Galois invariants of dessins d'enfants

Jordan S. Ellenberg

8 Sep 2000

1 Introduction

> The two main problems of the theory of dessins d'enfants are the following: i) given a dessin, i.e., a purely combinatorial object, find the equations for β and X explicitly; ii) find a list of (combinatorial? topological? algebraic?) invariants of dessins which completely identify their $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-orbits. The second problem can be interestingly weakened from $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ to $\widehat{GT}$, but it remains absolutely non-trivial. (Schneps, [20].)

We are still very far from obtaining satisfactory solutions to either of the two problems Schneps identifies. In this article we discuss the second problem.

We begin by discussing several known invariants of dessin d'enfants, with special attention to the "interesting weakening" Schneps suggests. In particular, we show that both the cartographic group and the lifting invariants of Fried are invariant not only under $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, but under the *a priori* larger group $\widehat{GT}$. So these invariants cannot be used in any attempt to distinguish $\widehat{GT}$ from $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

Our second purpose is to describe a new invariant of genus 0 dessins d'enfants, related to the braid group. We will associate to every dessin d'enfant m a certain homomorphism

$$\tilde{m} : \pi_1(\mathbb{P}^1 - \{0, 1, \infty\}) \to \hat{H}_n,$$

where $\hat{H}_n$ is the profinite completion of the spherical braid group on n strands. This association is a Galois invariant in the sense that, for each $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$,

$$\widetilde{m^\sigma} = (\tilde{m})^\sigma. \tag{1.1}$$

Here, the action of σ on $\tilde{m}$ is given by actions of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on $\pi_1(\mathbb{P}^1 - \{0, 1, \infty\})$ and on $\hat{H}_n$, described in Section 4. It is not clear, though it seems reasonable to expect, that (1.1) holds for all $\sigma \in \widehat{GT}$.

For notational convenience, we restrict our attention in this paper to studying covers $X \to \mathbb{P}^1$ branched at only 3 points. The moduli space of r-branched covers of $\mathbb{P}^1$ with specified local data is a *Hurwitz scheme*, which is a finite cover of $\mathcal{M}_{0,r}/\mathbb{Q}$. [9]. The problem of identifying $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-orbits of dessins d'enfants is analogous to the problem of identifying connected components of the Hurwitz scheme. (Indeed, when $r = 3$, the Hurwitz scheme is just a finite cover of $\mathcal{M}_{0,3} = \operatorname{Spec} \mathbb{Q}$, whose connected components are precisely the $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-orbits of dessins.) All of the invariants of dessins described in this paper can be easily modified to be functions of r-branched covers which are constant on connected components of the Hurwitz scheme.

It must be emphasized that the substance of this article remains on the "topological" side of the theory, in the sense that the invariants we discuss can all be defined and analyzed whether or not we are aware that there exist fields smaller than $\mathbb{C}$. A true understanding of the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on dessins d'enfant will presumably require investigations of the relation between the *arithmetic* features of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ (Frobenii, inertia groups, known elements of Galois cohomology groups, and so on) and the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on geometric fundamental groups. Much progress has been made in this direction when the fundamental group of $\mathbb{P}^1 - \{0, 1, \infty\}$ is replaced by a nilpotent or metabelian quotient [3, 12] but the general case remains extremely murky. The recent work of Zapponi [26] is perhaps the first truly arithmetic incursion into the subject.

2 Definitions and notations

Let p be a point in $\mathbb{P}^1(\bar{\mathbb{Q}}) - \{0, 1, \infty\}$, and write Π for the group $\pi_1(\mathbb{P}^1_{\bar{\mathbb{Q}}} - \{0, 1, \infty\}, p)$. The fundamental group Π is isomorphic to $\hat{F}_2$, the profinite free group on 2 generators, but the isomorphism is non-canonical. Choose loops around $0, 1, \infty$ in $X(\mathbb{C})$ based at p whose product is homotopically trivial, and denote the corresponding elements of Π by x_0, x_1, x_∞. Note that the conjugacy classes of x_0, x_1, and x_∞ are independent of our choice of loops.

The arithmetic fundamental group $\pi_1(\mathbb{P}^1_{\mathbb{Q}} - \{0, 1, \infty\})$ lies in an exact sequence

$$1 \to \Pi \to \pi_1(\mathbb{P}^1_{\mathbb{Q}} - \{0, 1, \infty\}) \to \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to 1,$$

which yields an outer action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on Π. Write

$$\alpha : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Out}(\Pi)$$

for this action. It follows from Belyi's theorem that α is in fact an injection.

We briefly review the relation between three-point covers of the line, embeddings of 1-simplices in Riemann surfaces, and homomorphisms from Π to symmetric groups. We direct the reader to Grothendieck's foundational article [10] and the volume [19] for a more thorough introduction.

A *Belyi map* is a morphism β from a smooth projective algebraic curve $X_{\bar{\mathbb{Q}}}$ to $\mathbb{P}^1_{\bar{\mathbb{Q}}}$ which is étale away from $\{0, 1, \infty\}$. The inverse image of the real interval $[0, 1]$ under $\beta_{\mathbb{C}}$ is a 1-simplex $\mathcal{D}$ embedded in $X(\mathbb{C})$, which is usually called a *dessin d'enfant*; since a Belyi map determines a dessin d'enfant, and the topological type of the dessin d'enfant determines a Belyi map, we will sometimes refer to β itself as a dessin d'enfant. If $X_{\bar{\mathbb{Q}}} \cong \mathbb{P}^1_{\bar{\mathbb{Q}}}$, we will call β a genus 0 dessin d'enfant.

The restriction of β to $\mathbb{P}^1 - \{0, 1, \infty\}$ is a finite étale cover; such covers are in bijection via Galois theory with finite-index subgroups $G \subset \Pi$. Finite subgroups of Π, in turn, correspond via the action on cosets to homomorphisms $m : \Pi \to S_n$, where $n = [\Pi : G] = \deg \beta$. Write m_β for the homomorphism arising in this way from the Belyi map β. It is easy to verify that there is a bijection between the set of isomorphism classes of Belyi maps of degree n and the set of conjugacy classes of homomorphisms from Π to S_n with transitive image. Thus, we will also refer to m_β as a dessin d'enfant.

A genus 0 dessin d'enfant is often specified by drawing a picture of the 1-simplex $\mathcal{D}$ embedded in the complex plane. The vertices lying over 0 are denoted by black dots, and the vertices over 1 by white dots. For example, Figure 1 shows the dessin d'enfant associated to the map $m : \Pi \to S_6$ sending x_0 to $(5, 4, 3, 2)$ and x_1 to $(1, 2)(5, 6)$. Bétréma, Péré, and Zvonkin have computed [1] that this dessin d'enfant is realized by the map

$$\beta(z) = -3^9 2^{-4} 5^{-5} z^4 (z^2 - 2z + 25/9).$$

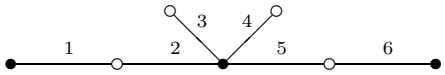

Figure 1: A 6-edge dessin d'enfant.

The main problem of dessin d'enfants is precisely to study the interplay between the algebro-geometric object β and the combinatorial object m_β. In particular: if σ is an element of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, then β^σ is another Belyi map, with a corresponding homomorphism m_{β^σ} satisfying

$$m_{\beta^\sigma} = m_\beta \circ \alpha(\sigma).$$

Note that α is defined only up to composition with an inner automorphism of Π; this ill-definedness is irrelevant, since we care about m only up to conjugacy in S_n.

We say that two homomorphisms $m, m' : \Pi \to S_n$ are *Galois conjugate* if $m' = m \circ \alpha(\sigma)$ for some $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, and in that case we write $m' = m^\sigma$. Our goal is then to describe combinatorial invariants of m which are left unchanged by Galois conjugation.

If g, g' are elements of a group, we use $g \sim g'$ to mean that g and g' are conjugate. We write $[g]$ for the conjugacy class of g. If ϕ, ϕ' are homomorphisms from G_1 to G_2, we use $\phi \sim \phi'$, or "ϕ is conjugate to ϕ'," to mean that ϕ is obtained from ϕ' by composition with an inner automorphism of G_1. In this article, all homomorphisms from Π to other groups will be defined only up to composition with an inner automorphism of Π, and all equations of homomorphisms should be understood to hold only up to such a composition.

3 Galois invariants of dessins d'enfants

In this section we will describe some of the known Galois invariants of dessin d'enfants. We will observe that these invariants are typically invariant under the action of a group of outer automorphisms of Π which is *a priori* larger than $\alpha(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}))$.

Definition 3.1. Let $\mathrm{Aut}^*(\Pi)$ be the group of automorphisms a of Π such that

$$a(x_0) \sim x_0^\lambda, a(x_1) \sim x_1^\lambda, a(x_\infty) \sim x_\infty^\lambda$$

for some $\lambda \in \hat{\mathbb{Z}}^*$. Define $\mathrm{Out}^*(\Pi)$ to be the quotient of $\mathrm{Aut}^*(\Pi)$ by the group of inner automorphisms.

Proposition 3.2. $\alpha(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})) \in \mathrm{Out}^*(\Pi)$.

Proof. This follows directly from the branch cycle argument of Fried–see for instance [8, §3]. In fact, $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ sends each x_i to a conjugate of $x_i^{\chi(\sigma)}$, where $\chi : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \hat{\mathbb{Z}}^*$ is the cyclotomic character. □

Definition 3.3. We say that two homomorphisms $m, m' : \Pi \to S_n$ are *combinatorially indistinguishable* if there is an element a of $\mathrm{Out}^*(\Pi)$ such that $m' = m \circ a$.

From Proposition 3.2, we have at once that Galois conjugate dessins are combinatorially indistinguishable.

In general, to prove that two dessins are combinatorially indistinguishable is more difficult than to prove they are not. For instance, one knows:

Proposition 3.4. *Let m, m' be combinatorially indistinguishable dessins. Then*

- *$m(x_0) \sim m'(x_0^\lambda), m(x_1) \sim m'(x_1^\lambda), m(x_\infty) \sim m'(x_\infty^\lambda)$ for some $\lambda \in \hat{\mathbb{Z}}^*$;*
- *The image of m and the image of m' are conjugate subgroups of S_n.*

Proof. The first statement is immediate from the definition of $\mathrm{Out}^*(\Pi)$. The second statement is merely the observation that $m \circ \alpha$ and m have the same image for any automorphism α of Π. □

The image of m is called the *monodromy group* of m; we denote it by $\mathrm{Mon}(m)$. We will write $\mathrm{Mon}(\beta)$ or $\mathrm{Mon}(\mathcal{D})$ when the dessin is specified by a Belyi map β or an embedded simplex $\mathcal{D}$. The monodromy group is also called the *edge-rotation group*, a notation which arises from the embedded simplex $\mathcal{D} \in X(\mathbb{C})$ attached to m. A loop around $0, 1$, or ∞ in the base induces a permutation of the edges of $\mathcal{D}$; the monodromy group is precisely the group generated by these permutations.

The triple of conjugacy classes $([m(x_0)], [m(x_1)], [m(x_\infty)])$ is called the *Nielsen class* of m. Define the *rational Nielsen class* of m to be the set of all triples $([m(x_0)]^\lambda, [m(x_1)]^\lambda, [m(x_\infty)]^\lambda)$, where λ ranges over $\hat{\mathbb{Z}}^*$. In general, a Nielsen class for a group G is a triple of conjugacy classes (c_0, c_1, c_∞). The action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on Nielsen classes is defined by

$$(c_0, c_1, c_\infty)^\sigma = (c_0^{\chi(\sigma)}, c_1^{\chi(\sigma)}, c_\infty^{\chi(\sigma)})$$

and a rational Nielsen class is a $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-orbit of Nielsen classes.

The rational Nielsen class and the monodromy group are the most well-known invariants of dessins d'enfant, and the rational Nielsen class is by far the easiest to compute. There are many examples of pairs of dessins d'enfant with identical monodromy groups and rational Nielsen classes which are, nonetheless, not Galois conjugate [15]. Such pairs can sometimes be teased apart by means of finer invariants, some of which we summarize below.

Cartographic group, and variants

(Reference: [15, §4])

The *cartographic group* $\mathrm{Cart}(m)$ of a dessin m is classically understood in terms of the corresponding 1-simplex $\mathcal{D}$. Consider the set of $2n$ directed edges, or *flags*, of $\mathcal{D}$. Let m_0' be the permutation on the flags induced by rotating each flag counterclockwise about the vertex toward which it points, and let τ be the permutation induced by reversing the direction of each flag. For example, we may number the flags of the dessin $\mathcal{D}$ in Figure 1 as follows: for each undirected edge n of $\mathcal{D}$, let the two flags over n be numbered n and $n+6$, with the lower number assigned to the edge pointing towards a black vertex. In this case, we have

$$m_0' = (5,4,3,2)(7,8)(11,12), \tau = (1,7)(2,8)(3,9)(4,10)(5,11)(6,12).$$

The cartographic group of m is defined to be the subgroup of S_{2n} generated by m_0' and τ.

Let $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ be the morphism sending z to $4z(1-z)$. Then the cartographic group attached to a Belyi map β is precisely the monodromy group $\mathrm{Mon}(\phi \circ \beta)$. Now ϕ is defined over $\mathbb{Q}$; so if $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, we have

$$\mathrm{Cart}(m^\sigma) = \mathrm{Mon}(\phi \circ \beta^\sigma) = \mathrm{Mon}(\phi^\sigma \circ \beta^\sigma) = \mathrm{Mon}(\phi \circ \beta) = \mathrm{Cart}(m).$$

Here, the equality signs mean "conjugate in S_{2n}". So Galois-conjugate dessins have conjugate cartographic groups.

It is not clear that combinatorially indistinguishable dessins have the conjugate cartographic groups. But the cartographic group is invariant under the action of a special subgroup of $\mathrm{Out}^*(\Pi)$, namely the Grothendieck-Teichmüller group $\widehat{GT}$. In fact, $\mathrm{Cart}(m)$ is an invariant for an even larger group, $\widehat{GT}_0$. For a full discussion of the group $\widehat{GT}$, we refer the reader to the articles on the subject in [19],[21]. We observe here only that

$$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \subset \widehat{GT} \subset \widehat{GT}_0 \subset \mathrm{Out}^*(\Pi),$$

and that it is felt to be at least plausible that the first inclusion is an equality.

The automorphism group of the algebraic curve $\mathbb{P}^1 - \{0, 1, \infty\}$ is isomorphic to S_3, and is generated by the involutions $z \to 1 - z$ and $z \to 1/z$. Any automorphism of $\mathbb{P}^1 - \{0, 1, \infty\}$ gives rise to an automorphism of Π; so from the whole automorphism group of the curve one obtains a subgroup P of $\mathrm{Out}(\Pi)$ which is isomorphic to S_3. We will be interested in particular in the outer automorphism $\theta \in \mathrm{Out}(\Pi)$ arising from the map $z \to 1 - z$. A representative for θ is the automorphism sending x_0 to x_1 and x_1 to x_0.

Definition 3.5. The group $\widehat{GT}_0$ is the subgroup of $\mathrm{Out}^*(\Pi)$ consisting of outer automorphisms commuting with every element of P.

Remark 3.6. The equivalence of Definition 3.5 with the more usual one is proved in [11].

Proposition 3.7. *The cartographic group is a $\widehat{GT}_0$-invariant.*

Proof. We need to prove that $\mathrm{Cart}(m \circ \alpha) = \mathrm{Cart}(m)$ for all $\alpha \in \widehat{GT}_0$.

Define m'_0, τ as above, and let $m' : \Pi \to S_{2n}$ be the homomorphism defined by

$$m'(x_0) = m'_0, m'(x_1) = \tau.$$

Define a subgroup $H \cong S_n \oplus S_n \hookrightarrow S_{2n}$ consisting of those permutations which act separately on the black-facing edges and the white-facing edges. Let K be the kernel of the homomorphism from Π to $\mathbb{Z}/2\mathbb{Z}$ sending x_0 to 0 and x_1 to 1; then $m'(K)$ lies in H. Evidently, $\mathrm{Cart}(m) = m'(\Pi)$ is the group generated by $m'(K)$ and τ.

We may think of K as the fundamental group of the étale double cover $X \to \mathbb{P}^1 - \{0, 1, \infty\}$ ramified only at $1, \infty$. The curve X is a line with four points removed, and by considering the topology of $X(\mathbb{C})$ one sees that K is generated by $x_0, x_1^{-1}x_0x_1$, and x_1^2. Since $m'(x_1)$ is an involution, we have that $m'(K)$ is generated by $m'(x_0) = m'_0$ and $m'(x_1^{-1}x_0x_1)$.

Now let us examine more carefully the relationship between m' and m. The permutation m'_0 acts as $m(x_0)$ on the black-facing edges and as $m(x_1)$ on the white-facing edges; that is, we can write $m'_0 \in S_n \oplus S_n$ as $m(x_0) \oplus m(x_1)$. Similarly, $m'(x_1^{-1}x_0x_1) = m(x_1) \oplus m(x_0)$. We are thus led to consider the homomorphism

$$m \oplus (m \circ \theta) : \Pi \to S_n \oplus S_n$$

where θ is the automorphism of Π switching x_0 and x_1, as above. We have shown precisely that $m'(K)$ is the image of $m \oplus (m \circ \theta)$.

Now let α be an element of $\widehat{GT}_0$; then we have

$$(m \circ \alpha) \oplus [(m \circ \alpha) \circ \theta] = m \circ \alpha \oplus [(m \circ \theta) \circ \alpha] = [m \oplus (m \circ \theta)] \circ \alpha.$$

But composing with the automorphism α of Π does not change the image of $m \oplus (m \circ \theta)$; we thus conclude that replacing m with $m \circ \alpha$ does not change $m'(K)$, whence does not change $\mathrm{Cart}(m)$. (As always, the equalities above are understood to mean "up to composition with inner automorphisms.")

□

Example 3.8. ([15, Ex. 5]) Let m_1 be the 7-edge dessin defined by

$$m_1(x_0) = (1,2,3)(4,5), m_1(x_1) = (3,4)(5,6,7)$$

and m_2 the dessin defined by

$$m_2(x_0) = (1,2)(3,4,5), m_2(x_1) = (2,3)(5,6,7).$$

The two dessins are in the same Nielsen class, and both have monodromy group S_7. However, the first dessin has cartographic group of size $2 \cdot 7!$, while the second has cartographic group of size $(7!)^2$. Thus, m_1 and m_2 are not Galois conjugate. The disparity in the cartographic groups in this case is related to the fact that $m_1 \circ \theta$ is isomorphic to m_1, while $m_2 \circ \theta$ is not isomorphic to m_2.

The argument we used to show that the cartographic group is Galois-invariant gives rise to a large class of related Galois invariants. We may take $\phi : \mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ to be *any* Belyi morphism such that $\phi(\{0,1,\infty\}) \subset \{0,1,\infty\}$. Then $\phi \circ \beta$ is a Belyi morphism for any Belyi morphism β, and $\mathrm{Mon}(\phi \circ \beta)$ is a Galois invariant of the dessin β. It is not at all clear that these Galois invariants are invariant under $\widehat{GT}$ as well.

We might think of the above construction as producing, not only Galois invariants, but Galois *equivariants.* That is: for ϕ as above, the correspondence c_ϕ defined by

$$c_\phi(m_\beta) = m_{\phi \circ \beta}$$

is Galois-equivariant, in the sense that

$$c_\phi(m)^\sigma = c_\phi(m^\sigma).$$

So if $c_\phi(m)$ and $c_\phi(m')$ are known not to be Galois conjugate (e.g., if they have different monodromy groups) then m and m' are also not Galois conjugate.

Lifting invariants

The use of lifting invariants to classify covers of $\mathbb{P}^1$ with identical rational Nielsen classes was developed by Fried [6, §III. D] in his study of components of Hurwitz moduli spaces and modular towers, and by Serre in his work on rigid triples in finite groups [23].

Let

$$1 \to H \to \hat{G} \xrightarrow{\phi} G \to 1$$

be an exact sequence of finite groups. Let $\hat{c} = (\hat{c}_0, \hat{c}_1, \hat{c}_\infty)$ be a Nielsen class in $\hat{G}$, and denote by c the image of $\hat{c}$ in G. Let F be an abelian extension of $\mathbb{Q}$ such that $\mathrm{Gal}(\bar{\mathbb{Q}}/F)$ fixes the Nielsen class c; such an extension exists by the proof of Proposition 3.2.

The *lifting invariant* of a dessin d'enfant is defined as follows. Suppose $m : \Pi \to G \subset S_n$ is a dessin with Nielsen class c. Consider the finite set of all triples $(\hat{m}_0, \hat{m}_1, \hat{m}_\infty)$ such that

- $\phi(\hat{m}_i) = m(x_i)$;
- The Nielsen class of $(\hat{m}_0, \hat{m}_1, \hat{m}_\infty)$ is $\hat{c}^{\chi(\sigma)}$, for some $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/F)$.

For each triple satisfying the two conditions above, the product $\hat{m}_0\hat{m}_1\hat{m}_\infty$ lies in H. Let $L_0(m)$ be the set of all elements of H arising in this way, and let $L(m)$ be the union of the sets $(L_0(m)^g)^{\chi(\sigma)}$ for all $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/F)$ and all $g \in \hat{G}$.

We should point out that $L(m)$ depends on our choice of $\hat{G}$ and $\hat{c}$; for simplicity we suppress this dependence in the notation.

The cyclotomic character χ naturally extends to the Grothendieck-Teichmüller group $\widehat{GT}$. Let $\widehat{GT}_F$ be the subgroup of $\sigma \in \widehat{GT}$ such that $\chi(\sigma) \in \chi(\mathrm{Gal}(\bar{\mathbb{Q}}/F))$.

Proposition 3.9. *$L(m)$ is invariant for the action of $\widehat{GT}_F$.*

Proof. The main point is a theorem of Schneps and Harbater concerning actions of $\widehat{GT}$ on moduli spaces of genus 0 curves [11]. Let $\hat{K}(0,n)$ be the (profinite) geometric fundamental group of the moduli space $\mathcal{M}_{0,n}$. Then $\hat{K}_{0,4}$ is isomorphic to Π. The group $\hat{K}_{0,5}$ has a standard presentation in generators $x_{i,j}$ for $1 \le i < j \le 5$.

As in [11, §1.1], there is an exact sequence of groups

$$1 \to \Pi' \xrightarrow{i} \hat{K}_{0,5} \xrightarrow{p_2} \Pi \to 1$$

where Π' is the subgroup generated by $x_{21}, x_{23}, x_{24}, x_{25}$; the presentation of Π' in these generators is subject only to the relation $x_{21}x_{23}x_{24}x_{25} = 1$. One also has a map

$$p_4 : \hat{K}_{0,5} \to \Pi$$

which sends x_{21} to x_0 and x_{23} to x_1. In particular, we have

$$p := p_4 \circ i : \Pi' \to \Pi$$

which sends x_{21} to x_0 and x_{23} to x_1, and kills x_{24}. The action of $\widehat{GT}$ on profinite braid groups defined by Drinfel'd yields an action of $\widehat{GT}$ on $\hat{K}(0,5)$, which restricts to an action of $\widehat{GT}$ on Π'.

Now Proposition 9 of [11] tells us that p is equivariant for the action of $\widehat{GT}$ on either side. We now rename the generators of Π' as follows:

$$x'_0 = x_{21}, x'_1 = x_{23}, x'_\infty = x_{25}, x'_a = x_{24}.$$

Now the action of $\widehat{GT}$ on Π' is *inertia-preserving*; that is,

$$[(x'_i)^\sigma] = [x'_i]^{\chi(\sigma)} \tag{3.2}$$

for $\sigma \in \widehat{GT}$ and $i = 0, 1, \infty, a$. Write $\alpha'(\sigma)$ for the outer automorphism of Π' corresponding to $\sigma \in \widehat{GT}$.

We say $\hat{m} : \Pi' \to \hat{G}$ is a *lift* of m if $\phi \circ \hat{m}$ is conjugate to $m \circ p$ and if there exists $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/F)$ such that $\hat{m}(x'_i)$ lies in $\hat{c}_i^{\chi(\sigma)}$ for $i = 0, 1, \infty$. Then $L(m)$ is just the set of elements of the form $m'(x'_a)^{-1}$ for all lifts m' of m.

Choose a σ in $\widehat{GT}_F$. If m' is a lift of m, then the commutativity of the diagram

$$\begin{array}{ccccc} \Pi' & \xrightarrow{\alpha'(\sigma)} & \Pi' & \xrightarrow{m'} & \hat{G} \\ {\scriptstyle p}\downarrow & & {\scriptstyle p}\downarrow & & {\scriptstyle \phi}\downarrow \\ \Pi & \xrightarrow{\alpha(\sigma)} & \Pi & \xrightarrow{m} & G \end{array}$$

together with the local condition (3.2) shows that $\alpha'(\sigma) \circ m'$ is a lift of m^σ; inverting σ, we see that every lift of m^σ is of this form. So $L(m^\sigma)$ consists precisely of elements of H of the form

$$m'((x'_a)^\sigma)^{-1}$$

which is conjugate to $m'(x'_a)^{-\chi(\sigma)}$ by (3.2). Since $L(m)$ is closed under exponentiation by $\chi(\sigma)$, we have $L(m^\sigma) = L(m)$ as desired. □

Example 3.10. ([6, §III. D])

Following Fried, we exhibit an example with 5 branch points. Take $G = A_5$ and let $\hat{G}$ be the unique non-split central extension of G with kernel $\mathbb{Z}/2\mathbb{Z}$. Let c be the conjugacy class of a 3-cycle in G, and let $\hat{c}$ be the conjugacy class of order-3 elements of $\hat{G}$ lying over c. Finally, take $\mathbf{c} = (c, c, c, c, c)$ and $\hat{\mathbf{c}} = (\hat{c}, \hat{c}, \hat{c}, \hat{c}, \hat{c})$.

Let

$$m : \pi_1(\mathbb{P}^1 - \{0, 1, \infty, a, b\}) \to G$$

be a homomorphism sending a generator of inertia at each puncture to an element of c. Then we can define $L(m) \subset \mathbb{Z}/2\mathbb{Z}$ by analogy with the definition above. Fried exhibits homomorphisms m^+ and m^- in this Nielsen class, with $L(m^+) = \{0\}$ and $L(m^-) = \{1\}$. It follows that the 5-branched covers of the line corresponding to m^+ and m^- are not Galois conjugate. (Moreover, they lie on different connected components of the relevant Hurwitz space.) In fact, Fried constructs examples of this kind with arbitrarily many branch points.

4 Definition of the braid group invariant

The second goal of this paper is to define a new invariant of genus-0 dessins d'enfants. The invariant takes the form of a homomorphism from Π to a certain braid group.

Let $V/\mathbb{Q}$ be the complement in $(\mathbb{P}^1)^n$ of the union of the hyperplanes $x_i = x_j$, for all $1 \leq i < j \leq n$. Then the symmetric group S_n acts without fixed points on V by permutation of coordinates; let U be the quotient of this action. The points of U over $\bar{\mathbb{Q}}$ are precisely the sets of n distinct points of $P^1(\bar{\mathbb{Q}})$. The geometric fundamental group of U is $\hat{H}_n$, the profinite completion of the spherical braid group on n strands [17, III, Th. 2.2]. Note that $\hat{H}_n$ acquires an outer action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ by virtue of its status as the geometric fundamental group of a variety over $\mathbb{Q}$. We write this action as a homomorphism

$$\alpha_b : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Out}(\hat{H}_n).$$

Observe also that the Galois cover $V \to U$, with Galois group S_n, induces a map

$$q : \hat{H}_n \to S_n.$$

Let $m : \Pi \to S_n$ be a genus 0 dessin d'enfant, and let $\beta : X \to \mathbb{P}^1$ be the corresponding Belyi map. Note that X is isomorphic to $\mathbb{P}^1_{\bar{Q}}$; we choose such an isomorphism and assume $X = \mathbb{P}^1_{\bar{Q}}$ from now on.

One now obtains a map

$$\tilde{\beta} : \mathbb{P}^1 - \{0, 1, \infty\} \to U$$

by the rule

$$\tilde{\beta}(t) = \{\beta^{-1}(t)\}.$$

This map of varieties over $\mathbb{Q}$ induces a map of geometric fundamental groups

$$\tilde{m} : \Pi \to \hat{H}_n.$$

Note that the pullback of the cover $V \to U$ by $\tilde{\beta}$ is precisely the restriction of β to $\mathbb{P}^1 - \{0, 1, \infty\}$. On the level of fundamental groups, this means that

$$m = q \circ \tilde{m}$$

Now the observation that $\widetilde{\beta^\sigma} = \tilde{\beta}^\sigma$ yields the following theorem.

Proposition 4.1. *Let m be a genus 0 dessin d'enfant. Define*

$$\tilde{m} : \Pi \to \hat{H}_n$$

as above. Then $\widetilde{m^\sigma} = \alpha_b(\sigma^{-1}) \circ \tilde{m} \circ \alpha(\sigma)$.

We think of $\tilde{m}$ as a kind of canonical lift of m from the symmetric group to the spherical braid group.

The topological fundamental group of $U(\mathbb{C})$ is just the ordinary spherical braid group H_n, which we recall is generated by elements $e_1, \ldots, e_{n-1}$ subject only to the relations

$$\begin{aligned} e_i e_j &= e_j e_i, |i-j| > 2 \\ e_i e_{i+1} e_i &= e_{i+1} e_i e_{i+1} \\ e_1 e_2 \ldots e_{n-1} e_{n-1} \ldots e_2 e_1 &= 1. \end{aligned}$$

Note that the Artin braid group B_n is generated by $e_1, \ldots, e_n$ subject only to the first two relations above.

The elements of H_n correspond to isotopy classes of n-strand braids in $\mathbb{P}^1(\mathbb{C}) \times [0, 1]$. In particular, e_i is the braid obtained by pulling strand i in front of strand $i + 1$. (See [2] for all facts used here about braid groups.)

The morphism $\tilde{\beta}$ yields a map of complex manifolds from $\mathbb{P}^1(\mathbb{C}) - \{0, 1, \infty\}$ to $U(\mathbb{C})$, which in turn yields a homomorphism of topological fundamental groups

$$< x_0, x_1 > \to H_n$$

whose profinite completion is $\tilde{m}$. By abuse of notation, we also refer to this topological map as $\tilde{m}$.

The topological meaning of $\tilde{m}$ is not hard to see. Let $\gamma : [0, 1] \to \mathbb{P}^1(\mathbb{C}) - \{0, 1, \infty\}$ be a loop in $\mathbb{P}^1(\mathbb{C}) - \{0, 1, \infty\}$ representing the class x_0 in the topological fundamental group. Now define

$$B = \{(z, t) \in \mathbb{P}^1(\mathbb{C}) \times [0, 1] : \beta(z) = \gamma(t)\}.$$

Then B is a braid, and we define $\tilde{m}(x_0)$ to be the isotopy class of B. The element $\tilde{m}(x_1)$ is defined similarly. In Figure 2 we illustrate this construction for the dessin d'enfant shown in Figure 1. In this case, we find $\tilde{m}(x_0) = e_2 e_3 e_4, \tilde{m}(x_1) = e_1 e_5$.

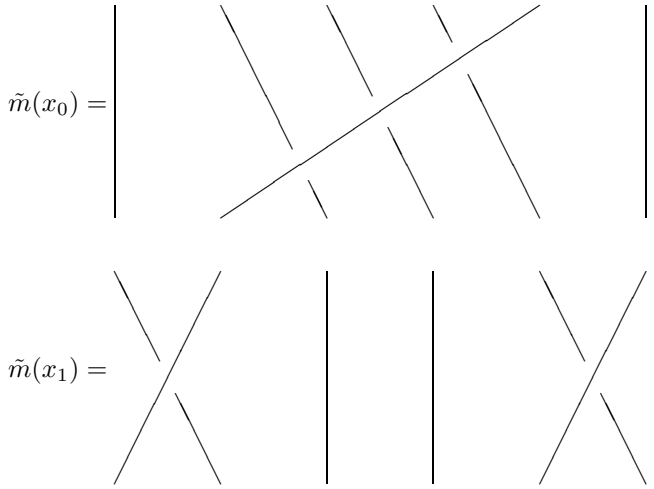

Figure 2: The braids associated to a 6-edge dessin.

5 Properties of the braid group invariant

To every genus 0 dessin $m : \Pi \to S_n$, we have associated a homomorphism $\tilde{m} : \Pi \to \hat{H}_n$, such that $\tilde{m}$ and $\tilde{m'}$ are Galois conjugate if and only if m and m' are Galois conjugate. We now discuss the following question: to what extent can the invariants described in Section 3 separate $\tilde{m}$ and $\tilde{m'}$?

Define a *twine class* in $\hat{H}_n$ to be a conjugacy class containing $e_{a_1} e_{a_2} \dots e_{a_r}$ for some *strictly increasing* sequence $a_1, \dots a_n$. For each conjugacy class $\mathbf{c}$ in S_n, there is a unique twine class $\tilde{\mathbf{c}}$ in $\hat{B}_n$ with $q(\tilde{\mathbf{c}}) = \mathbf{c}$. A *rational twine class* is the union of $\tilde{\mathbf{c}}^\lambda$ for some twine class $\tilde{\mathbf{c}}$ and all $\lambda \in \hat{\mathbb{Z}}$.

Proposition 5.1. *The conjugacy classes of $\tilde{m}(x_0), \tilde{m}(x_1)$, and $\tilde{m}(x_\infty)$ are all twine classes.*

Proof. Evident from the topological description above. □

In particular, this means that if m and m' are in the same Nielsen class, then so are $\tilde{m}$ and $\tilde{m'}$.

Remark 5.2. One has a corollary the following fact about equations in braid groups. Let m_0, m_1, m_∞ be permutations in S_n such that $m_0 m_1 m_\infty = 1$, and suppose that the total number of orbits in all three permutations is $n + 2$. Then there exist braids $\tilde{m}_0, \tilde{m}_1, \tilde{m}_\infty$ in $\hat{H}_n$ such that

- $\tilde{m}_i$ lies in the twine class over m_i;
- $m_0 m_1 m_\infty = 1$.

Question 1: Is there a purely group-theoretic proof of this fact?

Define the *braid monodromy group* $BM(m)$ of m to be the subgroup of $\hat{H}_n$ generated by $\tilde{m}(x_0)$ and $\tilde{m}(x_1)$.

Proposition 5.3. *If m and m' are Galois conjugate, their braid monodromy groups are related to each other by an automorphism of $\hat{H}_n$.*

Proof. It is immediate from Proposition 4.1 that the image of $\widetilde{m^\sigma}$ is the result of applying the automorphism $\alpha_b(\sigma^{-1})$ to the image of $\tilde{m}$. □

A symplectic quotient of the braid group

In general, the braid monodromy group is difficult to compute. In order to get more practical invariants, we will make use of known profinite Galois covers $U'_{\mathbb{Q}} \to U_{\mathbb{Q}}$. Such a cover, with Galois group G, corresponds to a surjection

$$pr : \pi_1(U_{\bar{\mathbb{Q}}}) = \hat{H}_n \to G$$

whose kernel is fixed by the outer action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on $\hat{H}_n$. The outer action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ then projects to an outer action of G. Suppose m and m' are Galois conjugate. Then $pr \circ \tilde{m}$ and $pr \circ \tilde{m}'$ are Galois conjugate as well. In particular, the images of $pr \circ \tilde{m}$ and $pr \circ \tilde{m}'$ differ via an automorphism in G; more precisely, they differ by an automorphism in the image of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Out}(G)$. In certain cases, we can specify this image exactly, making computation practical.

For example, let $n = 2g + 2$, and let U_{aff} be the open subscheme of U consisting of sets of n points on $\mathbb{A}^1$. Now we can define a curve C over U_{aff} whose fiber over the point $a = \{a_1, \ldots, a_n\}$ is the hyperelliptic genus g curve

$$C_a : y^2 = (x - a_1) \ldots (x - a_n).$$

Write $J \xrightarrow{j} U_{aff}$ for the Jacobian of C, which is a g-dimensional abelian scheme over U_{aff}. Let M be a positive integer. Then $J[M]$, the M-torsion subscheme of J, is a finite étale cover of U_{aff}.

The geometric fundamental group $\pi_1(U_{aff} \times_{\mathbb{Q}} \bar{\mathbb{Q}})$ is $\hat{B}_n$, the profinite completion of the Artin braid group. The action of $\hat{B}_n$ on $J[M]$ is linear and preserves the Weil pairing, which is to say that this action yields a homomorphism

$$h'_M : \hat{B}_n \to Sp_{2g}(\mathbb{Z}/M\mathbb{Z}).$$

Let S be the image of the natural injection $S_{2g+2} \hookrightarrow Sp_{2g}(\mathbb{Z}/2\mathbb{Z})$. Then for any even M, the image of h'_M is the preimage of S under the projection $Sp_{2g}(\mathbb{Z}/M\mathbb{Z}) \to Sp_{2g}(\mathbb{Z}/2\mathbb{Z})$. When M is odd, h'_M is surjective [25, Th. 7.3].

Since the cover $J[M] \to U$ is defined over $\mathbb{Q}$, the kernel of h'_M is fixed by the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. It follows that h'_M induces an action of Galois on $Sp_{2g}(\mathbb{Z}/M\mathbb{Z})$, for all odd N. Happily, this action is easy to describe explicitly.

For each $r \in (\mathbb{Z}/M\mathbb{Z})^*$, let A_r be an element of $\mathrm{GSp}_{2g}(\mathbb{Z}/M\mathbb{Z})$ which multiplies the symplectic form by r. If M is even, we require also that the projection of r to $Sp_{2g}(\mathbb{Z}/2\mathbb{Z})$ is trivial. Then conjugation by A_r is a well-defined outer automorphism of the image of h'_M. We denote this outer automorphism by α_r. Note that α_r depends only on the class of r in $(\mathbb{Z}/M\mathbb{Z})^*/[(\mathbb{Z}/M\mathbb{Z})^*]^2$.

Let $\chi_M : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to (\mathbb{Z}/M\mathbb{Z})^*$ be the mod M cyclotomic character.

Proposition 5.4. *The outer action of* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ *on the image of* h'_M *is given by*

$$\sigma \mapsto \alpha_{\chi_M(\sigma)}$$

for all M.

Proof. Let $Y_M \to U_{aff}$ be the Galois closure of $J[M] \to U$. Then a point of Y_M over $a \in U(\mathbb{Q})$ is a certain choice $\mathcal{B}$ of symplectic basis for $J[M]$. This choice of basis identifies the group of deck transformations of $Y_M \to U$ with the image of h'_M. The action of $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ replaces $\mathcal{B}$ by $\gamma\mathcal{B}$, where γ is a matrix in $\mathrm{GSp}_{2g}(\mathbb{Z}/M\mathbb{Z})$ multiplying the symplectic form by $\chi_M(\sigma)$ [18, §16]. If M is

even, we can modify γ by an element of $\mathrm{Sp}_{2g}(\mathbb{Z}/M\mathbb{Z})$ to make the projection of γ onto $\mathrm{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$ trivial.

Now a deck transformation corresponding to the symplectic matrix A with respect to $\mathcal{B}$ is given by the symplectic matrix $\gamma A \gamma^{-1}$ with respect to $\gamma\mathcal{B}$, which proves the desired result. □

We can compose h'_M with the quotient map $\mathrm{Sp}_{2g}(\mathbb{Z}/M\mathbb{Z}) \to \mathrm{Sp}_{2g}(\mathbb{Z}/M\mathbb{Z})/\pm 1$. It is easy to check from the description in Remark 5.6 that the composition factors through $\hat{H}_n$. We thus obtain a map

$$h_M : \hat{H}_n \to \mathrm{Sp}_{2g}(\mathbb{Z}/M\mathbb{Z})/\pm 1$$

which is equivariant for the action of Galois on both sides.

Remark 5.5. If m is a dessin, $h_2 \circ \tilde{m}$ is in fact the composition of m with the natural inclusion $S_{2g+2} \hookrightarrow \mathrm{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$.

It is natural to denote the inverse limit of the h_M by

$$h : \hat{H}_{2g+2} \to Sp_{2g}(\hat{\mathbb{Z}})/\pm 1.$$

Remark 5.6. It is not hard to write h down explicitly by drawing pictures of the action of H_{2g+2} on the homology of a genus g hyperelliptic curve X, branched over points $p_1, \ldots, p_{2g+2}$ in $\mathbb{P}^1$. For $i = 1, \ldots, 2g+1$, let h_i be the homology class of the lift to X of a counterclockwise loop enclosing branch points p_i and p_{i+1}. Then the h_i span $H_1(X, \mathbb{Z})$, and $h_1 + h_3 + \ldots + h_{2g+1} = 0$.

We can then define the $2g \times 2g$ matrix $h(e_i)$ by stipulating that $h(e_i)$ fixes h_j for $j = i$ or $|j - i| > 1$, that $h(e_i)(h_{i-1}) = h_{i-1} - h_i$, and that $h(e_i)(h_{i+1}) = h_{i+1} + h_i$. For example, when $g = 2$, we obtain the 5 matrices

$$h(e_1) = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, h(e_2) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, h(e_3) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$h(e_4) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{bmatrix}, h(e_5) = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Combining Proposition 5.3 and Proposition 5.4, we obtain the following invariant of dessins d'enfants.

Proposition 5.7. *If m and m' are conjugate by a Galois element σ, then the subgroups $h(BM(m))$ and $h(BM(m'))$ of $Sp_{2g}(\hat{\mathbb{Z}})/\pm 1$ are related by an outer automorphism $\alpha_{\chi(\sigma)}$.*

Remark 5.8. Suppose m sends x_∞ to an n-cycle, so that one can (and does) choose the corresponding Belyi map β to be a polynomial. Define a hyperelliptic curve

$$C_t/\bar{\mathbb{Q}}(t) : y^2 = \beta(x) - t.$$

Then $h(BM(m))$ is nothing more than the image of the action of $\mathrm{Gal}(\overline{\mathbb{Q}(t)}/\bar{\mathbb{Q}}(t))$ on the étale cohomology $H^1(C_t, \hat{\mathbb{Z}})$. Note that this definition makes sense even when the degree of β is odd. In the situation where β is a polynomial, our map

$$\tilde{\beta} : \mathbb{P}^1 - \{0, 1, \infty\} \to U$$

factors through U_{aff}, so we can define a map

$$\tilde{m} : \Pi \to \hat{B}_n$$

Now if $n = 2g + 1$ is odd, the natural inclusion $\hat{B}_n \to \hat{B}_{n+1}$ is Galois-equivariant, so we can define $h(BM(m))$ to be the image of the composition

$$\Pi \stackrel{\tilde{m}}{\to} \hat{B}_{2g+1} \to \hat{B}_{2g+2} \stackrel{h'}{\to} Sp_{2g}(\mathbb{Z}).$$

Examples

Example 5.9. We have already computed the braids $\tilde{m}(x_0)$ and $\tilde{m}(x_1)$ for the dessin m pictured in Figure 2. Using the presentation for h from Remark 5.6, one has

$$h(\tilde{m}(x_0)) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & 1 \end{bmatrix}, h(\tilde{m}(x_1) = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Using the computer program `GAP`, one can compute readily that the images of these matrices generate the whole of $Sp_{2g}(\mathbb{Z}/p\mathbb{Z})/\pm 1$, where $p = 3, 5$, or 7.

Unfortunately, the groups $\mathrm{Sp}_{2g}(\mathbb{Z}/M\mathbb{Z})/\pm 1$ grow very rapidly in g, making it difficult in practice to compute the subgroup $h(BM(m))$ when the dessin has more than a few edges. In practice, we have found that $h_M(BM(m))$ is almost always the whole of $\mathrm{Sp}_{2g}(\mathbb{Z}/M\mathbb{Z})/\pm 1$, where M is a small prime. One might wonder whether there are even any examples of dessins m such that $h_p(BM(m))$ is a proper subgroup of $\mathrm{Sp}_{2g}(\mathbb{Z}/p\mathbb{Z})/\pm 1$ for $p > 2$. Certainly one can construct examples by choosing M to be a non-primitive permutation representation of Π. However, even primitive m can yield small braid monodromy groups, as the following example shows.

Example 5.10. Let $p > 2$ be a prime, and let m be the dessin d'enfant defined by

$$\begin{aligned} m(x_0) &= (1,2)(3,4)\ldots(p-2,p-1) \\ m(x_1) &= (2,3)(4,5)\ldots(p-1,p). \end{aligned}$$

The corresponding Belyi map β is a projective linear transformation of a Tchebysheff polynomial. Since m has prime degree, it is primitive. On the other hand, the hyperelliptic curve

$$C_t/\bar{\mathbb{Q}}(t) : y^2 = \beta(x) - t$$

has real multiplication by the subfield of index 2 in $\mathbb{Q}(\zeta_p)$ [24, 5], possibly after some finite extension of the base $\bar{\mathbb{Q}}(t)$. Let $A \in \mathrm{Sp}_{2g}(\hat{\mathbb{Z}})$ be the image of the action of $\mathrm{End}(C_t \times \overline{\mathbb{Q}(t)})$ on $H^1(C_t \times \overline{\mathbb{Q}(t)}, \hat{\mathbb{Z}})$.

Then some finite-index subgroup of $h(BM(m))$ commutes with A, whence $h_M(BM(m))$ is a proper subgroup of $\mathrm{Sp}_{2g}(\mathbb{Z}/M\mathbb{Z})/\pm 1$ for all sufficiently large M. (Here we are defining $h(BM(m))$ as in Remark 5.8.)

Note that in this case the monodromy group $\mathrm{Mon}(m)$ is dihedral, which suggests the following problem.

Problem 2: Find a degree d dessin d'enfant such that $\mathrm{Mon}(m) = S_d$, but $h_M(BM(m))$ is a proper subgroup of $\mathrm{Sp}_{2g}(\mathbb{Z}/\hat{M}\mathbb{Z})/\pm 1$ for some odd M.

Example 5.11. Consider surjective homomorphisms

$$n : \Pi \to Sp_{2g}(\mathbb{Z}/5\mathbb{Z})$$

such that

$$n(x_0) \sim \begin{bmatrix} 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & 1 \end{bmatrix}, n(x_1) \sim \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}, n(x_\infty) \sim \begin{bmatrix} -1 & -2 & 1 & 0 \\ 1 & 1 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 1 & 0 & 0 \end{bmatrix}.$$

Using `GAP`, we find that there are 13 such dessins; by definition, each of these dessins has the same Nielsen class and monodromy group. However, we can see that these dessins do not form a Galois conjugacy class. Exactly one of the 13 choices of n lies over the homomorphism

$$\bar{n} = h_5 \circ \tilde{m} : \Pi \to Sp_{2g}(\mathbb{Z}/5\mathbb{Z})/\pm 1,$$

where m is the 6-edge dessin of Example 5.9. Fix this choice of n.

Since m is defined over $\mathbb{Q}$, it follows from Propositions 4.1 and 5.4 that

$$\bar{n}^\sigma = \alpha(\chi_5(\sigma)) \circ \bar{n}.$$

In particular, $\bar{n}$, whence also n, is defined over $\mathbb{Q}(\sqrt{5})$.

$\widehat{GT}$ and braid monodromy

Drinfel'd [4] discovered that the Grothendieck-Teichmüller group acted as a group of outer automorphisms of the pro-unipotent completion of the Artin braid group; Ihara and Matsumoto [13] showed that Drinfel'd's construction also yielded outer actions of $\widehat{GT}$ on $\hat{B}_n$ and $\hat{H}_n$. They also prove that this action extends the natural $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-action α_b on $\hat{H}_n$. We may therefore write $\alpha_b(\sigma)$ for the outer automorphism of $\hat{H}_n$ associated to $\sigma \in \widehat{GT}$.

It is thus natural for us to ask whether the braid invariant defined here is invariant not only under the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, but under all of $\widehat{GT}$.

Question 3: Let m be a genus 0 dessin d'enfant, and let σ be an element of $\widehat{GT}$.
Is it true that

$$\widetilde{m^\sigma} = \alpha_b(\sigma^{-1}) \circ \tilde{m} \circ \alpha(\sigma)$$

for all $\sigma \in \widehat{GT}$?

Note that Question 3 can have a positive answer only if the action of $\widehat{GT}$ preserves rational twine classes in $\hat{H}_n$. This weaker question seems interesting in its own right.

Question 4: Let $\tilde{\mathbf{c}}$ be a twine class in $\hat{H}_n$. Is it true that

$$\tilde{\mathbf{c}}^\sigma = \tilde{\mathbf{c}}^{\chi(\sigma)} \tag{5.3}$$

for all $\sigma \in \widehat{GT}$?

It is immediate from the definition of the action of $\widehat{GT}$ on $\hat{H}_n$ that the answer to Question 4 is yes if $\tilde{\mathbf{c}}$ is the conjugacy class of e_1. It follows from a result of Lochak and Schneps [16] that (5.3) is also satisfied when $\tilde{\mathbf{c}}$ is the class of e_1e_2.

For the proof, we need to introduce some basic facts and notation about the Grothendieck-Teichmüller group. Each element $\sigma \in \widehat{GT}$ can be written as (λ, f), where $\lambda = \chi(\sigma) \in \hat{\mathbb{Z}}$ and $f \in [\Pi, \Pi]$. If x, y, z are elements of a group G with $xyz = 0$, we denote by $f(x, y)$ the image of f under the homomorphism $\Pi \to G$ sending x_0 to x and x_1 to y. Let $\widehat{GT}^1$ be the kernel of the cyclotomic character χ of $\widehat{GT}$.

Then elements of $\widehat{GT}^1$ satisfy the relations

$$f(x_0, x_1)f(x_1, x_0) = 1$$

and

$$f(x_\infty, x_0)f(x_1, x_\infty)f(x_0, x_1) = 1.$$

We are now ready to prove that $\widehat{GT}$ preserves the rational twine class containing e_1e_2.

Proposition 5.12. *For all $\sigma = (\lambda, f) \in \widehat{GT}$,*

$$(e_1e_2)^\sigma \sim (e_1e_2)^\lambda$$

in $\hat{H}_n$.

Proof. We will prove the slightly stronger theorem that the conjugacy above is valid in $\hat{B}_n$. From [13], we have

$$(e_1e_2)^\sigma = e_1^\lambda f(e_1^2, e_2^2)^{-1} e_2^\lambda f(e_1^2, e_2^2). \tag{5.4}$$

for any n. It suffices to prove that (5.4) is conjugate to $(e_1e_2)^\lambda$ in $\hat{B}_3$.

Lemma 5.13. *The statement of the proposition holds whenever $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.*

Proof. The group $\hat{B}_3$ is the geometric fundamental group of the variety U_{aff} defined in Section 5, with $n = 3$. We may think of U_{aff} as the variety of cubic polynomials with non-vanishing discriminant, defined up to scalar multiplication. Now the map $t \to x^3 - t$ yields a morphism $\mathbb{P}^1 - \{0, 1, \infty\} \to U_{aff}$; since this map is defined over $\mathbb{Q}$, the resulting map of geometric fundamental groups

$$m : \Pi \to \hat{B}_3$$

is equivariant for the action of $\mathbb{Q}$ on both sides. Passing to complex manifolds, we see that $m(x_0) = e_1e_2$. Since $x_0^\sigma \sim x_0^{\chi(\sigma)}$ in Π, we have that $(e_1e_2)^\sigma \sim (e_1e_2)^{\chi(\sigma)}$ in $\hat{B}_3$. □

Choose $\sigma = (\lambda, f) \in \widehat{GT}$ and choose $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ with $\chi(\tau) = \lambda$. Then

$$[(e_1e_2)^\sigma] = [(e_1e_2)^\tau]^{(\sigma\tau^{-1})} = [(e_1e_2)^\lambda]^{(\sigma\tau^{-1})} = [(e_1e_2)^{\sigma\tau^{-1}}]^\lambda.$$

It thus suffices to verify the proposition for $\sigma \in \widehat{GT}^1$.

We now work in the quotient of $\hat{B}_3$ by its center, which is the pro-cyclic group generated by $(e_1e_2)^3$. Define $x = e_1^2, y = e_2^2$, and $z = e_2^{-2}e_1^{-2} = e_2^{-1}e_1^2e_2$. Then $xyz = 0$, and one finds

$$(e_1e_2)x(e_1e_2)^{-1} = y, (e_1e_2)y(e_1e_2)^{-1} = z, (e_1e_2)z(e_1e_2)^{-1} = x.$$

So we have

$$\begin{aligned}(e_1e_2)^\sigma &= e_1f(x,y)^{-1}e_2f(x,y)\\ &= e_1e_2f(z,y)^{-1}f(x,y)\\ &= e_1e_2f(y,z)f(x,y)\\ &= e_1e_2f(z,x)^{-1}.\end{aligned}$$

We now invoke a theorem of Lochak and Schneps [16, Th. 2, II'], which tells us that

$$f(z,x) = h(x,y)^{-1}h(z,x)$$

for some $h \in \Pi$. So

$$(e_1e_2)^\sigma = e_1e_2h(z,x)^{-1}h(x,y) = h(x,y)^{-1}e_1e_2h(x,y).$$

Lifting back to $\hat{B}_3$, we find that

$$(e_1e_2)^\sigma = wh(x,y)^{-1}e_1e_2h(x,y)$$

for some w in the center of $\hat{B}_3$. But w clearly lies in the commutator of $\hat{B}_3$, and the intersection of the commutator and the center of $\hat{B}_3$ is trivial. So $w = 1$, which proves the desired result. □

References

[1] J. Betrema. `http://dept-info.labri.u-bordeaux.fr/~betrema/arbres/index.html`.

[2] J. Birman. *Braids, links, and mapping class groups.* Number 82 in Ann. of Math. Studies. Princeton Univ. Press, 1974.

[3] P. Deligne. Le groupe fondmental de la droite projective moins trois points. In Ihara et al. [14], pages 79–297.

[4] V.G. Drinfel'd. On quasitriangular quasi-Hopf algebras and a group closely connected with $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. *Leningrad Math. J.*, 2:829–860, 1991.

[5] J. Ellenberg. Endomorphism algebras of Jacobians. Preprint.

[6] M. Fried. Introduction to modular towers. In Fried [7], pages 111–171.

[7] M. Fried, editor. *Recent Developments in the Inverse Galois Problem.* Number 186 in Contemp. Math. American Mathematical Society, 1995.

[8] M. Fried. Topics in Galois theory. In Fried [7], pages 15–32.

[9] M. Fried and R. Biggers. Moduli spaces of covers and the Hurwitz monodromy group. *J. Reine Angew. Math.*, 335:87–121, 1982.

[10] A. Grothendieck. Esquisse d'un programme. In Schneps and Lochak [21], pages 5–48.

[11] D. Harbater and L. Schneps. Fundamental groups of moduli and the Grothendieck-Teichmüller group. *Trans. Amer. Math. Soc.*, 352(7):3117–3148, 2000.

[12] Y. Ihara. Braids, Galois groups, and some arithmetic functions. In *Proceedings of the ICM (Kyoto, 1990)*, pages 99–120. Math. Soc. Japan, 1991.

[13] Y. Ihara and M. Matsumoto. On Galois actions on profinite completions of braid groups. In Fried [7], pages 173–200.

[14] Y. Ihara, K. Ribet, and J.-P. Serre, editors. *Galois groups over* $\mathbb{Q}$, volume 16 of *MSRI Publications*. Springer-Verlag, 1989.

[15] G. Jones and M. Streit. Galois groups, monodromy groups, and cartographic groups. In Schneps and Lochak [22], pages 25–65.

[16] P. Lochak and L. Schneps. A cohomological interpretation of the Grothendieck-Teichmüller group. *Invent. Math.*, 127(3):571–600, 1997. With an appendix by C. Scheiderer.

[17] G. Malle and B.H̃. Matzat. *Inverse Galois Theory*. Springer-Verlag, 1999.

[18] J.S. Milne. Abelian varieties. In *Arithmetic Geometry*. Springer-Verlag, 1986.

[19] L. Schneps, editor. *The Grothendieck theory of dessins d'enfants*. Number 200 in London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, 1994.

[20] L. Schneps. The Grothendieck-Teichmüller group $\widehat{GT}$: a survey. In Schneps and Lochak [21], pages 183–203.

[21] L. Schneps and P. Lochak, editors. *Geometric Galois actions: 1. Around Grothendieck's Esquisse d'un Programme*. Number 242 in London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, 1997.

[22] L. Schneps and P. Lochak, editors. *Geometric Galois actions: 2. The inverse Galois problem, moduli spaces and mapping class groups*. Number 243 in London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, 1997.

[23] J.-P. Serre. Revêtements à ramification impaire et thêta-caractéristiques. *C.R. Acad. Sci. Paris*, 311(9):547–552, 1990.

[24] W. Tautz, J. Top, and A. Verberkmoes. Explicit hyperelliptic curves with real multiplication and permutation polynomials. *Canad. J. Math.*, 43(5):1055–1064, 1991.

[25] J.-K. Yu. Toward a proof of the Cohen-Lenstra conjecture in the function field case. Preprint.

[26] L. Zapponi. The arithmetic of prime degree trees. Preprint.