \widehat{\pi_1 X^\sigma}$$

In §2 and §3 we summarise some background information on Beauville surfaces and the groups $G = PGL_2(p)$. In §4 and §5 we define and enumerate two different types of generating triples for G, which are used in §6 to construct Beauville surfaces. In §7 we determine the Galois orbits on these surfaces. This section includes a more general theorem of the above type, along with some further applications and open problems.

Acknowledgement The second author is grateful to the Departamento de Matemáticas, Universidad Autónoma de Madrid, for financially supporting a visit during which much of this research was carried out.

The first and third authors are partially supported by the grant MTM2009-11848 of the MICINN.

Finally, the first two authors are grateful to the ICMS of Edinburgh, where they first began working on Beauville surfaces.

2 Beauville surfaces and Beauville structures

Beauville surfaces were introduced by Catanese in [8] following an example of Beauville in [6], and their properties have subsequently been investigated by himself, Bauer and Grunewald [3, 4, 5]. A *Beauville surface* (of unmixed type) is a compact complex surface S such that

(a) S is isogenous to a higher product, that is, $S \cong (C_1 \times C_2)/G$ where C_1 and C_2 are projective curves of genus at least 2 and G is a finite group acting freely by holomorphic transformations on $C_1 \times C_2$;

(b) G acts faithfully on each C_i so that C_i/G is isomorphic to the projective line $\mathbb{P}^1(\mathbb{C})$ and the covering $C_i \to C_i/G$ is ramified over three points.

A rational function $C_i \to \mathbb{P}^1(\mathbb{C})$ ramified over at most three points is known as a Belyĭ function. By Belyĭ's Theorem [7], the existence of such a function is equivalent to C_i being defined over $\overline{\mathbb{Q}}$. When, as in condition (b), a Belyĭ function is a regular covering, C_i is called a *quasiplatonic curve*.

A group G arises in the above way if and only if it has generating triples (a_i, b_i, c_i) for $i = 1, 2$, of orders (l_i, m_i, n_i), such that

(1) $a_i b_i c_i = 1$ for each $i = 1, 2$,

(2) $l_i^{-1} + m_i^{-1} + n_i^{-1} < 1$ for each $i = 1, 2$, and

(3) no non-identity power of a_1, b_1 or c_1 is conjugate in G to a power of a_2, b_2 or c_2.

Such a pair of triples (a_i, b_i, c_i) is called a *Beauville structure* on G, of bitype $(l_1, m_1, n_1; l_2, m_2, n_2)$. Property (1) is equivalent to condition (b), with a_i, b_i and c_i representing the local monodromies over the three ramification points. Property (2) is equivalent to each C_i having genus at least 2, arising as a smooth quotient $\mathbb{H}/M_i$ of the hyperbolic plane $\mathbb{H}$, where M_i is the kernel of the natural epimorphism ρ_i from the triangle group Δ_i of type (l_i, m_i, n_i) onto G. Property (3) is equivalent to G acting freely on $C_1 \times C_2$. It is shown in [3] that properties (1) and (3) imply (2).

The fundamental group $\pi_1 S$ of a Beauville surface S is the inverse image of the diagonal subgroup under the natural epimorphism $\rho_1 \times \rho_2 : \Delta_1 \times \Delta_2 \to G \times G$, so that

$$\pi_1 S \cong \{(\gamma_1, \gamma_2) \in \Delta_1 \times \Delta_2 : \rho_1(\gamma_1) = \rho_2(\gamma_2)\}$$

It has a normal subgroup $M_1 \times M_2 \cong \pi_1 C_1 \times \pi_1 C_2 \cong \Pi_{g_1} \times \Pi_{g_2}$ with quotient group G, where Π_g denotes a surface group of genus g.

3 Properties of $PGL_2(p)$

From now onwards we let

$$G := PGL_2(p) = GL_2(p)/\{\lambda I \mid \lambda \in \mathbb{F}_p^*\},$$

a group of order $p(p^2-1)$, for some prime p. This group is complete, i.e. the centre $Z(G)$ and the outer automorphism group $\mathrm{Out}\, G$ are both trivial, so $\mathrm{Aut}\, G \cong G$, acting by conjugation. (See [17, §§II.6–II.8] for properties of G.)

Let $p > 2$, so that there are three conjugacy classes of maximal cyclic subgroups of G. These are

- elliptic subgroups, of order $p+1$, acting regularly on the projective line $\mathbb{P}^1(p)$ over $\mathbb{F}_p$;
- parabolic subgroups, of order p, with one fixed point and one regular orbit;
- hyperbolic subgroups, of order $p-1$, with two fixed points and one regular orbit.

The elliptic and hyperbolic cyclic subgroups C of order $p \pm 1$ have dihedral normalisers in G, of order $2(p \pm 1)$; each element $g \in C$ is conjugate in G to $g^{\pm 1}$, but to no other elements of C. The parabolic cyclic subgroups C of order p have normalisers of order $p(p-1)$; these are the stabilisers in G of points in $\mathbb{P}^1(p)$, isomorphic to the affine general linear group $AGL_1(p)$; in this case, all non-identity elements of C are conjugate to each other. In all cases except the involutions, the centraliser in G of a non-identity element is the unique maximal cyclic subgroup containing it; in the case of the involutions, it is the normaliser of that maximal cyclic subgroup, namely a dihedral group containing it as a subgroup of index 2.

The parabolic elements all lie in the subgroup $G^+ := PSL_2(p)$ of index 2 in G, whereas elliptic and hyperbolic elements, of order m dividing $p \pm 1$, lie in G^+ if and only if $(p \pm 1)/m$ is even. It follows that there are two conjugacy classes of involutions in G, one of them contained in G^+ and the other in $G \setminus G^+$. Any generating triple for G must contain one element of G^+, and two of $G \setminus G^+$.

For the rest of this paper we let $p \equiv 19 \bmod (24)$, or equivalently $p \equiv 3 \bmod (8)$ and $p \equiv 1 \bmod (3)$.

4 The first triples

Let k be any divisor of $p-1$ such that $(p-1)/k$ is odd, so the elements of this order in G all lie in $G \setminus G^+$. In particular, since $p \equiv 19 \bmod (24)$ we can write $k = 2k_0$ for some odd number k_0.

For each such k let $\mathbb{T}_k$ be the set of all triples (a_1, b_1, c_1) of type $(2, 3, k)$ in G. Since all elements of odd order lie in G^+, it follows that each such triple has $a_1 \in G \setminus G^+$, $b_1 \in G^+$, and $c_1 \in G \setminus G^+$. By our choice of p, all three elements of such a triple are hyperbolic, and hence so are all their non-identity powers.

Lemma 1. *If $(a_1, b_1, c_1) \in \mathbb{T}_k$ with $k > 10$ then b_1 and c_1^2 generate G^+.*

Proof. First let us note that c_1^2 lies in G^+. It is sufficient to show that no maximal subgroup of G^+ contains both of these elements. Dickson [10, Ch. XII] classified the maximal subgroups of the groups $PSL_2(q)$ for all prime powers q.

If q is an odd prime p then each maximal subgroup is of one of the following types:

- the stabiliser of a point in $\mathbb{P}^1(p)$, of order $p(p-1)/2$;
- a dihedral group of order $p \pm 1$;
- a subgroup isomorphic to A_4, S_4 or A_5.

Both b_1 and c_1^2 lie in point-stabilisers in G^+, but not in the same one, for otherwise b_1 and c_1 would lie in the same point-stabiliser in G, isomorphic to $AGL_1(p)$, whereas this group contains no triples of type $(2,3,k)$ for $k > 6$. The same argument deals with dihedral subgroups of order $p-1$, except that we replace point-stabilisers in G with dihedral subgroups of order $2(p-1)$. Dihedral subgroups of order $p+1$ are excluded since they have no elements of order 3, while A_4, S_4 and A_5 have none of order $k/2$ for $k > 10$. □

Corollary 1. *If $k > 10$ then each triple $(a_1, b_1, c_1) \in \mathbb{T}_k$ generates G.*

Proof. This follows immediately from Lemma 1, since G^+ is a maximal subgroup of G and $a_1 \notin G^+$. □

From now on, we will always assume that $k > 10$. There is a natural action of $\mathrm{Aut}\, G$ on $\mathbb{T}_k$. Since $\mathrm{Aut}\, G = \mathrm{Inn}\, G$, this action preserves the conjugacy classes containing the elements of each triple. By Corollary 1, only the identity automorphism can fix a triple in $\mathbb{T}_k$, so $\mathrm{Aut}\, G$ acts semiregularly (i.e. freely) on $\mathbb{T}_k$, with n_k orbits where $|\mathbb{T}_k| = n_k |\mathrm{Aut}\, G| = n_k p(p^2-1)$.

The triples $(a_1, b_1, c_1) \in \mathbb{T}_k$ all have their elements a_1 of order 2 in the same conjugacy class, namely the unique conjugacy class $\mathcal{A}$ of involutions in $G \setminus G^+$, and similarly their elements b_1 all lie in the unique class $\mathcal{B}$ of elements of order 3 in G. There are $\varphi(k)/2$ conjugacy classes $\mathcal{C}$ of elements of order k in G, so for each such class $\mathcal{C}$ let $\mathbb{T}_k(\mathcal{C})$ denote the set of triples in $\mathbb{T}_k$ with $c_1 \in \mathcal{C}$. Thus $\mathbb{T}_k$ is the disjoint union of the sets $\mathbb{T}_k(\mathcal{C})$, each of which is invariant under $\mathrm{Aut}\, G$ and is therefore a union of orbits of $\mathrm{Aut}\, G$.

Lemma 2. *For each conjugacy class $\mathcal{C}$ of elements of order k in G we have $|\mathbb{T}_k(\mathcal{C})| = p(p^2-1)$.* □

Proof. We can represent elements of G by pairs $\pm A$ of 2×2 matrices of determinant ± 1 over $\mathbb{F}_p$ (note that -1 is not a square in $\mathbb{F}_p$, since $p \equiv 3 \bmod (4)$). If $(a_1, b_1, c_1) \in \mathbb{T}_k(\mathcal{C})$ then there are $|\mathcal{A}| = p(p+1)/2$ possible choices for the involution a_1, and conjugating by a suitable element of G, we can assume that it is represented by the matrix

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The element b_1 of order 3 is represented by a matrix

$$B_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with $ad - bc = 1$ and (multiplying by -1 if necessary) $a + d = 1$. Then

$$A_1 B_1 = \begin{pmatrix} a & b \\ -c & -d \end{pmatrix},$$

so $a - d = \pm t$, the trace of a matrix representing elements of the (inverse-closed) class $\mathcal{C}$. Thus

$$a = \frac{1 \pm t}{2} \quad \text{and} \quad d = \frac{1 \mp t}{2},$$

so

$$bc = ad - 1 = \frac{-3 - t^2}{4}. \tag{1}$$

Now $t^2 \neq -3$, for otherwise $bc = 0$ and hence a_1 and b_1 have a common fixed point in $\mathbb{P}^1(p)$, contradicting Corollary 1. It follows that there are $p-1$ solutions $b, c \in \mathbb{F}_p^*$ of equation (1), and hence (allowing for the two choices for the $\pm$ sign) there are $2(p-1)$ possible elements b_1 represented by matrices B_1. Multiplying this by the number $p(p+1)/2$ choices for a_1, we see that there are $p(p^2-1)$ triples in $\mathbb{T}_k(\mathcal{C})$. □

Since $\mathrm{Aut}\, G$ has order $p(p^2-1)$, Lemma 2 shows that each $\mathbb{T}_k(\mathcal{C})$ is an orbit of this group, so we have:

Corollary 2. *If $k > 10$ then $\mathrm{Aut}\, G$ has $\varphi(k)/2$ orbits on $\mathbb{T}_k$, namely the sets $\mathbb{T}_k(\mathcal{C})$ where $\mathcal{C}$ ranges over the conjugacy classes of elements of order k in G. In particular, the orbit of a triple is characterized by the conjugacy class of its element of order k.* □

Corollary 3. *For $k > 10$ and a fixed element c of order k, we can take representatives of the $\varphi(k)/2$ orbits of $\mathrm{Aut}\, G$ on $\mathbb{T}_k$ of the form (a_i, b_i, c^{r_i}), for $i = 1, \ldots, \varphi(k)/2$, $1 \leq r_i \leq k/2$ and r_i coprime to k.* □

These $\varphi(k)/2$ orbits correspond to the torsion-free normal subgroups M_i ($i = 1, \ldots, \varphi(k)/2$) of the triangle group Δ_1 of type $(2, 3, k)$ such that $\Delta_1/M_i \cong G$ where, as noted in section 2, M_i is the kernel of the obvious epimorphism $\rho_i : \Delta_1 \to G$ determined by any triple of the corresponding orbit. Let X_i denote the quasiplatonic curve $\mathbb{H}/M_i$ uniformised by M_i.

Proposition 2. *The $\varphi(k)/2$ curves X_i have the following properties:*

1. *they are mutually non-isomorphic;*
2. *they all have automorphism group $\mathrm{Aut}\, X_i \cong G$;*
3. *they all have the real subfield $K = \mathbb{Q}(\zeta_k) \cap \mathbb{R}$ of the k-th cyclotomic field $\mathbb{Q}(\zeta_k)$ as their moduli field and field of definition, where $\zeta_k := \exp(2\pi i/k)$;*
4. *they form a single orbit under the Galois group $\mathrm{Gal}\, K/\mathbb{Q}$.* □

We recall that the field of moduli of an algebraic variety V defined over $\overline{\mathbb{Q}}$ is the subfield of $\overline{\mathbb{Q}}$ consisting of all elements fixed by the inertia group $I(V) = \{\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \mid V^\sigma \cong V\}$. The field of moduli is contained in any field of definition, but in general these two fields are not equal. However, Wolfart [27] has shown that quasiplatonic curves are always definable over their fields of moduli.

Let us stress here that in [25, Theorem 3] Streit proves the corresponding results for curves uniformised by normal subgroups of Δ_1 with quotient group isomorphic to $G^+ = PSL_2(p)$, where k divides $p \pm 1$. His method involves representing curves by their canonical models, and then studying the effect of Galois conjugation on local multipliers, the factors by which automorphisms multiply local coordinates near their fixed points. In order to prove the proposition we will need the following result from [15], which sums up Streit's method in a more general context.

Lemma 3. *Let G be a finite group and (a, b, c) a triple of generators of type (l, m, n) defining a curve C. Then for any $\sigma \in \mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$ the curve C^σ corresponds to a hyperbolic triple of generators $(a_\sigma, b_\sigma, c_\sigma)$ of G of the form*

$$a_\sigma = g a^\alpha g^{-1}, \qquad b_\sigma = h b^\beta h^{-1}, \qquad c_\sigma = c^\gamma$$

where $\sigma(\zeta_l^\alpha) = \zeta_l$, $\sigma(\zeta_m^\beta) = \zeta_m$ and $\sigma(\zeta_n^\gamma) = \zeta_n$ and $g, h \in G$.

In the particular case in which σ is complex conjugation, $(a_\sigma, b_\sigma, c_\sigma) = (a^{-1}, ab^{-1}a^{-1}, c^{-1})$.

Proof of Proposition 2. (1) We have $X_i \cong X_j$ if and only if $M_i^\gamma = M_j$ for some $\gamma \in PSL_2(\mathbb{R})$. If this is the case then $N(M_i)^\gamma = N(M_j)$, where $N(\ )$ denotes the normaliser in $PSL_2(\mathbb{R})$. Now M_i is normal in Δ_1, so $N(M_i)$ is a Fuchsian group containing Δ_1. By Singerman's classification [24], the triangle group of type $(2, 3, k)$ is a maximal Fuchsian group for $k > 6$, so $N(M_i) = \Delta_1$, and similarly $N(M_j) = \Delta_1$. Thus $\Delta_1^\gamma = \Delta_1$, so $\gamma \in N(\Delta_1) = \Delta_1$ and hence $M_i = M_j$, giving $i = j$.

(2) We have $\mathrm{Aut}\, X_i \cong N(M_i)/M_i$. The argument used to prove (1) shows that $N(M_i) = \Delta_1$, so $\mathrm{Aut}\, X_i \cong \Delta_1/M_i \cong G$.

(3) Let the triple $(a_1, b_1, c) \in \mathbb{T}_k(\mathcal{C})$ correspond to X_1. In view of the definition of a field of moduli, the first part of Lemma 3 clearly implies that the moduli field of X_1 is contained in $\mathbb{Q}(\zeta_k)$, and the second part of it states that the complex conjugate curve $\overline{X_1}$ is defined by $(a^{-1}, ab^{-1}a^{-1}, c^{-1})$, which lies in $\mathbb{T}_k(\mathcal{C})$ too, and therefore $\overline{X_1} \cong X_1$. As a consequence the moduli field of X_1 is contained in $K = \mathbb{Q}(\zeta_k) \cap \mathbb{R}$.

On the other hand, for every triple $(a', b', c') \in \mathbb{T}_k$, defining a curve X', we can suppose, by Corollary 3, that $c' = c^r$ for some r coprime to k. Now, by Lemma 3, for any element $\sigma \in \mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$ such that $\sigma(\zeta_k^r) = \zeta_k$ one has $(a_\sigma, b_\sigma, c_\sigma) = (g a^\alpha g^{-1}, h b^\beta h^{-1}, c^r)$, and by Corollary 2 it follows that $(a_\sigma, b_\sigma, c_\sigma)$ and (a', b', c') are $\mathrm{Aut}\, G$-equivalent. Hence $X_i^\sigma = X'$ and as a consequence the $\varphi(k)/2$ curves $X_1, \ldots, X_{\varphi(k)/2}$ are Galois conjugate.

Now, let us note that the field of moduli of a quasiplatonic curve is always a

field of definition of such a curve (see [27]), and therefore its degree is always greater than or equal to the cardinality of the Galois orbit of X_1. Since the field K has exactly degree $\varphi(k)/2$, it follows that K is the field of moduli (hence field of definition) of X_1, and therefore of each X_i.

(4) This follows from the proof of (3). □

4.1 An alternative proof of Lemma 2

Here we outline an alternative method of proof of Lemma 2 using character theory, which may be useful in groups where calculations with explicit elements, as above, are not so straightforward (see e.g. [14]). We use the following well-known result (see [22, §7.2] for this and other similar results):

Proposition 3. *If $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ are conjugacy classes in a finite group G, then the number of solutions $(a, b, c) \in \mathcal{A} \times \mathcal{B} \times \mathcal{C}$ of the equation $abc = 1$ is given by the formula*

$$\frac{|\mathcal{A}||\mathcal{B}||\mathcal{C}|}{|G|} \sum_{\chi} \frac{\chi(a)\chi(b)\chi(c)}{\chi(1)},$$

where χ ranges over the irreducible complex characters of G. □

The character table for $G = PGL_2(p)$ can be obtained from the generic character table for $GL_2(q)$ for all prime powers q (see [11, §15.9], for instance) by putting $q = p$ and restricting attention to those irreducible characters of $GL_2(q)$ which are constant on the scalar matrices, so that they correspond to representations of G.

In the case of Lemma 2 we have $|\mathcal{A}| = p(p+1)/2$, $|\mathcal{B}| = |\mathcal{C}| = p(p+1)$ and $|G| = p(p^2-1)$, so

$$|\mathbb{T}_k(\mathcal{C})| = \frac{p^2(p+1)^2}{2(p-1)} \sum_{\chi} \frac{\chi(a_1)\chi(b_1)\chi(c_1)}{\chi(1)}.$$

The character table for G shows that as $p \to \infty$ the sum on the right-hand side is dominated by the two characters χ of degree 1 (those of $G/G^+ \cong C_2$), which each contribute 1 to the summation. (More precise estimates of the character sum are aided by the fact that nearly half of the characters χ, specifically those of degree $p-1$, take the value 0 on hyperbolic elements, so they contribute nothing to the sum.) Thus

$$\frac{|\mathbb{T}_k(\mathcal{C})|}{|G|} = \frac{p(p+1)}{2(p-1)^2} \sum_{\chi} \frac{\chi(a_1)\chi(b_1)\chi(c_1)}{\chi(1)}$$

approaches 1 as $p \to \infty$. But this number is an integer, the number of (regular) orbits of $\mathrm{Aut}\, G = G$ on $T_k(\mathcal{C})$, so it must be equal to 1, giving $|\mathbb{T}_k(\mathcal{C})| = |G| = p(p^2-1)$. This argument provides a proof of Lemma 2 valid for sufficiently large primes $p \equiv 19 \bmod (24)$, but the careful proof it outlines, using exact character values, is valid for all such p.

5 The second triples

Now let l be any divisor of $p+1$ such that $(p+1)/l$ is odd. In this case, our choice of p implies that there is an odd number l_0 such that $l = 4l_0$. If (a_2, b_2, c_2) is any triple of type $(2, 4, l)$ in G, then $a_2 \in G^+$, $b_2 \in G \setminus G^+$, and $c_2 \in G \setminus G^+$. In this case the non-identity powers of a_2, b_2 and c_2 are all elliptic. Arguments similar to those used in the preceding section show that provided $l > 10$, each such triple generates G and there are $\varphi(l)/2$ orbits of $\mathrm{Aut}\, G$ on such triples, one for each of the $\varphi(l)/2$ conjugacy classes of elements c_2 of order l in G. (The involution a_2, represented by the matrix

$$A_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

has $p(p-1)/2$ conjugates, and the solutions of the analogue of equation (1) form two quadrics, each with $p+1$ points.) Since $l > 8$ the triangle group Δ_2 of type $(2, 4, l)$ is a maximal Fuchsian group [24]. Replacing the generator b_1 of order 3 with b_2 of order 4 is not significant, so as in the case of the first triples we find that the quasiplatonic curves Y_j corresponding to these orbits of triples satisfy:

Proposition 4. *The $\varphi(l)/2$ curves Y_j have the following properties:*

1. *they are mutually non-isomorphic;*
2. *they all have automorphism group $\mathrm{Aut}\, Y_j \cong G$;*
3. *they all have the real subfield $L = \mathbb{Q}(\zeta_l) \cap \mathbb{R}$ of the l-th cyclotomic field $\mathbb{Q}(\zeta_l)$ as their moduli field and field of definition;*
4. *they form a single orbit under the Galois group $\mathrm{Gal}\, L/\mathbb{Q}$ of L.* □

One can also apply the alternative argument given in §4.1, with minor modifications, to the triples of type $(2, 4, l)$ considered here: in this case the characters of degree $p+1$ vanish on the elliptic elements. This type of argument explains why we needed to choose both of the generating triples in G to include involutions: otherwise, we would have $|\mathcal{A}|, |\mathcal{B}|, |\mathcal{C}| \sim p^2$ as $p \to \infty$ and hence $\mathrm{Aut}\, G$ would have two orbits, rather than one, on generating triples in $\mathcal{A} \times \mathcal{B} \times \mathcal{C}$.

6 The Beauville surfaces

If (a_1, b_1, c_1) and (a_2, b_2, c_2) are triples in G of types $(2, 3, k)$ and $(2, 4, l)$, with $k, l > 10$, then since the non-identity powers of a_1, b_1 and c_1 are hyperbolic, while those of a_2, b_2 and c_2 are elliptic, these two triples form a Beauville structure of bitype $(2, 3, k; 2, 4, l)$, corresponding to a Beauville surface

$$S_{ij} = (X_i \times Y_j)/G.$$

Since $k = 2k_0$ and $l = 4l_0$ for coprime odd k_0 and l_0, the number of such surfaces S_{ij} is

$$\frac{\varphi(k)}{2}.\frac{\varphi(l)}{2} = \frac{\varphi(k_0)}{2}.\frac{2\varphi(l_0)}{2} = \frac{\varphi(k_0 l_0)}{2} = \frac{\varphi(m)}{4},$$

where

$$m = \mathrm{lcm}(k, l) = 4k_0 l_0.$$

By Proposition 2 the $\varphi(k)/2$ curves X_i are real and mutually non-isomorphic, as are the $\varphi(l)/2$ curves Y_j by Proposition 3. No pair X_i and Y_j can be isomorphic, since they are uniformised by surface groups with non-isomorphic normalisers Δ_1 and Δ_2. It therefore follows from Proposition 1 that the $\varphi(m)/4$ surfaces S_{ij} have mutually non-isomorphic fundamental groups. In particular, they are mutually non-homeomorphic.

Moreover, up to isomorphism there cannot be any more Beauville surfaces with group G and bitype $(2, 3, k; 2, 4, l)$. This is because if there was another Beauville surface S', its defining triples (a'_1, b'_1, c'_1) and (a'_2, b'_2, c'_2) would be conjugate to the two triples defining one of our surfaces S_{ij} by means of elements $g_1, g_2 \in G$. Now, if for $r = 1, 2$ we choose a preimage $\gamma_r \in \Delta_r$ of g_r under the epimorphism $\rho_r : \Delta_r \to G$ determined by the triple (a'_r, b'_r, c'_r) then, clearly the groups $\pi_1 S'$ and $\pi_1 S_{ij}$ uniformising the surfaces S' and S_{ij} (see section 2) are conjugate under the element $(\gamma_1, \gamma_2) \in \mathrm{Aut}(\mathbb{H} \times \mathbb{H})$. As a consequence, we can characterize the surface S_{ij} as the only Beauville surface with group G, bitype $(2, 3, k; 2, 4, l)$ and curves X_i and Y_j.

Example 1. *For $p = 19$ we can take $k = 18$ and $l = 20$. By the results of the previous sections there are $\varphi(18)/2 = 3$ orbits of $\mathrm{Aut}\, G$ on triples of generators of $G = PGL_2(19)$ of type $(2, 3, 18)$, and $\varphi(20)/2 = 4$ orbits on triples of type $(2, 4, 20)$. By computer means we can find representatives*

$$\begin{aligned}
(a_1, b_1, c_1) &= \left(\begin{pmatrix} 6 & 12 \\ 5 & 13 \end{pmatrix}, \begin{pmatrix} 3 & 12 \\ 12 & 13 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\right) \\
(a'_1, b'_1, c_1^5) &= \left(\begin{pmatrix} 2 & 6 \\ 9 & 17 \end{pmatrix}, \begin{pmatrix} 6 & 6 \\ 8 & 17 \end{pmatrix}, \begin{pmatrix} 13 & 0 \\ 0 & 1 \end{pmatrix}\right) \\
(a''_1, b''_1, c_1^7) &= \left(\begin{pmatrix} 11 & 10 \\ 7 & 8 \end{pmatrix}, \begin{pmatrix} 13 & 10 \\ 10 & 8 \end{pmatrix}, \begin{pmatrix} 14 & 0 \\ 0 & 1 \end{pmatrix}\right)
\end{aligned}$$

of the first three orbits, defining curves X_1, X_2, X_3, and representatives

$$\begin{aligned}
(a_2, b_2, c_2) &= \left(\begin{pmatrix} 0 & 9 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 10 & 9 \\ 2 & 15 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}\right) \\
(a'_2, b'_2, c_2^3) &= \left(\begin{pmatrix} 7 & 11 \\ 11 & 12 \end{pmatrix}, \begin{pmatrix} 13 & 7 \\ 17 & 12 \end{pmatrix}, \begin{pmatrix} 7 & 10 \\ 5 & 7 \end{pmatrix}\right) \\
(a''_2, b''_2, c_2^7) &= \left(\begin{pmatrix} 13 & 1 \\ 1 & 6 \end{pmatrix}, \begin{pmatrix} 12 & 6 \\ 4 & 13 \end{pmatrix}, \begin{pmatrix} 11 & 15 \\ 17 & 11 \end{pmatrix}\right) \\
(a'''_2, b'''_2, c_2^9) &= \left(\begin{pmatrix} 11 & 7 \\ 7 & 8 \end{pmatrix}, \begin{pmatrix} 11 & 13 \\ 9 & 14 \end{pmatrix}, \begin{pmatrix} 6 & 13 \\ 16 & 6 \end{pmatrix}\right)
\end{aligned}$$

of the last four orbits, defining curves Y_1, Y_2, Y_3, Y_4. *Any other triple* (r, s, t) *of type* $(2, 3, 18)$ *or* $(2, 4, 20)$ *can be mapped by an automorphism of* $PGL_2(19)$ *into one of the first three or last four orbits, depending on the conjugacy class of* t. *Consequently, we can construct* 12 *pairwise non-isomorphic Beauville surfaces of the form* $S_{ij} = (X_i \times Y_j)/PGL_2(19)$, *where* $1 \leq i \leq 3$ *and* $1 \leq j \leq 4$.

7 The Galois orbits

Since $K \cap L = \mathbb{Q}$, the compositum M of K and L, i.e. the subfield KL of $\overline{\mathbb{Q}}$ which they generate, has degree

$$|M : \mathbb{Q}| = |K : \mathbb{Q}||L : \mathbb{Q}| = \frac{\varphi(k)}{2}.\frac{\varphi(l)}{2} = \frac{\varphi(m)}{4}$$

over $\mathbb{Q}$. Since K and L are abelian extensions of $\mathbb{Q}$, so is M (it is, in fact, a proper subfield of $\mathbb{Q}(\zeta_m) \cap \mathbb{R}$). The Galois group $\operatorname{Gal} M/\mathbb{Q}$ of M over $\mathbb{Q}$ therefore has the form

$$\operatorname{Gal} M/\mathbb{Q} = \operatorname{Gal} M/L \times \operatorname{Gal} M/K \cong \operatorname{Gal} K/\mathbb{Q} \times \operatorname{Gal} L/\mathbb{Q}.$$

Since the direct factors act regularly on the sets of curves X_i and Y_j, it follows that $\operatorname{Gal} M/\mathbb{Q}$ acts regularly on the set of surfaces S_{ij}. These surfaces therefore form an orbit $\Omega = \Omega(p, k, l)$ of length $\varphi(m)/4$ under the absolute Galois group. We have thus proved:

Theorem 2. *For each prime* $p \equiv 19$ *mod* (24), *and for each pair of divisors* $k, l > 10$ *of* $p-1$ *and* $p+1$ *such that* $(p-1)/k$ *and* $(p+1)/l$ *are odd, there is an orbit of* $\operatorname{Gal}\overline{\mathbb{Q}}/\mathbb{Q}$ *consisting of* $\varphi(m)/4$ *Beauville surfaces with Beauville group* $PGL_2(p)$, *where* $m = \operatorname{lcm}(k, l)$, *and with mutually non-isomorphic fundamental groups.* □

For any prime $p \equiv 19 \bmod (24)$, one can satisfy the hypotheses of Theorem 2 by taking $k = p-1$ and $l = p+1$, thus proving Theorem 1 (see §1). The resulting Beauville structures have bitype $(2, 3, p-1; 2, 4, p+1)$, so that different Galois orbits $\Omega(p, p-1, p+1)$ correspond to Beauville structures of different bitypes. For a given p, the fundamental groups of these surfaces are all subgroups of index $|G| = p(p^2-1)$ in $\Delta_1 \times \Delta_2$; although they are mutually non-isomorphic, each is an extension of $\Pi_g \times \Pi_h$ by G, where the curves X_i and Y_j have genera

$$g = \frac{1}{12}(p-1)(p^2-5p-12) \quad \text{and} \quad h = \frac{1}{8}(p+1)(p^2-5p+8)$$

by the Riemann-Hurwitz formula.

The most general set of triples (p, k, l) satisfying the conditions of Theorem 2 arises as follows. Given any pair $k, l > 10$ with $k = 2k_0$ and $l = 4l_0$ for coprime odd k_0 and l_0, the latter coprime to 3, the congruences

$$p \equiv 19 \bmod (24), \quad p \equiv k+1 \bmod (2k), \quad p \equiv l-1 \bmod (2l)$$

are equivalent to

$$p \equiv 3 \bmod (8), \quad p \equiv 1 \bmod (k_0'), \quad p \equiv -1 \bmod (l_0)$$

where $k_0' = \mathrm{lcm}(3, k_0)$, and hence (since $8, k_0'$ and l_0 are mutually coprime) to a single congruence mod $(8k_0'l_0)$, satisfied by infinitely many primes p. For example, one could fix k and l, so that the bitype $(2, 3, k; 2, 4, l)$ and hence the group $\Delta_1 \times \Delta_2$ are fixed, by taking $k = 18$ and $l = 20$ for primes $p \equiv 19$ mod (360) for instance, but then the size $\varphi(k)\varphi(l)/4$ of the orbits $\Omega(p, k, l)$ is also fixed. This raises the question of whether there exist arbitrarily large Galois orbits of mutually non-homeomorphic Beauville surfaces, all corresponding to Beauville structures of the same bitype.

The kernel of the action of $\mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$ on a single orbit $\Omega = \Omega(p, k, l)$ is the subgroup $\mathrm{Gal}\,\overline{\mathbb{Q}}/M$ where $M = KL$. Note that KL is the moduli field of the surfaces $S_{ij} \in \Omega$. This is because $I(S_{ij}) = I(X_i \times Y_j) = I(X_i) \cap I(Y_j)$ and therefore the field of moduli of S_{ij} contains the compositum KL of the fields of moduli of X_i and Y_j while, on the other hand, the subfield fixed by $I(X_i \times Y_j)$ is included in KL, since it is a field of definition of $X_i \times Y_j$. The kernel of the action of $\mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$ on the union of all the orbits $\Omega(p, k, l)$ is therefore the intersection of these subgroups $\mathrm{Gal}\,\overline{\mathbb{Q}}/M$. This is $\mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{M}$ where $\mathbb{M}$ is the compositum of all the corresponding moduli fields M, a proper subfield of the maximal cyclotomic field

$$\mathbb{Q}^{\mathrm{ab}} = \bigcup_{n \in \mathbb{N}} \mathbb{Q}(\zeta_n).$$

This raises the problem of determining the kernel of the action of the absolute Galois group on all Beauville surfaces and, in particular, the question originally posed by Catanese in [5] of whether this action is faithful.

References

[1] H. Abelson, Topologically distinct conjugate varieties with finite fundamental group, *Topology* 13 (1974), 161–176.

[2] E. Artal, J. Carmona and J.I. Cogolludo, Effective invariants of braid monodromy, *Trans. Amer. Math. Soc.* 359 (2007), 165–183 .

[3] I. Bauer, F. Catanese and F. Grunewald, Beauville surfaces without real structures I, in *Geometric Methods in Algebra and Number Theory*, Progr. Math. 235, Birkhäuser Boston, Boston, 1–42 (2005).

[4] I. Bauer, F. Catanese and F. Grunewald, Chebycheff and Belyi polynomials, dessins denfants, Beauville surfaces and group theory, *Mediterr. J. Math.* 3 (2006), 121–146.

[5] I. Bauer, F. Catanese and F. Grunewald, The absolute Galois group acts faithfully on the connected components of the moduli space of surfaces of general type, arXiv:0706.1466v1.

[6] A. Beauville, Surfaces algébriques complexes, *Astérisque* 54, Société Mathématique de France, Paris (1978).

[7] G. V. Belyĭ, On Galois extensions of a maximal cyclotomic field, *Math. USSR Izvestija* 14 (1980), 247–256.

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

[9] F. Charles, Conjugate varieties with distinct real cohomology algebras, *J. Reine Angew. Math.* 630 (2005), 125–139.

[10] L.E. Dickson, *Linear Groups*, Dover, New York, 1958.

[11] F. Digne and J. Michel, *Representations of Finite Groups of Lie Type*, London Math. Soc. Student Texts 21, Cambridge University Press, Cambridge, 1991.

[12] R.W. Easton and R. Vakil, Absolute Galois acts faithfully on the components of the moduli space of surfaces: a Belyi-type theorem in higher dimension, *Int. Math. Res. Not. IMRN*, no. 20, Art. ID rnm080 (2007).

[13] Y. Fuertes, Non conjugate surfaces, preprint (2011).

[14] Y. Fuertes and G.A. Jones, Beauville structures and finite groups, J. Algebra **340** (2011), 13–27.

[15] G. González-Diez and D. Torres-Teigell, Non-homeomorphic Galois conjugate Beauville structures on $PSL(2,p)$, submitted.

[16] P. Griffiths and J. Harris, *Principles of Algebraic Geometry*, Wiley-Interscience, 1994

[17] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin - Heidelberg - New York, 1979.

[18] G.A. Jones and M. Streit, Galois groups, monodromy groups and cartographic groups, in *Geometric Galois actions, 2*, 25–65, London Math. Soc. Lecture Note Ser., 243, Cambridge Univ. Press, Cambridge, 1997.

[19] J.S. Milne and J. Suh, Nonhomeomorphic conjugates of connected Shimura varieties, *Amer. J. Math.* 132 (2010), 731–750.

[20] J-P. Serre, Géométrie algébrique et géométrie analytique, *Ann. Inst. Fourier* 6 (1956), 1–42.

[21] J-P. Serre, Exemples de variétés projectives conjuguées non homéomorphes, *C. R. Acad. Sci. Paris*, 258 (1964), 4194–4196.

[22] J-P. Serre, *Topics in Galois Theory*, Jones and Bartlett, Boston, MA, 1992.

[23] I. Shimada, Non-homeomorphic conjugate complex varieties, Singularities–Niigata–Toyama 2007, 285–301, Adv. Stud. Pure Math. **56**, Math. Soc. Japan, Tokyo, 2009.

[24] D. Singerman, Finitely maximal Fuchsian groups, *J. London Math. Soc.* (2) 6 (1972), 29–38.

[25] M. Streit, Field of definition and Galois orbits for the Macbeath-Hurwitz curves, *Arch. Math (Basel)* 74 (2000), 342–349.

[26] C. Voisin, *Hodge theory and complex algebraic geometry I*, Cambridge University Press, New York (2002).

[27] J. Wolfart, *ABC* for polynomials, dessins d'enfants and uniformization — a survey. Elementare und analytische Zahlentheorie, Schr. Wiss. Ges. Johann Wolfgang Goethe Univ. Frankfurt am Main, 20, Franz Steiner Verlag Stuttgart, Stuttgart, 2006, pp. 313–345. (http://www.math.uni-frankfurt.de/∼ wolfart/)

G. González-Diez:
Departamento de Matemáticas, Universidad Autónoma de Madrid, 28049, Madrid, Spain.
email: gabino.gonzalez@uam.es

G. A. Jones:
School of Mathematics, University of Southampton, Southampton SO17 1BJ, U.K.
email: G.A.Jones@maths.soton.ac.uk

D. Torres-Teigell:
Departamento de Matemáticas, Universidad Autónoma de Madrid, 28049, Madrid, Spain.
email: david.torres@uam.es