# Approximating Galois orbits of dessins

David Harbater* and Leila Schneps**

## §0. Introduction

Let $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. In this paper we study Belyi's action of $G_{\mathbb{Q}}$ on $\pi_1(\mathbb{P}^1 - \{0, 1, \infty\})$ on the level of finite covers . We show that this action can be made effective in terms of the natural outer action on $\pi_1$, and that this outer action can itself be approximated so as to obtain information about Galois orbits and fields of moduli of covers and dessins. We begin with some background and motivation, and then describe the structure of the paper.

**0.1. Background and motivation.** In the theory of branched covers of curves, the action of the arithmetic Galois group on the geometric Galois group is both important and mysterious, and provides a link between number theory and topology. This link arises from the fact that topological covering spaces over a punctured Riemann sphere can be defined as covers of algebraic curves, and that the covers are even arithmetic if the branch locus consists of points defined over $\overline{\mathbb{Q}}$. Namely, as Grothendieck showed [G], such a cover can be defined over $\overline{\mathbb{Q}}$ (and hence over some number field), and the same is true for $G$-Galois covers. If we fix an algebraic branch locus, then we may first ask how the absolute Galois group $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the set of such covers, and secondly ask what the field of moduli of such a cover is. In the $G$-Galois case, if $G$ has trivial center (and in certain other cases), the cover is defined over its field of moduli, so the latter question is equivalent to asking for the minimum field of definition $K$. That in turn has applications to the Inverse Galois Problem, via Hilbert's Irreducibility Theorem — for then $G$ is a Galois group over $K(t)$ and hence over $K$.

These questions can be made more explicit by rephrasing the situation in terms of group theory. Let $P_1, \ldots, P_r \in \mathbb{P}^1_{\overline{\mathbb{Q}}}$ be $r$ distinct points, and let $P_0 \in \mathbb{P}^1 - \{P_1, \ldots, P_r\}$ be a base point. Then we may choose a homotopy basis of counterclockwise loops $\gamma_i$ at $P_0$ around $P_i$ such that $\prod \gamma_i \sim 1$. To give a $G$-Galois cover branched at points $P_1, \ldots, P_r$ is then equivalent to giving its branch cycle description, i.e. an $r$-tuple of generators $(g_1, \ldots, g_r)$ of $G$ such that $\prod g_i = 1$, determined up to uniform conjugacy (corresponding to the choice of base point on the cover over $P_0$). The first question above

* Department of Mathematics, University of Pennsylvania, Philadelphia, PA 19104

** Faculté des Sciences, Université de Franche-Comté, 25030 Besançon Cedex

then becomes the problem of determining how $G_{\mathbb{Q}}$ acts on the set of such equivalence classes of $r$-tuples (e.g. by giving a formula for the action of $\sigma \in G_{\mathbb{Q}}$ on the set of branch cycle descriptions). Solving this would then answer the second question as well, since the field of moduli of a cover would be the fixed field of the stabilizer of the branch cycle description. We would thus like to have a "formula" for the field of moduli in terms of the branch cycles $g_i$. (The non-Galois case can be interpreted similarly, in terms of $r$-tuples of elements in an appropriate $S_n$, but for simplicity we focus on the Galois case here.)

Using his "branch cycle argument," Fried (cf. [F1]) showed a *branch cycle condition* that gives a weak form of the desired formula for the action of $G_{\mathbb{Q}}$. Namely, if each $P_i$ is defined over $K \subset \overline{\mathbb{Q}}$, and if $\sigma \in G_K$, then the branch cycle description $(g'_1, \ldots, g'_r)$ of $Y^\sigma \to \mathbb{P}^1$ satisfies the relation $g'_i \sim g_i^{\chi(\sigma)}$. (Here $\chi$ is the cyclotomic character and $\sim$ denotes conjugacy in $G$). More generally, if the branch locus is defined over $K \subset \overline{\mathbb{Q}}$ (but the individual $P_i$'s are not necessarily defined over $K$), then $g'_j \sim g_i^{\chi(\sigma)}$ if $\sigma(P_i) = P_j$.

Later, Belyi [B] considered the case of $r = 3$, where we may take $P_1 = 0$, $P_2 = 1$, $P_3 = \infty$. By considering the special case now known as "rigidity" (and treated independently, about the same time, by Matzat [M] and Thompson [T]), he showed that for certain triples the branch cycle condition $g'_i \sim g_i^{\chi(\sigma)}$ determines the field of moduli — and thus many simple groups can be realized as Galois groups over $\mathbb{Q}^{\mathrm{ab}}$ (or even over $\mathbb{Q}$, in some cases). Also, he showed that for a given $\sigma \in G_{\mathbb{Q}}$, there is a unique $f_\sigma \in \widehat{F}'_2$ (the commutator subgroup) such that $\sigma$ takes each triple $(g_1, g_2, g_3)$ to an expression of the form $(g_1^{\chi(\sigma)}, f_\sigma^{-1} g_2^{\chi(\sigma)} f_\sigma, \tilde{g}_3^{\chi(\sigma)})$ (for some $\tilde{g}_3 \sim g_3$). This provides a lifting of the natural map $G_{\mathbb{Q}} \to \mathrm{Out}(\widehat{F}_2)$ to a homomorphism $G_{\mathbb{Q}} \to \mathrm{Aut}(\widehat{F}_2)$. Moreover he showed a converse to Grothendieck's theorem, viz. that for every curve $Y$ defined over $\overline{\mathbb{Q}}$ there is a covering map $Y \to \mathbb{P}^1$ that is branched only over $\{0, 1, \infty\}$ — and hence $G_{\mathbb{Q}}$ acts faithfully on the set of étale covers of $\mathbb{P}^1 - \{0, 1, \infty\}$.

In the *Esquisse d'un Programme*, motivated in part by Belyi, Grothendieck suggested studying $G_{\mathbb{Q}}$ as a group of outer automorphisms of $\mathbb{P}^1 - \{0, 1, \infty\}$. More generally, he suggested viewing $G_{\mathbb{Q}}$ as a group of outer automorphisms of the groups $\widehat{K}(g, n) = \pi_1(\mathcal{M}_{g,n})$, where $\mathcal{M}_{g,n}$ is the moduli space of curves of genus $g$ with $r$ ordered marked points, and then trying to understand the outer action on $\widehat{K}(g, n)$ in terms of the one on $\widehat{K}(0, 4) = \widehat{F}_2$ (where $\mathcal{M}_{0,4} = \mathbb{P}^1 - \{0, 1, \infty\}$). In particular, he suggested that the action on the full "Teichmüller tower" of $\widehat{K}(g, n)$'s can be understood in terms of $\widehat{K}(0, 4)$, $\widehat{K}(1, 1)$, $\widehat{K}(0, 5)$, and $\widehat{K}(1, 2)$ (where the actions on the first two would provide the generators of the tower and the second two the relations). In addition, he showed how covers of $\mathbb{P}^1 - \{0, 1, \infty\}$ can be classified not

only by equivalence classes of triples, but also by "dessins d'enfants", which encode the same information graphically.

Since the action of an element $\sigma \in G_{\mathbb{Q}}$ is given by $\lambda_\sigma = \chi(\sigma) \in \hat{\mathbb{Z}}^*$ and $f_\sigma \in \widehat{F}_2'$ (as in [B]), the above involves characterizing the pairs $(\lambda, f) \in \hat{\mathbb{Z}}^* \times \widehat{F}_2'$ that arise from elements of $G_{\mathbb{Q}}$, and characterizing the actions of elements $\sigma \in G_{\mathbb{Q}}$ on the tower of $\widehat{K}(g,n)$'s in terms of $\lambda_\sigma$ and $f_\sigma$. Such characterizations would give an explicit description of $G_{\mathbb{Q}}$ as a subgroup of the outer automorphism group of $\widehat{K}(g,n)$, and in particular of $\widehat{K}(0,4) = \widehat{F}_2'$.

Some progress was made on the first point by the discovery of three necessary conditions for a pair $(\lambda, f) \in \hat{\mathbb{Z}}^* \times \widehat{F}_2$ to come from $G_{\mathbb{Q}}$. These properties come from work of Drinfel'd (cf. [D]), where he defined the Grothendieck-Teichmüller group $\widehat{GT}$ as a certain subgroup of $\mathrm{Aut}(\widehat{F}_2)$ (constructed in terms of "quasi-triangular quasi-Hopf algebras") that contains the image of $G_{\mathbb{Q}}$ under the Belyi lifting. Later, Ihara reinterpreted the inclusion of $G_{\mathbb{Q}}$ in $\widehat{GT}$ in terms of $\mathcal{M}_{0,4}$ and $\mathcal{M}_{0,5}$, braid groups, and "pro-loops" (cf. [I1], [I2]). The elements of $\widehat{GT}$ are automorphisms corresponding to pairs $(\lambda, f) \in \hat{\mathbb{Z}}^* \times \widehat{F}_2'$ satisfying a certain 2-cocycle condition (I), a 3-cocycle condition (II), and a 5-cocycle condition (III) (see the survey on $\widehat{GT}$ in this volume for details). The group $\widehat{GT}$ can be identified with the automorphism group of a tower of profinite Artin braid groups $\widehat{B}_n$; cf. [LS].

On the second point, Nakamura recently showed explicitly for $g \geq 1$ and $n = 0$ or 1, how the action of any $\sigma \in G_{\mathbb{Q}}$ on $\widehat{K}(g,n)$ can be expressed in terms of the action on $\widehat{K}(0,4)$. For $\widehat{K}(0,4) = \widehat{F}_2 = \langle x, y, z \mid xyz = 1 \rangle$, Belyi's action can be written more explicitly as

$$\sigma : x \mapsto x^\lambda,\ y \mapsto (y^\lambda)^{f(x,y)},\ z \mapsto (z^\lambda)^{f(x,z)x^{-m}}, \qquad (*)$$

where $\lambda = \lambda_\sigma = \chi(\sigma) \in \hat{\mathbb{Z}}^*$, $f = f_\sigma \in \widehat{F}_2'$, $m = (\lambda - 1)/2 \in \hat{\mathbb{Z}}$, and $u^v := v^{-1}uv$ for $u, v \in \widehat{F}_2$. In [N, Appendix], Nakamura described an analogue of Belyi's lifting that provides an action of $G_{\mathbb{Q}}$ on the group $\widehat{K}(0,5)$ (which is generated by elements $x_{i,i+1}$ for $i$ modulo 5) by

$$\sigma : x_{12} \mapsto x_{12}^\lambda,\ x_{23} \mapsto (x_{23}^\lambda)^{f(x_{12},x_{23})},\ x_{34} \mapsto (x_{34}^\lambda)^{f(x_{45},x_{34})},$$
$$x_{45} \mapsto x_{45}^\lambda,\ x_{51} \mapsto (x_{51}^\lambda)^{f(x_{45},x_{51})f(x_{12},x_{23})}, \qquad (**)$$

where $\lambda, f$ are as above. In his contribution to this volume, he discovered a similar formula for the action of $G_{\mathbb{Q}}$ on $\widehat{K}(g,0)$ and $\widehat{K}(g,1)$, with $g \geq 0$.

**0.2. Structure of the paper.** In the present paper, we continue the examination of $G_{\mathbb{Q}}$ and $\widehat{GT}$ as groups of outer automorphisms of the fundamental groups $\widehat{K}(0,n)$ of the moduli spaces $\mathcal{M}_{0,n}$, and the related problem of finding a "formula" for the action of $\sigma \in G_{\mathbb{Q}}$ on covers — i.e. finding $f_\sigma$ in terms of $\sigma$, at least on finite levels. We break this problem into two parts.

In §1 we treat the first half of this problem, viz. showing that the Belyi lifting $G_{\mathbb{Q}} \to \mathrm{Aut}(\widehat{F}_2)$ can be made "effective" in terms of the natural map $G_{\mathbb{Q}} \to \mathrm{Out}(\widehat{F}_2)$. That is, for every normal subgroup $N \subset \widehat{F}_2$ of finite index, we show that there is a finite index normal subgroup $\tilde{N} \subset \widehat{F}_2$ such that the Belyi lifting modulo $N$ can be computed in terms of the outer action of $G_{\mathbb{Q}}$ modulo $\tilde{N}$. Moreover we show how $\tilde{N}$ can be found explicitly in terms of $N$, and interpret this in terms of computing the action of $G_{\mathbb{Q}}$ on covers of $\mathbb{P}^1 - \{0, 1, \infty\}$. In §2 we prove analogous results for $\widehat{K}(0, 5)$. A basic ingredient is the definition (in 1.1) of a certain group $\mathcal{O}_n^{\#}$ of symmetric outer automorphisms of $\widehat{K}(0, n)$.

The second half of the problem, i.e. explicitly computing the outer action of a given $\sigma \in G_{\mathbb{Q}}$, remains open. In §3 we obtain partial results in this direction, which compute the $\widehat{GT}$-orbit of a dessin — thus approximating the $G_{\mathbb{Q}}$-orbit — and also yield information about the field of moduli of a dessin (or corresponding cover). This is achieved by using the result (cf. [HS]) that $\widehat{GT} \simeq \mathcal{O}_5^{\#}$, and by considering the image of $\mathcal{O}_5^{\#}$ in $\mathrm{Out}(\widehat{K}(0, 5)/N)$ for characteristic subgroups $N \subset \widehat{K}(0, 5)$ of finite index.

## §1. The Belyi lifting and four-point moduli

Let $F_2$ be the free group on two generators $x$ and $y$, which is the topological fundamental group of $\mathbb{P}^1 - \{0, 1, \infty\}$ (based at some point), with $x$ and $y$ being counterclockwise loops around 0 and 1 respectively. Let $\hat{F}_2$ be its profinite completion, which we identify with the algebraic fundamental group of $\mathbb{P}^1 - \{0, 1, \infty\}$ (with the same base point), and hence with $\widehat{K}(0, 4)$. Let $\widehat{F}_2'$ denote its commutator subgroup, and consider the *Belyi subgroup* $A \subset \mathrm{Aut}(\widehat{F}_2)$, defined (as in [B]) by

$$A = \big\{ F \in \mathrm{Aut}(\widehat{F}_2) \mid \exists \lambda \in \hat{\mathbb{Z}}^*, f \in \widehat{F}_2' \text{ such that } F(x) = x^{\lambda},\ F(y) = f^{-1} y^{\lambda} f,\ F(xy) \sim (xy)^{\lambda} \big\},$$

where $\sim$ denotes conjugacy in $\widehat{F}_2$. Giving $F \in A$ determines the pair $(\lambda, f)$ uniquely, so $A$ may also be regarded as a subset of $\hat{\mathbb{Z}}^* \times \widehat{F}_2'$, which is how we consider it henceforth.

Since any $\sigma \in G_{\mathbb{Q}}$ must take the full tower of finite covers (regarded as the "pro-universal cover" of $\mathbb{P}^1 - \{0, 1, \infty\}$) to itself, there is a natural map $\alpha : G_{\mathbb{Q}} \to \mathrm{Out}(\widehat{F}_2)$. Using that the centralizers of $x$ and $y$ are respectively the pro-cyclic subgroups $\langle x \rangle$ and $\langle y \rangle$, Belyi deduced that $\alpha$ may be lifted to a homomorphism $\beta : G_{\mathbb{Q}} \to A \subset \mathrm{Aut}(\widehat{F}_2)$. The map $\beta$, known as the *Belyi lifting*, corresponds to a section of the fundamental exact sequence

$$1 \to \widehat{F}_2 \to \pi_1(\mathbb{P}^1_{\mathbb{Q}} - \{0, 1, \infty\}) \to G_{\mathbb{Q}} \to 1$$

obtained via a certain *tangential base point* for $\pi_1$ (cf. [IM]).

The goal of this section is to show that the Belyi lifting $\beta : G_{\mathbb{Q}} \to \mathrm{Aut}(\widehat{F}_2)$ is effective in terms of the natural map $\alpha : G_{\mathbb{Q}} \to \mathrm{Out}(\widehat{F}_2)$. We describe our approach to this in 1.2 below; before that, we need to define some important subgroups of the automorphism and outer automorphism groups of the pure mapping class groups $\widehat{K}(0,n) = \pi_1(\mathcal{M}_{0,n})$. (For basic facts about $\widehat{K}(0,n)$, cf. section 1.1 of the survey on $\widehat{GT}$ in this volume.)

**1.1. Symmetric automorphisms of pure mapping class groups.** For each $n$, the symmetric group $S_n$ acts on the moduli space $\mathcal{M}_{0,n}$ by permuting the order of the marked points. For $n = 4$, the automorphism group of $\mathcal{M}_{0,4} = \mathbb{P}^1 - \{0, 1, \infty\}$ is $S_3$, and the map $\sigma^{(4)} : S_4 \to \mathrm{Aut}(\mathcal{M}_{0,4})$ is surjective with kernel equal to the even involutions in $S_4$ (which form a Klein four group). On the other hand, for $n > 4$, the map $S_n \to \mathrm{Aut}(\mathcal{M}_{0,n})$ is an isomorphism. For all $n$, the map $S_n \to \mathrm{Aut}(\mathcal{M}_{0,n})$ induces a homomorphism $\sigma^{(n)} : S_n \to \mathrm{Out}(\widehat{K}(0,n))$, which again is injective for $n > 4$ and has Klein four kernel if $n = 4$. (In fact, by a version of Grothendieck's anabelian conjecture — see the article by Ihara and Nakamura in this volume — the image of this homomorphism is exactly the subgroup of $\mathrm{Out}(\widehat{K}(0,n))$ that commutes with the natural outer action of $G_{\mathbb{Q}}$ on $\widehat{K}(0,n)$.)

For any group $G$, the outer automorphism group $\mathrm{Out}(G)$ acts on the set of conjugacy classes $[g]$ of elements of $G$, and we may make the following

**Definition.** For all $n \geq 4$, let $\mathcal{O}_n^{\#}$ be the subgroup of outer automorphisms $\overline{F} \in \mathrm{Out}\big(\widehat{K}(0,n)\big)$ such that

(i) for each $i, j$, we have $\overline{F}([x_{ij}]) = [x_{ij}^{\lambda}]$ for some $\lambda \in \hat{\mathbb{Z}}^*$;

(ii) $\overline{F}$ commutes with $\sigma^{(n)}(S_n)$ in $\mathrm{Out}(\widehat{K}(0,n))$.

Note that for $\overline{F} \in \mathcal{O}_n^{\#}$, the value of $\lambda$ is independent of $i, j$ by the symmetry condition (ii); so we may write $\lambda = \lambda(\overline{F})$. Let $\mathcal{A}_n^{\#}$ denote the inverse image of $\mathcal{O}_n^{\#}$ under the natural map $\mathrm{Aut}(\widehat{K}(0,n)) \to \mathrm{Out}(\widehat{K}(0,n))$, and write $\lambda(F) = \lambda(\overline{F})$ if $F \in \mathcal{A}_n^{\#}$ maps to $\overline{F} \in \mathcal{O}_n^{\#}$. A key fact [HS, 1.2] is that the image of the natural map $G_{\mathbb{Q}} \hookrightarrow \mathrm{Out}(\widehat{K}(0,n))$ is contained in $\mathcal{O}_n^{\#}$.

In this section, we restrict attention to the case $n = 4$, identifying $\widehat{K}(0,4)$ with $\widehat{F}_2$ via $x_{12} = x$ and $x_{23} = y$, and viewing $\mathcal{O}_4^{\#} \subset \mathrm{Out}(\widehat{F}_2)$ and $\mathcal{A}_4^{\#} \subset \mathrm{Aut}(\widehat{F}_2)$. Since $\beta : G_{\mathbb{Q}} \hookrightarrow \mathrm{Aut}(\widehat{F}_2)$ lifts $\alpha : G_{\mathbb{Q}} \hookrightarrow \mathrm{Out}(\widehat{F}_2)$ and since $\alpha(G_{\mathbb{Q}}) \subset \mathcal{O}_4^{\#}$, we have that $\beta(G_{\mathbb{Q}}) \subset \mathcal{A}_4^{\#}$. Our explicit description below of $\beta$ in terms of $\alpha$ will be based on the following result, which is essentially well-known (cf. [IM]), but is explicitly proved in this form in [HS, 1.2].

**Theorem 1.** *There is a unique section $s$ of the natural homomorphism $\mathcal{A}_4^{\#} \to \mathcal{O}_4^{\#}$ whose image lies in the Belyi subgroup $A$ of $\mathrm{Aut}(\widehat{F}_2)$. This section satisfies $\beta = s\alpha : G_{\mathbb{Q}} \hookrightarrow \mathrm{Aut}(\widehat{F}_2)$.*

**1.2. Explicit computation of the Belyi lifting.** Our goal in §1 is to compute $\beta$ explicitly in terms of $\alpha$, on the level of finite covers. That is, we will show that for any normal subgroup $N \subset \widehat{F}_2$ of finite index, there is a smaller such subgroup $\tilde{N}$ — which we determine explicitly — such that the reduction of $\beta$ modulo $N$ is determined by that of $\alpha$ modulo $\tilde{N}$.

Our approach to this is to use Theorem 1, and the section $s$ of $\mathcal{A}_4^\# \to \mathcal{O}_4^\#$. We show that $s$ is effectively computable, in the sense that $s(\overline{F})$ modulo $N$ is determined by $\overline{F}$ modulo $\tilde{N}$, where $\tilde{N}$ depends only on $N$ (and not on $\overline{F}$). The computation of $\beta$ in terms of $\alpha$ then follows from the relation $\beta = s\alpha$.

The rest of §1 is thus devoted to finding an $\tilde{N}$ for each $N$, and describing how to compute $s(\overline{F})$ modulo $N$ in terms of $\overline{F}$ modulo $\tilde{N}$ — and hence $\beta$ modulo $N$ in terms of $\alpha$ modulo $\tilde{N}$. First, we need to define these reductions of $\alpha$ and $\beta$.

Let $\Gamma$ be the set of normal subgroups $N$ of finite index in $\widehat{F}_2$. For each $N \in \Gamma$, consider the quotient group $G_N = \widehat{F}_2/N$. Then giving the quotient map $\widehat{F}_2 \twoheadrightarrow G_N$ is equivalent to giving a triple $(a, b, c)$ of generators of $G_N$ such that $abc = 1$, corresponding (via Riemann's Existence Theorem) to a pointed $G_N$-Galois cover $X \to \mathbb{P}^1_{\mathbb{Q}} - \{0, 1, \infty\}$. The set of equivalence classes of such triples (under uniform conjugacy) can be identified with the set of isomorphism classes of $G_N$-Galois dessins, each corresponding to a $G_N$-Galois cover $X \to \mathbb{P}^1_{\mathbb{Q}} - \{0, 1, \infty\}$.

For $N \in \Gamma$, the action of $G_{\mathbb{Q}}$ on $G_N$-Galois covers lifts to an action on the set of triples $\{(a, b, c) \,|\, a, b, c \text{ generate } G_N,\ abc = 1\}$, via the map $\beta : \sigma \mapsto (\lambda_\sigma, f_\sigma) \in A \subset \hat{\mathbb{Z}}^* \times \widehat{F}_2'$. Since $a, b \in G_N$ determine $c \in G_N$, we can view this as an action on pairs of generators $(a, b) \in G_N$. Note that this action factors through $(\mathbb{Z}/n\mathbb{Z})^* \times G_N'$, where $n$ is the exponent of $G_N$. Namely, $\sigma \in G_{\mathbb{Q}}$ takes a pair of generators $(a, b)$ of $G$ to $(a^{\lambda_{\sigma,N}}, f_{\sigma,N}^{-1} b^{\lambda_{\sigma,N}} f_{\sigma,N})$, where $\lambda_{\sigma,N}$ is the image of $\lambda_\sigma$ in $(\mathbb{Z}/n\mathbb{Z})^*$ and $f_{\sigma,N}$ is the image of $f_\sigma$ in $G_N'$. We thus obtain a reduction map $\beta_N : G_{\mathbb{Q}} \to A_N \subset (\mathbb{Z}/n\mathbb{Z})^* \times G_N'$ of $\beta$ (modulo $N$), where $A_N$ is the image of $A$ under $\hat{\mathbb{Z}}^* \times \widehat{F}_2' \to (\mathbb{Z}/n\mathbb{Z})^* \times G_N'$.

Next, we define the reductions $\alpha_N$ of $\alpha$, for each $N \in \Gamma$. For this, observe that we may identify $\mathrm{Aut}(\widehat{F}_2)$ with the set of pairs of generators $(x', y')$ of $\widehat{F}_2$, via $F \mapsto (F(x), F(y))$. Thus $\mathrm{Out}(\widehat{F}_2)$ becomes identified with the set of equivalence classes of such pairs (with respect to uniform conjugacy), and $\mathcal{O}_4^\#$ is identified with a subset of this set of equivalence classes. For each $N \in \Gamma$, let $\mathcal{O}_4^\#/N$ be the quotient of this subset under translation by $N$; this is a set whose elements are equivalence classes of (certain) pairs of generators of $G_N$. The reduction $\alpha_N : G_{\mathbb{Q}} \to \mathcal{O}_4^\#/N$ is then the composition of $\alpha$ with the reduction map $\mathcal{O}_4^\# \twoheadrightarrow \mathcal{O}_4^\#/N$.

In this section, as noted above, our goal is to find $\beta_N$ in terms of an appropriate $\alpha_{\tilde{N}}$. This is only part of the larger problem of understanding the

Belyi map completely by computing each $\beta_N$ directly, thereby bridging the gap from combinatorial group theory to arithmetic in Riemann's Existence Theorem. The other, more difficult part is to compute $\alpha_N$ directly for any given $N$. A weaker approach to that problem is the subject of §3.

**1.3. Construction of $\tilde{N}$.** The basic ingredient in the explicit construction of $\tilde{N}$ is a construction of Serre, given in the first of his two letters published in this volume. Namely, let $G$ be a finite group, let $u \in G$, and let $r$ be a positive integer. Following [S, Lemme 0], we consider the abelian group $R$ consisting of maps $f : G \to \mathbb{Z}/r\mathbb{Z}$ satisfying $f(ug) = f(g)$ for all $g \in G$. Let $e \in R$ be the element corresponding to the characteristic function of the subgroup $\langle u \rangle \subset G$. Also, consider the action of $G$ on $R$ given by $f^g(x) := f(xg)$, where $g \in G$, $f \in R$, $x \in G$. With respect to this action we form the semidirect product $R \rtimes G$, and denote this group by $\Sigma_r(G, u)$. For each $g \in G$, let $g^* = eg \in \Sigma_r(G, u)$. The following result slightly generalizes [S, Lemme 0], which considers the case that $r = o = p$, a prime number.

**Lemma 2.** (cf. [S]) *Let $G$ be a finite group, let $u \in G$, let $r$ be a positive integer, and let $G^* = \Sigma_r(G, u)$.*
*(a) Let $o = \mathrm{ord}(u)$ in $G$. Then $\mathrm{lcm}(r, o) = \mathrm{ord}(u^*)$ in $G^*$.*
*(b) If two powers of $u^*$ are conjugate in $G^*$ then they are equal.*
*(c) Under the quotient map $G^* \to G$, the image of the normalizer $\mathrm{Nor}_{G^*}\langle u^* \rangle$ is $\langle u \rangle$.*

Proof. The proofs of (a) and (b) are straightforward computations. By part (b), the normalizer $\mathrm{Nor}_{G^*}\langle u^* \rangle$ is equal to the centralizer $Z_{G^*}(u^*)$. Since (following [S]) the group law on $G^*$ shows that the image of $Z_{G^*}(u^*)$ under $G^* \to G$ is $\langle u \rangle$, part (c) follows. ♢

The two following lemmas are needed for the construction of $\tilde{N}$.

**Lemma 3.** *Let $G$ be a finite group with generators $a, b$. Let $A = \langle a \rangle$ and $B = \langle a \rangle$, and let $\bar{G}$ be the subgroup of $A \times B \times G$ generated by the two elements $\bar{a} := (a, 1, a)$ and $\bar{b} := (1, b, b)$. Then*
*(a) The orders of $\bar{a}, \bar{b}$ in $\bar{G}$ are respectively equal to the orders of $a, b$ in $G$;*
*(b) The third projection map defines a surjection $\bar{G} \twoheadrightarrow G$ taking $\bar{a}, \bar{b}$ to $a, b$;*
*(c) If $i, j \in \mathbb{Z}$ and $\bar{a}^i\bar{b}^j$ lies in the commutator subgroup $\bar{G}'$ of $\bar{G}$, then $\bar{a}^i = \bar{b}^j = 1$.*

Proof. Assertions (a) and (b) are immediate. Since the commutator subgroup of $A \times B \times G$ is $1 \times 1 \times G'$, and since $\bar{a}^i\bar{b}^j = (a^i, b^j, a^ib^j)$, the last assertion then follows. ♢

We may combine these constructions as follows: Let $a = \pi(x), b = \pi(y) \in G$. Using $G, a, b$, define $\bar{G}, \bar{a}, \bar{b}$ as in Lemma 3 above. Thus we have a

surjection $\bar{G} \twoheadrightarrow G$, taking $\bar{a} \mapsto a$ and $\bar{b} \mapsto b$. Choose any positive integer $r$ that is divisible by the exponent of $\bar{G}$. By the construction in Lemma 2, we obtain the group $\Sigma_r(\bar{G}, \bar{b})$ together with elements $\bar{a}^*, \bar{b}^*$. Again applying this construction (but with the order of the two elements reversed), we obtain the group $\Sigma_r(\Sigma_r(\bar{G}, \bar{b}), \bar{a}^*)$, together with elements $\tilde{a} := \bar{a}^{**}$, $\tilde{b} := \bar{b}^{**}$. Let $\tilde{G}$ be the subgroup generated by $\tilde{a}, \tilde{b}$. Thus we have a surjection $\bar{\eta} : \tilde{G} \twoheadrightarrow \bar{G}$ taking $\tilde{a}, \tilde{b}$ to $\bar{a}, \bar{b}$ respectively. Let $\tilde{\pi} : \widehat{F}_2 \twoheadrightarrow \tilde{G}$ be the map taking $x$ to $\tilde{a}$ and $y$ to $\tilde{b}$, so that the composition $\bar{\pi} = \bar{\eta} \circ \tilde{\pi} : \widehat{F}_2 \twoheadrightarrow \bar{G}$ is the map taking $x$ to $\bar{a}$ and $y$ to $\bar{b}$.

Thus for any finite group $G$ and surjection $\pi : \widehat{F}_2 \twoheadrightarrow G$, we obtain in this manner an explicit choice of finite groups $\bar{G}, \tilde{G}$ and a factorization $\widehat{F}_2 \overset{\tilde{\pi}}{\twoheadrightarrow} \tilde{G} \overset{\bar{\eta}}{\twoheadrightarrow} \bar{G} \twoheadrightarrow G$ of $\pi$. We then have:

**Lemma 4.** *Let $G$ be a finite group and $\pi : \widehat{F}_2 \twoheadrightarrow G$ a surjection. Consider the groups $\bar{G}, \tilde{G}$ and factorization $\widehat{F}_2 \overset{\tilde{\pi}}{\twoheadrightarrow} \tilde{G} \overset{\bar{\eta}}{\twoheadrightarrow} \bar{G} \twoheadrightarrow G$ of $\pi$ as above. Write $\bar{\pi} = \bar{\eta} \circ \tilde{\pi}$. Then:*

*(a) The orders of $\tilde{\pi}(x), \tilde{\pi}(y) \in \tilde{G}$ are divisible by $r$ and the exponent of $G$.*
*(b) If two powers of $\tilde{\pi}(x)$ are conjugate in $\tilde{G}$ then they are equal.*
*(c) $\bar{\eta}\big(\mathrm{Nor}_{\tilde{G}}\langle\tilde{\pi}(x)\rangle\big) = \langle\bar{\pi}(x)\rangle$ and $\bar{\eta}\big(\mathrm{Nor}_{\tilde{G}}\langle\tilde{\pi}(y)\rangle\big) = \langle\bar{\pi}(y)\rangle$.*
*(d) If $\bar{\pi}(x)^i\bar{\pi}(y)^j$ lies in the commutator subgroup $\bar{G}'$ of $\bar{G}$ for some $i, j \in \mathbb{Z}$, then $\bar{\pi}(x)^i = \bar{\pi}(y)^j = 1$.*

Proof. Condition (a) is clear from Lemma 2(a) and the fact that $\exp(G)$ divides $\exp(\bar{G})$ and hence $r$. Condition (b) follows from Lemma 2(b), and condition (c) follows from Lemma 2(c) applied to each of the two uses of that construction. Condition (d) is just Lemma 3(c). ♢

**Definition of $\tilde{N}$.** Given a normal subgroup $N \subset \widehat{F}_2$ of finite index, with $\pi : \widehat{F}_2 \twoheadrightarrow G = \widehat{F}_2/N$ the corresponding quotient map, we have defined $\widehat{F}_2 \overset{\tilde{\pi}}{\twoheadrightarrow} \tilde{G} \twoheadrightarrow G$ (depending on a choice of positive integer $r$). Define the subgroup $\tilde{N}$ associated to $N$ by

$$\tilde{N} = \ker\left(\widehat{F}_2 \twoheadrightarrow \tilde{G}\right) \subset N.$$

Let $n, \tilde{n}$ be the exponents of $G, \tilde{G}$ respectively. Write $a = \pi(x)$, $b = \pi(y)$, $\tilde{a} = \tilde{\pi}(x)$, and $\tilde{b} = \tilde{\pi}(y)$. As before we let $\mathcal{O}_4^\#/N$ be the reduction modulo $N$ of the pairs $(x', y') \in \widehat{F}_2^2$ such that $x \mapsto x', y \mapsto y'$ represents an element of $\mathcal{O}_4^\#$; and similarly for $\mathcal{O}_4^\#/\tilde{N}$. For any $\ell \in (\mathbb{Z}/\tilde{n}\mathbb{Z})^*$ and $s|\tilde{n}$ let $\ell_s \in (\mathbb{Z}/s\mathbb{Z})^*$ denote the reduction of $\ell$ modulo $s$, and for any $f \in \tilde{G}$ let $f_N \in G$ denote its reduction modulo $N$ (i.e. its image in $G$).

**Lemma 5.** *In the above situation, let $(\ell, f), (k, g) \in (\mathbb{Z}/\tilde{n}\mathbb{Z})^* \times \tilde{G}'$, and suppose that the pairs $(\tilde{a}^\ell, f^{-1}\tilde{b}^\ell f), (\tilde{a}^k, g^{-1}\tilde{b}^k g)$ represent the same element of $\mathcal{O}_4^\#/\tilde{N}$. Then*

*(a)* $\ell_r = k_r$ *and hence* $\ell_n = k_n$*;*
*(b)* $f_N = g_N$*.*

Proof. Since $\tilde{a}^\ell$, $\tilde{a}^k$ are conjugate in $\tilde{G}$, Lemma 4(b) says that these two elements are equal. Thus Lemma 4(a) yields part (a) of the proposition.

So there is an element $h \in \tilde{G}$ such that conjugation by $h$ takes $(\tilde{a}^\ell, f^{-1}\tilde{b}^\ell f)$ to $(\tilde{a}^\ell, g^{-1}\tilde{b}^k g)$. Thus $h \in Z_{\tilde{G}}(\tilde{a}^\ell) = Z_{\tilde{G}}(\tilde{a})$, using that $\ell \in (\mathbb{Z}/\tilde{n}\mathbb{Z})^*$. Also, $ghf^{-1} \in \mathrm{Nor}_{\tilde{G}}\langle\tilde{b}^\ell\rangle = \mathrm{Nor}_{\tilde{G}}\langle\tilde{b}\rangle$. Let $\tilde{G} \twoheadrightarrow \bar{G}$ be as in the construction above, and write $\bar{N} = \ker(\widehat{F}_2 \twoheadrightarrow \bar{G})$, $\bar{a} = \tilde{a}_{\bar{N}}$, $\bar{b} = \tilde{b}_{\bar{N}}$. By Lemma 4(c), we have

$$h_{\bar{N}} = \bar{a}^i, \quad g_{\bar{N}}\bar{a}^i f_{\bar{N}}^{-1} = (ghf^{-1})_{\bar{N}} = \bar{b}^j \qquad (*)$$

for some integers $i, j$. Since $f, g \in \tilde{G}'$, we have that $f_{\bar{N}}, g_{\bar{N}} \in \bar{G}'$. So $\bar{a}^i\bar{b}^{-j} \in \bar{G}'$, and hence $\bar{a}^i = \bar{b}^{-j} = 1$ by Lemma 4(d). Thus (*) yields $g_{\bar{N}}f_{\bar{N}}^{-1} = 1$. So $f_{\bar{N}} = g_{\bar{N}}$ and thus $f_N = g_N$. ♢

**1.4. The main result.** Recall that the goal of this section is to make the section $s : \mathcal{O}_4^\# \to A \cap \mathcal{A}_4^\#$ of Theorem 1 explicit. This is done in the following theorem: for $N \in \Gamma$ and $\tilde{N}$ as above, it shows how to compute $s(\overline{F})$ modulo $N$ in terms of $\overline{F}$ modulo $\tilde{N}$.

**Theorem 6.** *Let* $N$ *be a normal subgroup of* $\widehat{F}_2$ *of finite index, and let* $n$ *be the exponent of* $G = \widehat{F}_2/N$*. Define* $\widehat{F}_2 \overset{\tilde{\pi}}{\twoheadrightarrow} \tilde{G} \twoheadrightarrow G$ *as in the construction above, and let* $\tilde{N} = \ker(\widehat{F}_2 \twoheadrightarrow \tilde{G})$*. For* $\overline{F} \in \mathcal{O}_4^\#$*, write* $F = s(\overline{F}) = (\lambda, f) \in A \subset \hat{\mathbb{Z}}^* \times \widehat{F}_2'$*, and let* $F_N$ *be the image of* $F$ *in* $A_N \subset (\mathbb{Z}/n\mathbb{Z})^* \times G'$*.*

*(a)* $F_N$ *depends only on* $\overline{F}_{\tilde{N}}$*, the image of* $\overline{F}$ *in* $\mathcal{O}_4^\#/\tilde{N}$*.*

*(b) Explicitly,* $F_N$ *is given in terms of* $\overline{F}_{\tilde{N}}$ *as follows, where we write* $a = \pi(x)$*,* $b = \pi(y)$*,* $\tilde{a} = \tilde{\pi}(x)$*,* $\tilde{b} = \tilde{\pi}(y)$*: Let* $(\tilde{a}', \tilde{b}')$ *be any element of the equivalence class* $\overline{F}_{\tilde{N}}$*. Choose* $\tilde{d}, \tilde{e} \in \tilde{G}$ *and* $\ell \in \mathbb{Z}$ *such that* $\tilde{a}' = \tilde{d}^{-1}\tilde{a}^\ell\tilde{d}$ *and* $\tilde{b}' = \tilde{e}^{-1}\tilde{b}^\ell\tilde{e}$*, and choose* $i, j \in \mathbb{Z}$ *such that* $\tilde{e}\tilde{d}^{-1} \equiv \tilde{b}^j\tilde{a}^{-i} \bmod \tilde{G}'$*. Then* $F_N = (\ell_n, b^{-j}ed^{-1}a^i)$*, where* $\ell_n$ *is the reduction of* $\ell$ *modulo* $n$*, and where* $d, e$ *are the images of* $\tilde{d}, \tilde{e}$ *in* $G$*.*

Proof. (a) Assume that $\overline{F}, \overline{E} \in \mathcal{O}_4^\#$ have the same image in $\mathcal{O}_4^\#/\tilde{N}$. Let $F = s(\overline{F}), E = s(\overline{E}) \in A \cap \mathcal{A}_4^\#$, and identify these lifts with the corresponding pairs $(\lambda_F, f_F), (\lambda_E, f_E) \in \hat{\mathbb{Z}}^* \times \widehat{F}_2'$. By hypothesis, the images of $(x^{\lambda_F}, f_F^{-1}y^{\lambda_F}f_F)$ and $(x^{\lambda_E}, f_E^{-1}y^{\lambda_E}f_E)$ in $\tilde{G}\times\tilde{G}$ represent the same element of $\mathcal{O}_4^\#/\tilde{N}$. So by Lemma 5, $\lambda_F$ and $\lambda_E$ have the same image in $(\mathbb{Z}/n\mathbb{Z})^*$, and $f_F$ and $f_E$ have the same image in $G'$. Thus $F, E$ have the same image in $A_N$, i.e. $F_N = E_N$.

(b) We show that the construction described can be carried out, and that the asserted equality holds regardless of choices made in the construction.

Let $\tilde{n}$ be the exponent of $\tilde{G}$. Viewing $F \in \mathrm{Aut}(\widehat{F}_2)$, we have that $F(x) = x^\lambda$ and $F(y) = f^{-1}yf$, with $f \in \widehat{F}_2'$. So each element of the equivalence class

$\overline{F}_{\tilde{N}}$ is of the form $(\tilde{a}^{\lambda_{\tilde{n}}}, f_{\tilde{N}}^{-1}\tilde{b}^{\lambda_{\tilde{n}}}f_{\tilde{N}})$, where $\lambda_{\tilde{n}} \in (\mathbb{Z}/\tilde{n}\mathbb{Z})^*$ is the reduction of $\lambda \in \hat{\mathbb{Z}}^*$ modulo $\tilde{n}$ and where $f_{\tilde{N}} \in \tilde{G}'$ is the reduction of $f$ modulo $\tilde{N}$. Thus $(\tilde{a}', \tilde{b}')$ is uniformly conjugate to $(\tilde{a}^{\lambda_{\tilde{n}}}, f_{\tilde{N}}^{-1}b^{\lambda_{\tilde{n}}}f_{\tilde{N}})$, and so the desired $\tilde{d}, \tilde{e}, \ell$ exist (though are not necessarily unique). Since $\tilde{a}, \tilde{b}$ generate $\tilde{G}$, it follows that the abelianization $\tilde{G}^{\mathrm{ab}} = \tilde{G}/\tilde{G}'$ is generated by the images of these elements; hence the desired $i, j$ exist (but again are not unique). Thus the pair $(\ell_n, b^{-j}ed^{-1}a^i) \in (\mathbb{Z}/n\mathbb{Z})^* \times G$ can be constructed. Moreover the second entry lies in $G'$, because $\tilde{b}^{-j}\tilde{e}\tilde{d}^{-1}\tilde{a}^i \in \tilde{G}'$. It remains to show that this pair equals $F_N = (\lambda_N, f_N)$, and so is independent of the above choices.

By Lemma 5, it suffices to show that $(\tilde{a}^{\lambda_{\tilde{n}}}, f_{\tilde{N}}^{-1}\tilde{b}^{\lambda_{\tilde{n}}}f_{\tilde{N}})$ and $(\tilde{a}^{\ell}, \tilde{g}^{-1}\tilde{b}^{\ell}\tilde{g})$ represent the same element of $\mathcal{O}_4^{\#}/\tilde{N}$, where $\tilde{g} = \tilde{b}^{-j}\tilde{e}\tilde{d}^{-1}\tilde{a}^i$. The first of these pairs represents the element $\overline{F}_{\tilde{N}} \in \mathcal{O}_4^{\#}/\tilde{N}$, as does $(\tilde{a}', \tilde{b}') = (\tilde{d}^{-1}\tilde{a}^{\ell}\tilde{d}, \tilde{e}^{-1}\tilde{b}^{\ell}\tilde{e})$. But the latter pair is uniformly conjugate, via $\tilde{d}^{-1}\tilde{a}^i$, to $(\tilde{a}^{\ell}, \tilde{a}^{-i}\tilde{d}\tilde{e}^{-1}\tilde{b}^{\ell}\tilde{e}\tilde{d}^{-1}\tilde{a}^i) = (\tilde{a}^{\ell}, \tilde{g}^{-1}\tilde{b}^{\ell}\tilde{g})$. So the two given pairs represent the same element of $\mathcal{O}_4^{\#}/\tilde{N}$ (regardless of choices made above). ♢

As a consequence, we obtain the desired result that the Belyi lifting $\beta : G_{\mathbb{Q}} \to \mathrm{Aut}(\widehat{F}_2)$ is determined, and can be constructed, at finite levels via $\alpha : G_{\mathbb{Q}} \to \mathrm{Out}(\widehat{F}_2)$:

**Corollary.** *Given $N \in \Gamma$ of exponent $n$, let $\tilde{N} \in \Gamma$ be as in the above construction, and let $n$ be the exponent of $G_N = \widehat{F}_2/N$. Then for every $\sigma \in G_{\mathbb{Q}}$, the image $\beta_N(\sigma) \in A_N \subset (\mathbb{Z}/n\mathbb{Z})^* \times G'_N$ is determined by $\alpha_{\tilde{N}}(\sigma) \in \mathcal{O}_4^{\#}/\tilde{N}$, and is computed by applying the procedure of Theorem 6(b) to that element.*

Proof. This is an immediate consequence of Theorem 6, using the result from Theorem 1 that $\beta = s\alpha$. ♢

Theorem 6 can be reinterpreted as saying that the section $s$ is uniformly continuous. Namely, as above the Belyi group $A \subset \mathrm{Aut}(\widehat{K}(0,4))$ can be regarded as a subset of $\hat{\mathbb{Z}}^* \times \widehat{F}_2'$ (though the group law on $A$ — given by composition — is not the one induced by the usual group law on $\hat{\mathbb{Z}}^* \times \widehat{F}_2'$). Given $N \in \Gamma$, let $n$ be the exponent of $G = \widehat{F}_2/N$, and consider the map $A \twoheadrightarrow A_N$ induced by restricting the map $\hat{\mathbb{Z}}^* \times \widehat{F}_2' \twoheadrightarrow (\mathbb{Z}/n\mathbb{Z})^* \times G'$ to $A$. Consider the weakest topology on $A$ such that these maps $A \twoheadrightarrow A_N$ (for $N \in \Gamma$) are continuous with respect to the discrete topology on $A_N$. In fact, this is a uniform structure on $A$, with respect to the partial ordering of normal subgroups under inclusion. Similarly, we obtain a topology, and uniform structure, on $\mathcal{O}_4^{\#}$, via its maps to the sets $\mathcal{O}_4^{\#}/N$. Theorem 6(a) can then be restated as:

**Corollary.** *The section $s : \mathcal{O}_4^{\#} \to A$ is uniformly continuous.*

Here the uniformity of the continuity corresponds to the fact that $s(\overline{F})$ modulo $N$ is determined by $\overline{F}$ modulo $\tilde{N}$, where $\tilde{N}$ is independent of $\overline{F}$ (and depends only on $N$).

## §2. Generalization of the Belyi lifting to five-point moduli

This section is an analogue of §1 for the moduli space $\mathcal{M}_{0,5}$ and its fundamental group $\widehat{K}(0,5)$ (the profinite pure mapping class group), which replace $\mathcal{M}_{0,4} = \mathbb{P}^1 - \{0,1,\infty\}$ and $\widehat{K}(0,4) = \widehat{F}_2$ considered before. To begin with, we have a natural map $\mu : G_{\mathbb{Q}} \to \mathrm{Out}\big(\widehat{K}(0,5)\big)$, which will play the role of the natural map $\alpha : G_{\mathbb{Q}} \to \mathrm{Out}(\widehat{K}(0,4))$ used in §1. Furthermore, Nakamura [N, Theorem A20] generalized the Belyi lifting $\beta$ to a lifting $\nu : G_{\mathbb{Q}} \to \mathrm{Aut}(\widehat{K}(0,5))$ of $\mu$. The image of the lifting $\nu$ is contained in a certain group $A_5 \subset \mathrm{Aut}(\widehat{K}(0,5))$ which generalizes the Belyi group $A$ considered in §1. Specifically,

$$\begin{aligned} A_5 := \big\{ F \in \mathrm{Aut}(\widehat{K}(0,5)) \mid \exists \lambda \in \hat{\mathbb{Z}}^*, f \in \widehat{F}_2' : F(x_{12}) = x_{12}^{\lambda}, \\ F(x_{23}) = f(x_{12},x_{23})^{-1} x_{23}^{\lambda} f(x_{12},x_{23}), \\ F(x_{34}) = f(x_{45},x_{34})^{-1} x_{34}^{\lambda} f(x_{45},x_{34}), \\ F(x_{45}) = x_{45}^{\lambda},\ F(x_{51}) \sim (x_{51})^{\lambda} \big\}. \end{aligned}$$

(This is a slightly different expression than in [N, Appendix], due to minor differences in choices made in the set-ups.) As in the case of $\mathcal{M}_{0,4}$, an element of $A_5$ determines the pair $(\lambda, f) \in \hat{\mathbb{Z}}^* \times \widehat{F}_2'$. Furthermore the liftings $\beta$ and $\nu$ satisfy a certain agreeable compatibility relation: they associate the same pair $(\lambda, f)$ to a given element of $G_{\mathbb{Q}}$. The groups $\mathcal{O}_5^{\#}$ and $\mathcal{A}_5^{\#}$ were defined in 1.1, and the images of $\mu$ and $\nu$ lie in $\mathcal{O}_5^{\#}$ and $\mathcal{A}_5^{\#}$ respectively.

The structure of this section is exactly parallel to that of §1. In Theorem 7 of 2.1, we give a result from [HS], analogous to Theorem 1 of 1.1, asserting the existence of a section $s_5$ of the homomorphism $\mathcal{A}_5^{\#} \to \mathcal{O}_5^{\#}$ such that $\nu = s_5\mu$. In 2.2 we use Theorem 7 to outline the precise nature of the "explicit determination" of $\nu$ in terms of $\mu$ which is the goal of this section, and in 2.3 we give a generalization of Serre's construction to show that $\nu$ is effective in terms of $\mu$, leading to the main result (Theorem 10 and its corollaries) given in 2.4.

### 2.1. Symmetric automorphisms of $\widehat{K}(0,5)$.

Let $\mathcal{O}_5^{\#}$ and $\mathcal{A}_5^{\#}$ be the subgroups of $\mathrm{Out}(\widehat{K}(0,5))$ and $\mathrm{Aut}(\widehat{K}(0,5))$ respectively defined in 1.1. The following result generalizes to the case $n = 5$ the statement of Theorem 1 which concerned the case $n = 4$. As above, $\mu : G_{\mathbb{Q}} \to \mathrm{Out}\big(\widehat{K}(0,5)\big)$ is the natural map, and $\nu : G_{\mathbb{Q}} \to \mathrm{Aut}(\widehat{K}(0,5))$ is Nakamura's lifting of $\mu$.

**Theorem 7.** ([HS], 2.2) *There is a unique section $s_5$ of the natural homomorphism $\mathcal{A}_5^{\#} \to \mathcal{O}_5^{\#}$ whose image lies in the generalized Belyi subgroup $A_5$ of $\mathrm{Aut}\big(\widehat{K}(0,5)\big)$. This section satisfies $\nu = s_5\mu : G_{\mathbb{Q}} \hookrightarrow \mathrm{Aut}\big(\widehat{K}(0,5)\big)$.*

We will also need the following result from [HS, 2.2].

**Lemma 8.** *For each $F \in \mathcal{A}_5^{\#}$, let $\overline{F}$ be the image of $F$ in $\mathcal{O}_5^{\#}$ and let $\xi(\overline{F})$ be the equivalence class of $(F(x_{12}), F(x_{23})) \in \widehat{K}(0,5) \times \widehat{K}(0,5)$ with respect to the equivalence relation $\sim$ of uniform conjugacy. Then $\xi : \mathcal{O}_5^{\#} \to \widehat{K}(0,5) \times \widehat{K}(0,5)/\sim$ is a well-defined injection.*

**2.2. Explicit computation of the generalized Belyi lifting.** Here we provide an analogue of our remarks in 1.2, with $\widehat{K}(0,5)$ playing the role of $\widehat{F}_2 = \widehat{K}(0,4)$. The goal of §2 is to show that Nakamura's lifting $\nu : G_{\mathbb{Q}} \to \mathrm{Aut}(\widehat{K}(0,5))$ is effective in terms of the natural map $\mu : G_{\mathbb{Q}} \to \mathrm{Out}(\widehat{K}(0,5))$. That is, we show that for any normal subgroup $M \subset \widehat{K}(0,5)$ of finite index, there exists a smaller such subgroup $\tilde{M}$ — which we give explicitly in terms of $M$ — such that the reduction of $\nu$ modulo $M$ is determined by that of $\mu$ modulo $\tilde{M}$. More generally, consider the map $s_5 : \mathcal{O}_4^{\#} \to \mathcal{A}_5^{\#}$ as in Theorem 7. Thus $s_5$ is the unique section of $\mathcal{A}_5^{\#} \to \mathcal{O}_5^{\#}$ whose image lies in $A_5$, and $\nu = s_5 \circ \mu$. We show that the map $s_5$ is effective (thus implying the effectivity of $\nu$ in terms of $\mu$), and interpret this (in the second corollary to Theorem 10) as showing that $s_5$ is uniformly continuous.

Thus, parallel to §1, the goal of this section is to find an explicit $\tilde{M}$ for each $M$ having the above property, and to describe how to compute $s_5(\overline{F})$ modulo $M$ in terms of $\overline{F}$ modulo $\tilde{M}$ — and thus $\nu$ modulo $M$ in terms of $\mu$ modulo $\tilde{M}$. As before, we first need to define the reductions of $\mu$ and $\nu$.

So let $\Gamma_5$ be the set of normal subgroups $M$ of finite index in $\widehat{K}(0,5)$, and for $M \in \Gamma_5$ consider the quotient group $G_M = \widehat{K}(0,5)/M$. For each $\sigma \in G_{\mathbb{Q}}$, the map $\nu : G_{\mathbb{Q}} \to A_5 \cap \mathcal{A}_5^{\#} \subset \mathrm{Aut}(\widehat{K}(0,5))$ assigns an automorphism of $\widehat{K}(0,5)$ that is characterized by a unique pair $(\lambda_\sigma, f_\sigma) \in \hat{\mathbb{Z}}^* \times \widehat{F}_2'$. (Here, as before, we regard $\widehat{F}_2$ as a subgroup of $\widehat{K}(0,5)$ via the inclusion $\iota : x \mapsto x_{12}, y \mapsto x_{23}$.) As in §1, we identify elements $F \in A_5$ with the associated pairs $(\lambda, f)$. For $M \in \Gamma_5$ with exponent $m$, let $A_{5,M}$ be the image of $A_5$ under the map $\hat{\mathbb{Z}}^* \times \widehat{F}_2' \twoheadrightarrow (\mathbb{Z}/m\mathbb{Z})^* \times H_M' \subset (\mathbb{Z}/m\mathbb{Z})^* \times G_M'$, where $H_M \subset G_M$ is the subgroup generated by the images of $x_{12}, x_{23}$. We then obtain the reduction $\nu_M : G_{\mathbb{Q}} \to A_{5,M}$ by composing $\nu$ with this map.

Continuing as in 1.2, we define the reduction $\mu_M$ of $\mu$ for $M \in \Gamma_5$: For each $\overline{F} \in \mathcal{O}_5^{\#}$ and any lift $F \in \mathcal{A}_5^{\#}$ of $\overline{F}$, consider the pair $(F(x_{12}), F(x_{23})) \in \widehat{K}(0,5) \times \widehat{K}(0,5)$. This is well defined in terms of $\overline{F}$ up to uniform conjugacy in $\widehat{K}(0,5)$. Conversely, this equivalence class of pairs uniquely determines $\overline{F}$ by Lemma 8. So we may identify $\mathcal{O}_5^{\#}$ with the set of equivalence classes of

pairs arising in this manner. For each $M \in \Gamma_5$, let $\mathcal{O}_5^{\#}/M$ be the quotient of this set under translation by $M$; this is a set whose elements are equivalence classes of (certain) pairs of elements of $G_M$. The reduction $\mu_M : G_{\mathbb{Q}} \to \mathcal{O}_5^{\#}/M$ is then the composition of $\mu$ with the reduction map $\mathcal{O}_5^{\#} \twoheadrightarrow \mathcal{O}_5^{\#}/M$.

In 2.3 below we construct the desired $\tilde{M}$ in terms of $M$, and we use this to compute $\nu_M$ in terms of $\mu_{\tilde{M}}$ in 2.4. The related problem of understanding $\mu$ modulo $M$ directly is considered in §3 below, in the weaker form of finding information about the images of $\mu$ and $\nu$ modulo $M$.

**2.3. Construction of $\tilde{M}$.** We draw here on the construction used in 1.3, which relied on an idea of Serre. There, for each normal subgroup $N$ of finite index in $\widehat{F}_2 = \widehat{K}(0,4)$, we let $G = G_N$ be the quotient $\widehat{F}_2/N$. We then associated a certain subgroup $\bar{N} \subset N$ that is also normal in $\widehat{F}_2$ of finite index, and the corresponding quotient group $\bar{G} = \widehat{F}_2/\bar{N}$, satisfying the properties of Lemma 2. Choosing a positive integer $r$ that is divisible by the exponent of $\bar{G}$ (and thus in particular by the exponent of $G$), we then applied Serre's construction twice and obtained a certain group $\tilde{G}$, corresponding to a normal subgroup $\tilde{N}$ of finite index in $\widehat{F}_2$ contained in $N$.

Using this, we consider the following analogous construction for normal subgroups $M$ of $\widehat{K}(0,5)$ of finite index. First, recall that for each positive $n \geq 5$ and each $i$ modulo $n$, there is a surjection $p_i : \widehat{K}(0,n) \twoheadrightarrow \widehat{K}(0,n-1)$ that suppresses the generators $x_{ij}$ of $\widehat{K}(0,n)$ for all $j$; in particular we may consider $p_4$ with $n = 5$. In the other direction, there is an inclusion $\iota : \widehat{F}_2 \hookrightarrow \widehat{K}(0,5)$ given by $x \mapsto x_{12}$, $y \mapsto x_{23}$. Thus $\iota$ is a section of $p_4 : \widehat{K}(0,5) \twoheadrightarrow \widehat{K}(0,4) = \widehat{F}_2$. Next, given $M \in \Gamma_5$, let $G = G_M = \widehat{K}(0,5)/M$ and let $\pi : \widehat{K}(0,5) \twoheadrightarrow G$ be the quotient map. Let $H \subset G$ be the image of $\phi = \pi \circ \iota : \widehat{F}_2 \to G$; i.e. $H$ is generated by the two elements $a = \pi(x_{12}) = \phi(x)$ and $b = \pi(x_{23}) = \phi(y)$. Let $N$ be the kernel of $\widehat{F}_2 \twoheadrightarrow H$, so that $H = \widehat{F}_2/N$. The above construction first yields a certain finite group $\bar{H}$. Then, taking a positive integer $r$ that is divisible by the exponents of $\bar{H}$ and of $G$, we obtain a finite group $\tilde{H}$, together with a factorization $\widehat{F}_2 \overset{\tilde{\phi}}{\twoheadrightarrow} \tilde{H} \overset{\bar{\theta}}{\twoheadrightarrow} \bar{H} \twoheadrightarrow H$ of $\phi$. Let $\tilde{N} = \ker \tilde{\phi}$ and $\bar{N} = \ker \bar{\phi}$, where $\bar{\phi} = \bar{\theta} \circ \tilde{\phi}$. Thus $\tilde{H} = \widehat{F}_2/\tilde{N}$ and $\bar{H} = \widehat{F}_2/\bar{N}$. Finally, let $\tilde{M} = M \cap p_4^{-1}(\tilde{N})$ and $\bar{M} = M \cap p_4^{-1}(\bar{N})$, and let $\tilde{G} = \widehat{K}(0,5)/\tilde{M}$ and $\bar{G} = \widehat{K}(0,5)/\bar{M}$.

Observe that the inclusion $\iota : \widehat{F}_2 \hookrightarrow \widehat{K}(0,5)$ compatibly lifts the inclusions $\tilde{\epsilon} : \tilde{H} \hookrightarrow \tilde{G}$ and $\bar{\epsilon} : \bar{H} \hookrightarrow \bar{G}$ that correspond to the inclusions $\bar{M} \subset p_4^{-1}(\bar{N})$ and $\tilde{M} \subset p_4^{-1}(\tilde{N})$ of normal subgroups of $\widehat{K}(0,5)$. Similarly, $\iota$ lifts the natural inclusion $\epsilon : H \hookrightarrow G$. Also, using the definitions of $\tilde{G}, \bar{G}$, it is easy to check that $p_4 : \widehat{K}(0,5) \twoheadrightarrow \widehat{K}(0,4)$ descends compatibly to surjections $\tilde{q} : \tilde{G} \twoheadrightarrow \tilde{H}$, $\bar{q} : \bar{G} \twoheadrightarrow \bar{H}$ such that $\tilde{\epsilon}, \bar{\epsilon}$ are sections of $\tilde{q}, \bar{q}$ respectively.

Thus given a normal subgroup $M \subset \widehat{K}(0,5)$ of finite index, we have a

quotient map $\pi : \widehat{K}(0,5) \twoheadrightarrow G = \widehat{K}(0,5)/M$, a factorization $\widehat{K}(0,5) \xrightarrow{\tilde{\pi}} \tilde{G} \twoheadrightarrow G$ of $\pi$ (depending on a choice of positive integer $r$), and a finite index subgroup $\tilde{M} = \ker \tilde{\pi} \subset M$. We also have corresponding quotients $\tilde{H} = \widehat{F}_2/\tilde{N}$ and $H = \widehat{F}_2/N$. With notation as above, these yield an explicit commutative diagram

$$\begin{array}{ccccccc}
\widehat{K}(0,5) & \xrightarrow{\tilde{\pi}} & \tilde{G} & \xrightarrow{\bar{\eta}} & \bar{G} & \longrightarrow & G \\
\uparrow{\scriptstyle \iota} & & \uparrow{\scriptstyle \tilde{\epsilon}} & & \uparrow{\scriptstyle \bar{\epsilon}} & & \uparrow{\scriptstyle \epsilon} \\
\widehat{F}_2 = \widehat{K}(0,4) & \xrightarrow{\tilde{\phi}} & \tilde{H} & \xrightarrow{\bar{\theta}} & \bar{H} & \longrightarrow & H
\end{array}$$

and we identify the lower groups with their images in the upper groups. Under this identification, $\tilde{\pi}(x_{12}), \tilde{\pi}(x_{23})$ lie in $\tilde{H}$, since $x_{12}, x_{23} \in \widehat{K}(0,5)$ are the images of $x, y \in \widehat{F}_2$. Let $m, \tilde{m}$ be the exponents of $G, \tilde{G}$ respectively. Write $a = \pi(x_{12})$, $b = \pi(x_{23})$, $\tilde{a} = \tilde{\pi}(x_{12})$, and $\tilde{b} = \tilde{\pi}(x_{23})$. As above we have the sets $\mathcal{O}_5^{\#}/M$ and $\mathcal{O}_5^{\#}/\tilde{M}$, which consist of certain equivalence classes of pairs in $G^2$ and $\tilde{G}^2$ respectively, under uniform conjugacy. For any $\ell \in (\mathbb{Z}/\tilde{m}\mathbb{Z})^*$ and $s|\tilde{m}$, let $\ell_s \in (\mathbb{Z}/s\mathbb{Z})^*$ denote the reduction of $\ell$ modulo $s$, and for any $f \in \tilde{G}$ let $f_M \in G$ denote its reduction modulo $M$ (i.e. its image in $G$). We then have the following analogue of Lemma 5 of 1.3:

**Lemma 9.** *In the above situation, let $(\ell, f), (k, g) \in (\mathbb{Z}/\tilde{m}\mathbb{Z})^* \times \tilde{H}'$, and suppose that $(\tilde{a}^\ell, f^{-1}\tilde{b}^\ell f)$ and $(\tilde{a}^k, g^{-1}\tilde{b}^k g)$ represent the same element of $\mathcal{O}_5^{\#}/\tilde{M}$. Then the pairs also represent the same element of $\mathcal{O}_4^{\#}/\tilde{N}$. Moreover*
*(a) $\ell_r = k_r$ and hence $\ell_m = k_m$;*
*(b) $f_M = g_M$.*

Proof. The elements $\tilde{a}, \tilde{b}, f, g$ lie in the image of $\tilde{\pi}\iota = \tilde{\epsilon}\tilde{\phi}$ and hence in the image of $\tilde{\epsilon}$. By hypothesis, there is an element $h \in \tilde{G}$ such that conjugation by $h$ takes $(\tilde{a}^\ell, f^{-1}\tilde{b}^\ell f)$ to $(\tilde{a}^\ell, g^{-1}\tilde{b}^k g)$ in $\tilde{G}^2$. Applying $\tilde{q} : \tilde{G} \twoheadrightarrow \tilde{H}$, and using that $\tilde{\epsilon}$ is a section of $\tilde{q}$, we deduce that conjugation by $\tilde{q}(h) \in \tilde{H} \subset \tilde{G}$ takes $(\tilde{a}^\ell, f^{-1}\tilde{b}^\ell f)$ to $(\tilde{a}^\ell, g^{-1}\tilde{b}^k g)$ in $\tilde{H}^2$. Since these two pairs are uniformly conjugate with respect to $\tilde{H}$ (and not just with respect to $\tilde{G}$), it follows that they represent the same element of $\mathcal{O}_4^{\#}/\tilde{N}$ (and not just of $\mathcal{O}_5^{\#}/\tilde{M}$).

Thus the situation here is a special case of that of Lemma 5, so Lemma 5(a) implies that $\ell_r = k_r$. Thus $\ell_m = k_m$, since $m = \exp(G)$ divides $r$ by assumption. This yields assertion (a) of the proposition. Also, Lemma 5(b) says that $f_N = g_N$. By the commutativity of the above diagram, $f_M = \epsilon(f_N) \in G$ and similarly for $g$; this yields assertion (b). ♢

**2.4. The main result.** Using this, we obtain the following analogue of Theorem 6, which makes explicit the section $s_5 : \mathcal{O}_5^{\#} \to A_5 \cap \mathcal{A}_5^{\#} \subset \mathcal{A}_5^{\#}$

of Theorem 7. Namely, for $M \in \Gamma_5$ and $\tilde{M}$ as above, it computes $s_5(\overline{F})$ modulo $M$ in terms of $\overline{F}$ modulo $\tilde{M}$.

**Theorem 10.** *Let $M$ be a normal subgroup of $\widehat{K}(0,5)$ of finite index, and let $m$ be the exponent of $G = \widehat{K}(0,5)/M$. Define $\widehat{K}(0,5) \overset{\tilde{\pi}}{\twoheadrightarrow} \tilde{G} \twoheadrightarrow G$ as in the construction above, and let $\tilde{M} = \ker(\widehat{K}(0,5) \twoheadrightarrow \tilde{G})$. For $\overline{F} \in \mathcal{O}_5^{\#}$, write $F = s_5(\overline{F}) = (\lambda, f) \in A_5 \subset \hat{\mathbb{Z}}^* \times \widehat{F}_2'$, and let $F_M$ be the image of $F$ in $A_{5,M} \subset (\mathbb{Z}/m\mathbb{Z})^* \times G'$.*
*(a) Then $F_M$ depends only on $\overline{F}_{\tilde{M}}$, the image of $\overline{F}$ in $\mathcal{O}_5^{\#}/\tilde{M}$.*
*(b) Explicitly, $F_M$ is given in terms of $\overline{F}_{\tilde{M}}$ as follows, where we write $a = \pi(x_{12})$, $b = \pi(x_{23})$, $\tilde{a} = \tilde{\pi}(x_{12})$, $\tilde{b} = \tilde{\pi}(x_{23})$: Let $(\tilde{a}', \tilde{b}')$ be any element of the equivalence class $\overline{F}_{\tilde{M}}$. Choose $\tilde{d}, \tilde{e} \in \tilde{H} = \langle \tilde{a}, \tilde{b} \rangle$ and $\ell \in \mathbb{Z}$ such that $\tilde{a}' = \tilde{d}^{-1}\tilde{a}^{\ell}\tilde{d}$ and $\tilde{b}' = \tilde{e}^{-1}\tilde{b}^{\ell}\tilde{e}$, and choose $i, j \in \mathbb{Z}$ such that $\tilde{e}\tilde{d}^{-1} \equiv \tilde{b}^{j}\tilde{a}^{-i} \bmod \tilde{H}'$. Then $F_M = (\ell_m, b^{-j}ed^{-1}a^{i})$, where $\ell_m$ is the reduction of $\ell$ modulo $m$, and where $d, e$ are the images of $\tilde{d}, \tilde{e}$ in $G$.*

Proof. Theorem 10 follows from Lemma 9 exactly as Theorem 6 followed from Lemma 5. ♢

Thus parallel to §1, we obtain the desired consequence that Nakamura's lifting $\nu : G_{\mathbb{Q}} \to \mathrm{Aut}(\widehat{K}(0,5))$ is determined, and can be constructed, at finite levels via $\mu : G_{\mathbb{Q}} \to \mathrm{Out}(\widehat{K}(0,5))$:

**Corollary.** *Given $M \in \Gamma_5$ of exponent $m$, let $\tilde{M} \in \Gamma_5$ be as in the above construction, and let $m$ be the exponent of $G_M = \widehat{K}(0,5)/M$. Then for every $\sigma \in G_{\mathbb{Q}}$, the image $\nu_M(\sigma) \in A_{5,M} \subset (\mathbb{Z}/m\mathbb{Z})^* \times G'_M$ is determined by $\mu_{\tilde{M}}(\sigma) \in \mathcal{O}_5^{\#}/\tilde{M}$, and is computed by applying the procedure of Theorem 10(b) to that element.*

Proof. This is an immediate consequence of Theorem 10, using the result from Theorem 7 that $\nu = s_5 \circ \mu$. ♢

As in §1, we may put a topology and uniform structure on $A_5$ via the normal subgroups $M \in \Gamma_5$, and similarly on $\mathcal{O}_5^{\#}$ via the maps to the sets $\mathcal{O}_5^{\#}/M$. Parallel to the second corollary to Theorem 6, we then may restate Theorem 10 as:

**Corollary.** *The section $s_5 : \mathcal{O}_5^{\#} \to A_5$ is uniformly continuous.*

## §3. The $\widehat{GT}_0$ and $\widehat{GT}$-orbits of dessins

As discussed in the introduction, we would like to compute the action of $G_{\mathbb{Q}}$ on Galois dessins, thus relating the arithmetic of covers to their combinatorics. In the previous sections, we described how to compute canonical actions of $G_{\mathbb{Q}}$ on the fundamental groups of $\mathcal{M}_{0,4} = \mathbb{P}^1 - \{0, 1, \infty\}$ and

$\mathcal{M}_{0,5}$ in terms of the natural outer actions. To complete the description we would like to be able to describe the outer action of an element of $G_{\mathbb{Q}}$ on these fundamental groups $\widehat{K}(0,4)$ and $\widehat{K}(0,5)$. Unfortunately this seems beyond reach at present, and here we content ourselves with somewhat less — namely finding the $\widehat{GT}_0$- and $\widehat{GT}$-orbits of a dessin, which approximate the $G_{\mathbb{Q}}$-orbit and yield information about the field of moduli of the corresponding cover. We do so by using the relationship of $\widehat{GT}_0$ and $\widehat{GT}$ to the groups $\mathcal{O}_n^{\#}$ considered above.

The $\widehat{GT}_0$- and $\widehat{GT}$-orbits of a dessin will be found by an iterative process, computing somewhat larger orbits under computable finite groups, which converge to the true $\widehat{GT}_0$- and $\widehat{GT}$-orbits after finitely many steps (and thus, in the latter case, to the $G_{\mathbb{Q}}$-orbit, if $\widehat{GT}$ turns out to be the same as $G_{\mathbb{Q}}$). The key idea is that we can explicitly find subgroups of the outer automorphism groups of finite quotients of $\widehat{K}(0,n)$ that are defined by finite-level properties analogous to the defining properties of $\mathcal{O}_n^{\#}$. We explain the procedure in 3.4 and 3.5, after giving an overview in 3.1 and some necessary definitions and results in 3.2 and 3.3. Then, in 3.6, we use these orbits to obtain information about the field of moduli of a Galois dessin.

**3.1. Approximation of the Galois orbit of a dessin.** Given a dessin $D$, it is unknown how to find its $G_{\mathbb{Q}}$-orbit effectively, since this involves understanding the connection between the combinatorics of a dessin (or of a branch cycle description) and the arithmetic of a cover. But some $G_{\mathbb{Q}}$-orbits can be separated, using known invariants such as the geometric Galois group and valency list of the dessin (as well as less obvious invariants, e.g. via obstructed components of modular towers [F2]). In the special case of rigidity, it is possible to understand the $G_{\mathbb{Q}}$-orbit and the field of moduli. In general, though, the known invariants give only *approximative* orbits which contain the Galois orbit but may be quite crude.

However, even approximations are useful for the inverse Galois problem. For instance the order of an approximative orbit is greater or equal to the order of the true Galois orbit, and so gives an upper bound on the degree of the field of moduli of the dessin. Moreover, if the approximative orbit turns out to consist only of $D$, then this is also true of the Galois orbit, so $D$ has field of moduli $\mathbb{Q}$ — and its geometric Galois group $G$ is thus a Galois group over $\mathbb{Q}$, under mild hypotheses on $G$ [CH, 2.8(c)]. This viewpoint provides our motivation for finding approximative orbits of dessins. In keeping with the approach of the preceding sections, we use the fact that $G_{\mathbb{Q}}$ is contained in the larger groups $\mathcal{O}_n^{\#} \subset \mathrm{Out}\big(\widehat{K}(0,n)\big)$ [HS, 1.2]. By finding the orbits under these larger groups, we thus obtain approximate $G_{\mathbb{Q}}$-orbits. This approach takes advantage of the fact that the action of $\mathcal{O}_n^{\#}$ on dessins is known, and extends that of the subgroup $G_{\mathbb{Q}}$ (though what is

not known explicitly is the precise injection $G_{\mathbb{Q}} \hookrightarrow \mathcal{O}_n^{\#}$). In addition, this approach reflects the conjecture that the Grothendieck-Teichmüller group $\widehat{GT}$ is isomorphic to $G_{\mathbb{Q}}$, together with the following theorem:

**Theorem 11.** [HS, 1.3, 2.3] *$\widehat{GT}_0 \simeq \mathcal{O}_4^{\#}$ and $\widehat{GT} \simeq \mathcal{O}_5^{\#}$.*

Thus if the conjecture on $\widehat{GT}$ is correct, then by finding the $\mathcal{O}_5^{\#}$-orbit of a dessin we are actually finding the $G_{\mathbb{Q}}$-orbit. (For definitions and background on $\widehat{GT}$ and the larger group $\widehat{GT}_0$, see the survey on $\widehat{GT}$ in this volume.)

**3.2. Automorphism groups on finite levels.** Before computing approximations, let us define some important groups of outer automorphisms of the pure profinite mapping class groups $\widehat{K}(0,n)$.

Let $\mathcal{O}_n = \mathrm{Out}\big(\widehat{K}(0,n)\big)$ be the group of outer automorphisms. As in 1.1, there is a natural outer $S_n$-action on $\widehat{K}(0,n)$, i.e. a homomorphism $\sigma^{(n)} : S_n \to \mathcal{O}_n$. In terms of this, we defined the groups $\mathcal{O}_n^{\#}$ in 1.1.

If $N$ is any characteristic subgroup of finite index of $\widehat{K}(0,n)$, then automorphisms of $\widehat{K}(0,n)$ preserve $N$ and thus pass to the quotient $\widehat{K}(0,n)/N$. The same is true for outer automorphisms, giving rise to a natural homomorphism

$$\psi_N^n : \mathcal{O}_n \to \mathrm{Out}\big(\widehat{K}(0,n)/N\big).$$

Similarly, for characteristic subgroups $M \subset N$ of finite index in $\widehat{K}(0,n)$, we have a homomorphism

$$\psi_{M,N}^n : \mathrm{Out}\big(\widehat{K}(0,n)/M\big) \to \mathrm{Out}\big(\widehat{K}(0,n)/N\big).$$

We then define the mod $N$ reductions of the groups $\mathcal{O}_n$ and $O_n^{\#}$:

- $\mathcal{O}_{n,N} = \psi_N^n\big(\mathcal{O}_n\big),\ \ \mathcal{O}_{n,N}^{\#} = \psi_N^n\big(\mathcal{O}_n^{\#}\big)$.

Let $\sigma_N^{(n)}$ denote the composition of homomorphisms $\psi_N^n \circ \sigma^{(n)}$ for $n \geq 4$. As sketched above, we will define the *approximations* $\mathcal{O}_n(N)$ and $\mathcal{O}_n^{\#}(N)$ of the finite groups $\mathcal{O}_{n,N}$ and $\mathcal{O}_{n,N}^{\#}$ as groups of outer automorphisms of $K(0,n)/N$ having properties analogous to those of $\mathcal{O}_n$ and $\mathcal{O}_n^{\#}$. (We indicate "approximations" by putting $N$ in parentheses, whereas the actual images are indicated by an $N$ in the subscript.) Namely, writing $(x_{ij})_N$ for the image of $x_{ij}$ in $K(0,n)/N$ and $e$ for the exponent of $K(0,n)/N$, we define

- $\mathcal{O}_n(N) = \mathrm{Out}(K(0,n)/N)$,
- $\mathcal{O}_n^{\#}(N) = \big\{\overline{F} \in \mathcal{O}_n(N) \mid$ (i) $\exists \lambda \in \big(\mathbb{Z}/e\mathbb{Z}\big)^* : (\forall i,j)\, \overline{F}\big([(x_{ij})_N]\big) = [(x_{ij})_N^{\lambda}]$;
  (ii) $\overline{F}$ commutes with $\sigma_N^{(n)}(S_n)$ in $\mathcal{O}_n(N)\big\}$.

It is immediate from the definitions that $\mathcal{O}_{n,N} \subset \mathcal{O}_n(N)$; it is also easily seen that $\mathcal{O}_{n,N}^{\#} \subset \mathcal{O}_n^{\#}(N)$ since elements of $\mathcal{O}_{n,N}^{\#}$ inherit properties (i)

and (ii) from the analogous properties in $\mathcal{O}_n^{\#}$. The main point is that the approximative groups $\mathcal{O}_n(N)$ and $\mathcal{O}_n^{\#}(N)$ can be *computed* (unlike $\mathcal{O}_{n,N}$ and $\mathcal{O}_{n,N}^{\#}$). Moreover these two groups serve as good approximations since (as we will show in 3.3) the two above containments become equalities in the limit, with respect to the inverse systems given by the maps $\psi_{M,N}^n$.

**3.3. Inverse systems and inverse limits.** In this section we prove some results on inverse limits of the automorphism groups defined in 3.2.

**Lemma 12.** *Let $G$ be any finitely generated group, and let $\widehat{G}$ denote the profinite completion of $G$, i.e. the inverse limit of the quotients of $G$ by all the normal subgroups of finite index. Then the inverse limit of the quotients of $G$ by all the characteristic subgroups of finite index is also isomorphic to $\widehat{G}$, i.e. the characteristic subgroups of $G$ form a cofinal system.*

Proof. It suffices to show that every normal subgroup $N$ of finite index in $G$ contains a characteristic subgroup $\breve{N}$ of finite index. In particular we can let $\breve{N}$ be the intersection of all the normal subgroups $N^*$ of $G$ such that $G/N^* \simeq G/N$. There are only finitely many of these; indeed, they are the kernels of the homomorphisms of $G$ into a finite group, and since $G$ is finitely generated there are only finitely many such homomorphisms. ♢

**Corollary.** *For all $n \geq 4$, we have*

$$\varprojlim_N \widehat{K}(0,n)/N = \widehat{K}(0,n)$$

*as $N$ runs over the characteristic subgroups of finite index of $\widehat{K}(0,n)$.*

Proof. By the lemma, we know that since the discrete pure mapping class group $K(0,n)$ is finitely generated, it is the inverse limit of the finite quotients $K(0,n)/N$ for characteristic subgroups $N$ of $K(0,n)$. But the characteristic subgroups of finite index of $\widehat{K}(0,n)$ are in bijection with those of $K(0,n)$, so the finite quotients of $K(0,n)$ and of $\widehat{K}(0,n)$ by corresponding subgroups are in one-to-one correspondence. ♢

If $N$ is any characteristic subgroup of finite index in $\widehat{K}(0,n)$, then along with the homomorphism $\psi_N^n$ of 3.2, there are natural homomorphisms

$$\Psi_N^n : \widehat{K}(0,n) \to \widehat{K}(0,n)/N$$
$$\tilde{\psi}_N^n : \mathrm{Aut}\big(\widehat{K}(0,n)\big) \to \mathrm{Aut}\big(\widehat{K}(0,n)/N\big).$$

Similarly, if $M \subset N$ are characteristic subgroups of finite index of $\widehat{K}(0,n)$, then along with $\psi_{M,N}^n$ of 3.2 we have natural homomorphisms:

$$\Psi_{M,N}^n : \widehat{K}(0,n)/M \to \widehat{K}(0,n)/N$$
$$\tilde{\psi}_{M,N}^n : \mathrm{Aut}\big(\widehat{K}(0,n)/M\big) \to \mathrm{Aut}\big(\widehat{K}(0,n)/N\big).$$

The diagram

$$\begin{array}{ccc} \mathrm{Aut}\big(\widehat{K}(0,n)/M\big) & \xrightarrow{\tilde{\psi}^n_{M,N}} & \mathrm{Aut}\big(\widehat{K}(0,n)/N\big) \\ \downarrow & & \downarrow \\ \mathrm{Out}\big(\widehat{K}(0,n)/M\big) & \xrightarrow{\psi^n_{M,N}} & \mathrm{Out}\big(\widehat{K}(0,n)/N\big) \end{array} \qquad (*)$$

commutes, and for all $x \in \widehat{K}(0,n)/M$ and $\Phi \in \mathrm{Aut}\big(\widehat{K}(0,n)/M\big)$, we have

$$\tilde{\psi}^n_{M,N}(\Phi)(\Psi^n_{M,N}(x)) = \Psi^n_{M,N}\big(\Phi(x)\big) \qquad (**)$$

**Theorem 13.** *(a) For all $n \geq 4$, the groups $\mathcal{O}_{n,N}$ form an inverse system as $N$ runs over the characteristic subgroups of finite index of $\widehat{K}(0,n)$, and so do the groups $\mathcal{O}_n(N)$. Moreover, we have*

$$\varprojlim_N \mathcal{O}_{n,N} = \varprojlim_N \mathcal{O}_n(N) = \mathcal{O}_n.$$

*(b) For all $n \geq 4$, the groups $\mathcal{O}^{\#}_{n,N}$ form an inverse system as $N$ runs over the characteristic subgroups of $K(0,n)$, and so do the groups $\mathcal{O}^{\#}_n(N)$. Moreover, we have*

$$\varprojlim_N \mathcal{O}^{\#}_{n,N} = \varprojlim_N \mathcal{O}^{\#}_n(N) = \mathcal{O}^{\#}_n.$$

Proof. (a) The groups $\mathcal{O}_n(N)$ form an inverse system under the maps $\psi^n_{M,N}$ since these maps are well-defined. Moreover, whenever $M \subset N$, we have $\psi^n_N = \psi^n_{M,N} \circ \psi^n_M$, so $\mathcal{O}_{n,N} = \psi^n_N(\mathcal{O}_n) = (\psi^n_{M,N} \circ \psi^n_M)(\mathcal{O}_n) = \psi^n_{M,N}(\mathcal{O}_{n,M})$ by the definition of the $\psi^n_{M,n}$; so the $\mathcal{O}_{n,N}$ also form an inverse system under the maps $\psi^n_{M,N}$. Next we define homomorphisms from $\mathcal{O}_n$ to $\varprojlim \mathcal{O}_{n,N}$ and to $\varprojlim \mathcal{O}_n(N)$; then we will define homomorphisms in the other direction and show that they are mutual inverses, so isomorphisms. Let $\phi \in \mathcal{O}_n$. For $N$ a finite-index characteristic subgroup, $\phi_N = \psi^n_N(\phi)$ is in $\mathcal{O}_{n,N} \subset \mathcal{O}_n(N)$; so $\phi \mapsto (\phi_N)_N$ is a group homomorphism from $\mathcal{O}_n$ to each of the two inverse limits. Conversely, consider an element $(\phi_N)_N$ in either inverse limit, where the $\phi_N$'s are compatible elements of $\mathcal{O}_{n,N}$ (resp. $\mathcal{O}_n(N)$). Then $(\phi_N)_N$ gives an outer automorphism $\phi$ of $\widehat{K} = \widehat{K}(0,n)$, defined by $\phi((\alpha_N)_N) = \big(\phi_N(\alpha_N)\big)_N$; here we use the identification in the corollary to Lemma 12. (This $\phi$ really is an outer automorphism since it is trivial on the identity, respects relations in $\widehat{K}$ and is invertible — all consequences of the

analogous behavior on the finite levels.) This map $(\phi_N)_N \mapsto \phi$ is inverse to the previous map $\phi \mapsto (\phi_N)_N$, so both are isomorphisms. (The difference between the inverse systems of $\mathcal{O}_{n,N}$ and of $\mathcal{O}_n(N)$ is that the $\psi^n_{M,N}$ restrict to surjections on the $\psi^n_{M,N}$, but not necessarily for the $\mathcal{O}_n(N)$.)

(b) The $\mathcal{O}^{\#}_{n,N}$ form an inverse system under the restriction to the subgroups $\mathcal{O}^{\#}_{n,N} \subset \mathcal{O}_{n,N}$ of the homomorphisms $\psi^n_{M,N}$ for the same reason as the $\mathcal{O}_{n,N}$ in (a). To show that $\big(\{\mathcal{O}^{\#}_n(N)\}, \{\psi^n_{M,N}\}\big)$ also forms an inverse system, we check that $\psi^n_{M,N}\big(\mathcal{O}^{\#}_n(M)\big) \subset \mathcal{O}^{\#}_n(N)$. Let $\phi \in \mathcal{O}^{\#}_n(M)$, so $\phi$ has the properties (i) and (ii) in the definition of the groups $\mathcal{O}^{\#}_n(M)$; we need to check that $\psi^n_{M,N}(\phi)$ has the corresponding two properties.

Let $\phi \in \mathcal{O}^{\#}_n(M)$. Let us show that $\psi^n_{M,N}(\phi)$ has property (i), viz. that it sends the conjugacy class of $(x_{ij})_N$ to that of $(x_{ij})^{\lambda}_N$ for each pair $i, j$. Since $\phi$ has property (i) (for $M$), there is a lifting $\Phi$ of $\phi$ in $\mathrm{Aut}\big(K(0,n)/M\big)$ such that $\Phi(x_{ij}) = \alpha_{ij}^{-1} x_{ij}^{\lambda} \alpha_{ij}$ for some $\alpha_{ij} \in \widehat{K}(0,n)/M$. By (**) with this $\Phi$,

$$\begin{aligned}\tilde{\psi}^n_{M,N}(\Phi)\big((x_{ij})_N\big) &= \tilde{\psi}^n_{M,N}(\Phi)\big(\Psi^n_{M,N}((x_{ij})_M)\big) = \Psi^n_{M,N}\big(\Phi\big((x_{ij})_M\big)\big)\\ &= \Psi^n_{M,N}\big(\alpha_{ij}^{-1}(x_{ij})^{\lambda}_M \alpha_{ij}\big) = \Psi^n_{M,N}(\alpha_{ij})^{-1}(x_{ij})^{\lambda}_N \Psi^n_{M,N}(\alpha_{ij}).\end{aligned}$$

But $\tilde{\psi}^n_{M,N}(\Phi)$ is a lifting of $\psi^n_{M,N}(\phi)$ to $\mathrm{Aut}\big(\widehat{K}(0,n)/N\big)$ by the diagram (*), and the existence of a lifting sending each $(x_{ij})_N$ to a conjugate of $(x_{ij})^{\lambda}_N$ shows that $\psi^n_{M,N}(\phi)$ has property (i). Property (ii), i.e. that $\psi^n_{M,N}$ commutes with $\sigma^{(n)}_M(S_n)$, follows immediately since $\psi^n_{M,N} \circ \sigma^{(n)}_M = \sigma^{(n)}_N$.

Let us show that the inverse limits of the two systems $\mathcal{O}^{\#}_{n,N}$ and $\mathcal{O}^{\#}_n(N)$ are both isomorphic to $\mathcal{O}^{\#}_n$. For any $\phi \in \mathcal{O}^{\#}_n$, setting $\phi_N = \psi^n_N(\phi)$, the element $(\phi_N)_N$ belongs to both $\varprojlim \mathcal{O}^{\#}_{n,N}$ and $\varprojlim \mathcal{O}^{\#}_n(N)$. Conversely, let $(\phi_N)_N$ lie in $\varprojlim \mathcal{O}^{\#}_{n,N}$ (resp. $\varprojlim \mathcal{O}^{\#}_n(N)$). We showed in the proof of (a) that $(\phi_N)_N$ determines an element $\phi$ of $\mathcal{O}_n$, so we only need to show that $\phi$ has properties (i) and (ii) of the definition of $\mathcal{O}^{\#}_n$. But these two properties hold if they hold on every finite level, which proves the result. (Again here, as in (a), the inverse system of the $\mathcal{O}^{\#}_{n,N}$ consists of surjective homomorphisms whereas this is not necessarily true for the $\mathcal{O}^{\#}_n(N)$.) ♢

**Corollary.** *The groups $\widehat{GT}_0$ and $\widehat{GT}$ are profinite groups.*

Proof. We know by Theorem 11 that $\widehat{GT}_0 = \mathcal{O}^{\#}_4$ and $\widehat{GT} = \mathcal{O}^{\#}_5$. By the preceding theorem $\mathcal{O}^{\#}_4$ is the inverse limit of the finite groups $\mathcal{O}^{\#}_4(N)$ or $\mathcal{O}^{\#}_{4,N}$ as $N$ runs through the characteristic subgroups of $\widehat{K}(0,4)$, and $\mathcal{O}^{\#}_5$ is the inverse limit of the groups $\mathcal{O}^{\#}_5(M)$ or $\mathcal{O}^{\#}_{5,M}$ as $M$ runs through the characteristic subgroups of $\widehat{K}(0,5)$. ♢

**3.4. Approximation of the $\widehat{GT}_0$-orbit of a dessin.** We explain here our approach to the approximation and computation of the $\widehat{GT}_0$- and $\widehat{GT}$-orbits

of a dessin $D$; for simplicity we assume that $D$ is Galois. The somewhat easier case of $\widehat{GT}_0$ and $\widehat{K}(0,4)$ is actually carried out here, while that of $\widehat{GT}$ and $\widehat{K}(0,5)$ is treated in 3.5. As before we identify $\widehat{F}_2 = \langle x, y, z | xyz = 1\rangle$ with $\widehat{K}(0,4)$ via the isomorphism $x \mapsto x_{12}$, $y \mapsto x_{23}$.

For any finite group $G$ with two generators, the $G$-Galois dessins $D$ are in bijection with normal subgroups $N \subset \widehat{K}(0,4)$ together with isomorphisms $\widehat{K}(0,4)/N \xrightarrow{\sim} G$ (determined up to an inner automorphism). They are also in bijection with uniform conjugacy classes of triples $(a,b,c)$ of generators of $G$ such that $abc = 1$; viz. the branch cycle description of the corresponding $G$-Galois cover, where $a = x_N$, $b = y_N$, and $c = z_N$. Since $abc = 1$, we may classify $G$-Galois dessins simply by the pair $(x_N, y_N)$. Now there is a natural action of $\mathcal{O}_4^\#$ on the set of $G$-Galois dessins, which by Theorem 1 extends the action of $G_{\mathbb{Q}}$ on this set. Also, given $D, N, G$ as above, if $\breve{N} \subset \widehat{K}(0,4)$ is any finite index characteristic subgroup contained in $N$, the action of $\mathcal{O}_4^\#$ on the orbit of $D$ factors through the finite group $\mathcal{O}^\#_{4,\breve{N}}$ — and thus the $\widehat{GT}_0$-orbit of $D$ is the same as the $\mathcal{O}^\#_{4,\breve{N}}$-orbit (and is equal to the set $\mathcal{O}_4^\#/N$ of §1). Unfortunately, it is unclear how to find exactly which elements of the finite group $\mathrm{Out}(G)$ lie in $\mathcal{O}^\#_{4,\breve{N}}$, since the definition of $\mathcal{O}^\#_{4,\breve{N}}$ involves the infinite group $\widehat{GT}_0 \simeq \mathcal{O}_4^\#$.

So instead, we take an indirect approach, using the fact that we can find the elements of the (possibly) larger finite group $\mathcal{O}_4^\#(\breve{N}) \subset \mathrm{Out}(G)$, along with the fact that the $\mathcal{O}^\#_{4,\breve{N}}$-action extends to an $\mathcal{O}_4^\#(\breve{N})$-action. Namely, for $\overline{F} \in \mathcal{O}_4^\#(\breve{N})$, we define $D_{\overline{F}}$ to be the $G$-Galois dessin corresponding to the equivalence class of the pair $\big((F(x_{\breve{N}}))_N\,,\,(F(y_{\breve{N}}))_N\big)$ in $G^2$, where $F \in \mathrm{Aut}(\widehat{K}(0,4)/\breve{N})$ is a lifting of $\overline{F}$. (The equivalence class of the pair is independent of the choice of lifting $F$.) We call the orbit of $D$ under $\mathcal{O}_4^\#(\breve{N})$ the *$\breve{N}$-approximative $\widehat{GT}_0$-orbit of $D$*.

We can thus explicitly compute the $\breve{N}$-approximative $\widehat{GT}_0$-orbit of any $G$-Galois dessin $D$, where $G = \widehat{K}(0,4)/N$:

(1) Let $\breve{N}$ be any characteristic subgroup of finite index in $\widehat{K}(0,4)$ that is contained in $N$ — e.g. the $\breve{N}$ in the proof of Lemma 12.

(2) Compute the finite group $\mathcal{O}_4^\#(\breve{N})$ from the definition.

(3) For each element $\overline{F}$ of $\mathcal{O}_4^\#(\breve{N})$, compute $\big((F(x_{\breve{N}}))_N\,,\,(F(y_{\breve{N}}))_N\big) \in G^2$.

By taking smaller and smaller choices of $\breve{N}$, we can compute the actual $\widehat{GT}_0$-orbit of $D$ in finitely many steps. Namely, by Lemma 12, there is a cofinal sequence of finite index characteristic subgroups $N_0 \subset N_1 \subset \cdots$ of $\widehat{K}(0,4)$ inside any given normal subgroup $N$ of finite index. In this situation we have the following corollary of Theorem 13:

**Corollary.** *Let $D$ be a $G$-Galois dessin, corresponding to a normal subgroup $N \subset \widehat{K}(0,4)$ of finite index. Let $\{N_i\}$ be a cofinal sequence of finite index characteristic subgroups of $\widehat{K}(0,4)$ contained in $N$. Then for all $i \gg 0$, the $N_i$-approximative $\widehat{GT}_0$-orbit of $D$ is equal to the $\widehat{GT}_0$-orbit of $D$.*

Proof. By Theorem 13(b) together with Theorem 11, the inverse limit of the groups $\mathcal{O}_4^{\#}(N_i)$ is isomorphic to $\mathcal{O}_4^{\#} \simeq \widehat{GT}_0$. Thus the descending intersection of the finite groups $\psi^4_{N_i,N_0}\big(\mathcal{O}^{\#}(N_i)\big)$ is equal to $\psi^4_{N_0}(\mathcal{O}_4^{\#}) = \mathcal{O}^{\#}_{4,N_0} \subset \mathcal{O}_4^{\#}(N_0)$. By finiteness, there exists an integer $I \geq 0$ such that $\psi^4_{N_i,N_0}\big(\mathcal{O}^{\#}(N_i)\big) = \mathcal{O}^{\#}_{4,N_0} \subset \mathcal{O}_4^{\#}(N_0)$ for all $i \geq I$. Since the actions of $\mathcal{O}_4^{\#}(N_i)$ and of $\mathcal{O}_4^{\#}$ factor through $\mathcal{O}_4^{\#}(N_0)$, the result follows. ♢

Thus this procedure computes the $\widehat{GT}_0$-orbit of a Galois dessin $D$, after finitely many steps. Since $G_{\mathbb{Q}} \subset \widehat{GT} \subset \widehat{GT}_0$, the $\widehat{GT}_0$-orbit of $D$ contains the $G_{\mathbb{Q}}$-orbit — but an even better approximation to the $G_{\mathbb{Q}}$-orbit would be obtained by computing the $\widehat{GT}$-orbit. That analogous construction is the subject of 3.5.

**3.5. Approximation of the $\widehat{GT}$-orbit of a dessin.** By using an analogue of the procedure of 3.4 with $\widehat{K}(0,5)$ replacing $\widehat{K}(0,4)$, we can find the $\widehat{GT}$-orbit of a dessin $D$ — thus separating more $G_{\mathbb{Q}}$-orbits and obtaining finer information about the field of moduli of the corresponding cover of $\mathbb{P}^1 - \{0,1,\infty\}$. As in 3.4 we rely on Theorem 11, to identify $\widehat{GT}$ with $\widehat{K}(0,5)$. As before, we identify $\widehat{K}(0,4)$ with a subgroup of $\widehat{K}(0,5)$ via the injection $\iota : x_{12} \mapsto x_{12},\ x_{23} \mapsto x_{23}$. Recall that $\iota$ is a section of the surjection $p_4 : \widehat{K}(0,5) \twoheadrightarrow \widehat{K}(0,4) \simeq \langle x_{12}, x_{23}\rangle$, and yields a decomposition $\widehat{K}(0,5) \simeq \langle x_{14}, x_{24}, x_{34}\rangle \rtimes \langle x_{12}, x_{23}\rangle$.

So let $D$ be a $G$-Galois dessin and let $N$ be the corresponding normal subgroup in $\widehat{K}(0,4) \simeq \widehat{F}_2$. Thus $G \simeq \widehat{K}(0,4)/N \simeq \widehat{K}(0,5)/M$, where $M = p_4^{-1}(N) \simeq \langle x_{14}, x_{24}, x_{34}\rangle \rtimes N$. By Theorem 7, there is a natural action of $\mathcal{O}_5^{\#}$ on the set of $G$-Galois dessins. So the $\mathcal{O}_5^{\#}$-orbit of $D$ contains the $G_{\mathbb{Q}}$-orbit, and is in turn contained in the $\mathcal{O}_4^{\#}$-orbit (by the compatibility of the $\mathcal{O}_4^{\#}$- and $\mathcal{O}_5^{\#}$-actions [HS, 2.2]). If $\breve{M} \subset \mathcal{O}_5^{\#}$ is any finite index characteristic subgroup contained in $M$, the action of $\mathcal{O}_5^{\#}$ factors through the finite group $\mathcal{O}^{\#}_{5,\breve{M}}$ — and so the $\widehat{GT}$-orbit of $D$ is the same as the $\mathcal{O}^{\#}_{5,\breve{M}}$-orbit (and is equal to the set $\mathcal{O}_5^{\#}/M$ of §2). As in 3.4, though, it is unclear how to find exactly which elements of the finite group $\mathrm{Out}(G)$ lie in $\mathcal{O}^{\#}_{5,\breve{M}}$.

Thus, as with $\widehat{GT}_0$, we take an indirect approach to finding the $\widehat{GT}$-orbit, by using that we can find the elements of the (possibly) larger finite group $\mathcal{O}_5^{\#}(\breve{M}) \subset \mathrm{Out}(G)$, along with the fact that the $\mathcal{O}^{\#}_{5,\breve{M}}$-action extends to an $\mathcal{O}_5^{\#}(\breve{M})$-action. Namely, for $\overline{F} \in \mathcal{O}_5^{\#}(\breve{M})$, if $F \in \mathrm{Aut}(\widehat{K}(0,5)/\breve{M})$ is any lifting of $\overline{F}$, then we define $D_{\overline{F}}$ to be the $G$-Galois dessin corresponding to

the uniform conjugacy class of the pair $\left(\left(F\left((x_{12})_{\breve{M}}\right)\right)_M, \left(F\left((x_{23})_{\breve{M}}\right)\right)_M\right) \in (\widehat{K}(0,5)/M)^2 \simeq (\widehat{K}(0,4)/N)^2 \simeq G^2$. This equivalence class is well-defined, since conjugacy in $\widehat{K}(0,5)/\breve{M}$ maps to conjugacy in $G = \widehat{K}(0,5)/M$. We call the orbit of $D$ under $\mathcal{O}_5^{\#}(\breve{M})$ the *$\breve{M}$-approximative $\widehat{GT}$-orbit of $D$*.

As in 3.4, we can thus explicitly compute the $\breve{M}$-approximative $\widehat{GT}$-orbit of any $G$-Galois dessin $D$, where $G = \widehat{K}(0,4)/N$:

(1′) Let $\breve{M}$ be any characteristic subgroup of finite index in $\widehat{K}(0,5)$ that is contained in $M = p_4^{-1}(N)$ — e.g. choose $\breve{M}$ as in the proof of Lemma 12.

(2′) Compute the finite group $\mathcal{O}_5^{\#}(\breve{M})$ from the definition.

(3′) Compute $\left(\left(F\left((x_{12})_{\breve{M}}\right)\right)_M, \left(F\left((x_{23})_{\breve{M}}\right)\right)_M\right) \in G^2$ for each $\overline{F} \in \mathcal{O}_5^{\#}(\breve{M})$.

Again as in 3.4, by taking smaller and smaller choices of $\breve{M}$, we can compute the actual $\widehat{GT}$-orbit of $D$ in finitely many steps. Namely, again by Lemma 12, there is a cofinal sequence of finite index characteristic subgroups $M_0 \subset M_1 \subset \cdots$ of $\widehat{K}(0,5)$ inside $M = p_4^{-1}(N)$ for any given normal subgroup $N \subset \widehat{K}(0,4)$ of finite index. We then obtain the following $\widehat{GT}$-version of the corollary in 3.4, whose proof is essentially the same as before:

**Corollary.** *Let $D$ be a $G$-Galois dessin, corresponding to a normal subgroup $N \subset \widehat{K}(0,4)$ of finite index. Let $\{M_i\}$ be a cofinal sequence of finite index characteristic subgroups of $\widehat{K}(0,5)$ contained in $M = p_4^{-1}(N)$. Then for all $i \gg 0$, the $M_i$-approximative $\widehat{GT}$-orbit of $D$ is equal to the $\widehat{GT}$-orbit of $D$.*

This procedure thus computes the $\widehat{GT}$-orbit of a Galois dessin $D$ after finitely many steps, and so approximates (and conjecturally equals) the $G_{\mathbb{Q}}$-orbit of $D$. This complements the construction of §2 (just as that of 3.4 complements the construction of §1). Unlike the constructions in sections 1 and 2, though, the procedure here (and in 3.4) is not effective, because we do not know how to determine *a priori* how large $i$ should be, or even when we have reached the goal! To be better able to exploit this construction, we would thus like to be able to solve the following

**Problem.** Given a normal subgroup $N \subset \widehat{F}_2$ of finite index, corresponding to a $G$-Galois dessin $D$ (where $G = \widehat{F}_2/N$), find a characteristic subgroup $M \subset \widehat{K}(0,5)$ of finite index such that the $M$-approximative $\widehat{GT}$-orbit of $D$ is equal to the $\widehat{GT}$-orbit of $D$.

Still, successive steps of the above refining procedure either improve the approximation or leave it unchanged, and thus (even without solving this problem) they provide increasingly better information about the field of moduli of $D$ — which can be used as in 3.6 below.

**3.6. Stabilizers and fields of moduli.** The above approach may be used to obtain explicit information about the field of moduli $K$ of a $G$-Galois dessin $D$ (i.e. of the corresponding $G$-Galois cover $X \to \mathbb{P}^1 - \{0, 1, \infty\}$). For example, the degree $[K : \mathbb{Q}]$ is equal to the order of the $G_{\mathbb{Q}}$-orbit of $D$ (or of $X$), since that order is the index of the stabilizer $G_{\mathbb{Q}}^D$ of $D$ in $G_{\mathbb{Q}}$, and hence is the degree of the fixed field of $G_{\mathbb{Q}}^D$ — i.e. the degree of the field of moduli. Since the $\widehat{GT}$-orbit contains the $G_{\mathbb{Q}}$-orbit, and since any $\breve{M}$-approximative $\widehat{GT}$-orbit of $D$ contains the $\widehat{GT}$-orbit, we obtain

**Proposition 14.** *Let $K$ be the field of moduli of a $G$-Galois dessin $D$, where $G = \widehat{K}(0,4)/N$. Then $[K : \mathbb{Q}]$ is bounded above by the order of the $\breve{M}$-approximative $\widehat{GT}$-orbit of $D$, for any finite index characteristic subgroup $\breve{M} \subset M = p_4^{-1}(N)$ of $\widehat{K}(0,5)$.*

The approximative $\widehat{GT}$-actions, i.e. the actions of the $\mathcal{O}_5^{\#}(\breve{M})$'s on dessins, also provide computable information about the Galois group of the field of moduli $K$ of a $G$-Galois dessin $D$. Below, we write $\psi_N^{5\#} : \mathcal{O}_5^{\#} \twoheadrightarrow \mathcal{O}_{5,\breve{M}}^{\#}$ for the restriction of the map $\psi_N^5 : \mathcal{O}_5 \twoheadrightarrow \mathcal{O}_{5,\breve{M}}$ (cf. 3.2 and Theorem 13). Also, if a group $\Gamma$ acts on a set of $G$-Galois dessins, we denote the stabilizer of $D$ in $\Gamma$ by $\Gamma^D$, and the intersection of the conjugates of $\Gamma^D \subset \Gamma$ by $C^D(\Gamma)$.

**Proposition 15.** *(a) With notation as above, let $\tilde{K}$ be the Galois closure of $K$. Then $\mathrm{Gal}(\tilde{K}/\mathbb{Q})$ is a subquotient of each $\mathcal{O}_5^{\#}(\breve{M})/C^D(\mathcal{O}_5^{\#}(\breve{M}))$.*

*(b) If $\mathcal{O}_5^{\#}(\breve{M})^D$ is normal in $\mathcal{O}_5^{\#}(\breve{M})$, then $K/\mathbb{Q}$ is Galois, and $\mathrm{Gal}(K/\mathbb{Q})$ is a subgroup of $\mathcal{O}_5^{\#}(\breve{M})/\mathcal{O}_5^{\#}(\breve{M})^D$.*

Proof. Since $C^D(\mathcal{O}_5^{\#}(\breve{M}))$ is normal in $\mathcal{O}_5^{\#}(\breve{M})$ and contained in $\mathcal{O}_5^{\#}(\breve{M})^D$, we have that $C_{\breve{M}}^D := C^D(\mathcal{O}_5^{\#}(\breve{M})) \cap \mathcal{O}_{5,\breve{M}}^{\#}$ is normal in $\mathcal{O}_{5,\breve{M}}^{\#}$ and contained in $(\mathcal{O}_{5,\breve{M}}^{\#})^D$. So $C_{\breve{M}}^D \subset C^D(\mathcal{O}_{5,\breve{M}}^{\#})$, and $\mathcal{O}_{5,\breve{M}}^{\#}/C_{\breve{M}}^D \subset \mathcal{O}_5^{\#}(\breve{M})/C^D(\mathcal{O}_5^{\#}(\breve{M}))$. Since the action of $\widehat{GT} \simeq \mathcal{O}_5^{\#}$ on the orbit of $D$ factors through $\mathcal{O}_{5,\breve{M}}^{\#}$ via $\psi_N^{5\#}$ (cf. 3.4), we have that $(\psi_N^{5\#})^{-1}(C_{\breve{M}}^D) \subset C^D(\mathcal{O}_5^{\#})$ and $\mathcal{O}_5^{\#}/(\psi_N^{5\#})^{-1}(C_{\breve{M}}^D) = \mathcal{O}_{5,\breve{M}}^{\#}/C_{\breve{M}}^D$. Since the action of $G_{\mathbb{Q}}$ on dessins factors through $\mu : G_{\mathbb{Q}} \hookrightarrow \mathcal{O}_5^{\#}$, $(\psi_N^{5\#}\mu)^{-1}(C_{\breve{M}}^D) \subset C^D(G_{\mathbb{Q}})$ and $G_{\mathbb{Q}}/(\psi_N^{5\#}\mu)^{-1}(C_{\breve{M}}^D) \subset \mathcal{O}_5^{\#}/(\psi_N^{5\#})^{-1}(C_{\breve{M}}^D)$. Combining the above equalities and inclusions, we have that $\mathrm{Gal}(\tilde{K}/\mathbb{Q}) = G_{\mathbb{Q}}/C^D(G_{\mathbb{Q}})$ is a quotient of $G_{\mathbb{Q}}/(\psi_N^{5\#}\mu)^{-1}(C_{\breve{M}}^D)$, which in turn is a subgroup of $\mathcal{O}_5^{\#}(\breve{M})/C^D(\mathcal{O}_5^{\#}(\breve{M}))$. This proves (a).

For (b), observe that ${G_{\mathbb{Q}}}^D$ is the inverse image of $\mathcal{O}_5^{\#}(\breve{M})^D$ under the composition $G_{\mathbb{Q}} \hookrightarrow \widehat{GT} \xrightarrow{\sim} \mathcal{O}_5^{\#} \twoheadrightarrow \mathcal{O}_{5,\breve{M}}^{\#} \hookrightarrow \mathcal{O}_5^{\#}(\breve{M})$, since the action of $G_{\mathbb{Q}}$ on the orbit of $D$ factors through these maps. Since $\mathcal{O}_5^{\#}(\breve{M})^D$ is normal in $\mathcal{O}_5^{\#}(\breve{M})$, it follows that $G_{\mathbb{Q}}^D$ is normal in $G_{\mathbb{Q}}$, so that $K$ is Galois over $\mathbb{Q}$.

It also follows that $\mathcal{O}_5^{\#}(\breve{M})^D = C^D(\mathcal{O}_5^{\#}(\breve{M}))$. Thus $(\psi_N^{5\#}\mu)^{-1}(C^D_{\breve{M}})$, which is the inverse image of $C^D(\mathcal{O}_5^{\#}(\breve{M}))$ under the above composition, is equal to $G_{\mathbb{Q}}^D$. So $\mathrm{Gal}(K/\mathbb{Q})$ equals $(\psi_N^{5\#}\mu)^{-1}(C^D_{\breve{M}})$, which was observed to be a subgroup of $\mathcal{O}_5^{\#}(\breve{M})/C^D(\mathcal{O}_5^{\#}(\breve{M})) = \mathcal{O}_5^{\#}(\breve{M})/\mathcal{O}_5^{\#}(\breve{M})^D$. ♢

It is also possible to use the actions of the $\mathcal{O}_5^{\#}(\breve{M})$'s in order to find cyclotomic number fields that contain the field of moduli of a given $G$-Galois dessin (and thus, when $G$ has trivial center, over which the corresponding $G$-Galois cover is defined [CH, 2.8(c)]). For $m \in \mathbb{Z}$, let $\mathcal{O}_n^{\#}(\breve{M})_m \subset \mathcal{O}_n^{\#}(\breve{M})$ be the subgroup of elements for which we may take $\lambda \equiv 1 (\mathrm{mod}\, m)$ in (i) of the definition of $\mathcal{O}_n^{\#}(\breve{M})$ (in 3.2).

**Proposition 16.** *(a) If some $\mathcal{O}_n^{\#}(\breve{M})_0$ stabilizes a $G$-Galois dessin $D$, then the corresponding $G$-Galois cover is defined over $\mathbb{Q}^{\mathrm{ab}}$.*

*(b) If $m > 0$ and some $\mathcal{O}_n^{\#}(\breve{M})_m$ stabilizes a $G$-Galois dessin $D$, then the field of moduli of the corresponding $G$-Galois cover is contained in $\mathbb{Q}(\zeta_m)$.*

Proof. Under $G_{\mathbb{Q}} \to \mathcal{O}_5^{\#}(\breve{M})$, $G_{\mathbb{Q}^{\mathrm{ab}}}$ maps to $\mathcal{O}_n^{\#}(\breve{M})_0$ and $G_{\mathbb{Q}(\zeta_m)}$ maps to $\mathcal{O}_n^{\#}(\breve{M})_m$ for $m > 0$. So $\mathbb{Q}^{\mathrm{ab}}$ and $\mathbb{Q}(\zeta_m)$ contain the respective fields of moduli. This proves (b), and (a) then follows by [CH, 2.8(a)]. ♢

In particular, taking $m = 1$, we conclude that if some $\mathcal{O}_5^{\#}(\breve{M})$ stabilizes a $G$-Galois dessin $D$, then the field of moduli of $D$ is equal to $\mathbb{Q}$.

Note that one may obtain stronger conclusions from the above results not only by shrinking $\breve{M}$, but also by replacing $\mathcal{O}_5^{\#}(\breve{M})$ by a smaller subgroup $\mathcal{O}_5^{\circ}(\breve{M})$ that is known to contain $\mathcal{O}^{\#}_{5,\breve{M}}$. Because of Theorem 7, the definition of $A_5$, and the fact that the automorphism $\theta \in \mathrm{Aut}(\widehat{K}(0,5))$ defined by $\theta(x_{i,i+1}) = x_{5-i,6-i}$ descends to an automorphism $\theta$ of $\widehat{K}(0,5)/\breve{M}$, we may in particular take $\mathcal{O}_5^{\circ}(\breve{M})$ to consist of the elements $\overline{F} \in \mathcal{O}^{\#}_{5,\breve{M}} \subset \mathrm{Out}(\widehat{K}(0,5)/\breve{M})$ having a lifting $F \in \mathrm{Aut}(\widehat{K}(0,5)/\breve{M})$ for which there is an $f \in \langle (x_{12})_{\breve{M}}, (x_{23})_{\breve{M}} \rangle$ with $F\big((x_{12})_{\breve{M}}\big) = (x_{12})^{\lambda}_{\breve{M}}$; $F\big((x_{23})_{\breve{M}}\big) = f^{-1}(x_{23})^{\lambda}_{\breve{M}} f$; $F\big((x_{34})_{\breve{M}}\big) = \theta(f)^{-1}(x_{34})^{\lambda}_{\breve{M}}\theta(f)$; and $F\big((x_{45})_{\breve{M}}\big) = (x_{45})^{\lambda}_{\breve{M}}$. (One could shrink $\mathcal{O}_5^{\circ}(\breve{M})$ further by also using $F\big((x_{51})_{\breve{M}}\big)$, via the expression (**) in 0.1 and the analogous result for $\mathcal{O}_5^{\#}$ in [HS, 2.2].)

The above raises several questions: For a given characteristic subgroup $\breve{M} \subset M = p_4^{-1}(N)$, to what extent does $\mathcal{O}_5^{\circ}(\breve{M})$ yield better information about the field of moduli and the Galois orbit than just using $\mathcal{O}_5^{\#}(\breve{M})$? As $\breve{M}$ shrinks, how fast does the information given by $\mathcal{O}_5^{\#}(\breve{M})$ improve? To what extent does the information given by $\mathcal{O}_5^{\#}(\breve{M})$ go beyond that given by $\mathcal{O}_4^{\#}(\breve{N})$, where $\breve{N} = p_4(\breve{M}) \subset \widehat{K}(0,4)$? And to what extent do computations using the above give information beyond that obtainable by rigidity?

**References**


[B] G.V. Belyi, On Galois extensions of a maximal cyclotomic field, *Math. USSR Izvestija* (translations) **14** (1980), No. 2, 247-256.

[CH] K. Coombes and D. Harbater, Hurwitz families and arithmetic Galois groups, *Duke Math. J.* **52** (1985), 821-839.

[D] V.G. Drinfel'd, On quasitriangular quasi-Hopf algebras and a group closely connected with $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, *Leningrad Math. J.* Vol. 2 (1991), No. 4, 829-860.

[F1] M. Fried, Fields of definition of function fields and Hurwitz families — groups as Galois groups, *Comm. Alg.* **5** (1977), 17-82.

[F2] M. Fried, Introduction to Modular Towers: Generalizing dihedral group–modular curve connections, in *Recent Developments in the Inverse Galois Problem*, M. Fried et al., Eds., AMS Contemp. Math. Series, vol. 186, 1995, 111-171.

[G] A. Grothendieck, Revêtements étales et groupe fondamental (SGA 1). Lecture Notes in Math. **224**, Springer-Verlag, Berlin-Heidelberg-New York, 1971.

[GTD] *The Grothendieck Theory of Dessins d'Enfants*, L. Schneps, ed., London Math. Soc. Lecture Notes **200**, Cambridge University Press, 1994.

[HS] D. Harbater and L. Schneps, Fundamental groups of moduli and the Grothendieck-Teichmüller group, preprint.

[I1] Y. Ihara, Braids, Galois groups, and some arithmetic functions, Proceedings of the ICM, Kyoto, Japan, 1990, 99-120.

[I2] Y. Ihara, On the embedding of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ into $\widehat{GT}$, in [GTD].

[IM] Y. Ihara and M. Matsumoto, On Galois Actions of Profinite Completions of Braid Groups, in *Recent Developments in the Inverse Galois Problem*, M. Fried et al., Eds., AMS Contemp. Math. Series, vol. 186, 1995, 173-200.

[LS] P. Lochak and L. Schneps, The Grothendieck-Teichmüller group as automorphisms of braid groups, in [GTD].

[M] B.H. Matzat, Zur Konstruction von Zahl- und Funktionkorpern mit vorgegebener Galoisgruppe, *J. reine angew. Math.* **349** (1984), 179-220.

[N] H. Nakamura, Galois rigidity of pure sphere braid groups and profinite calculus, *J. Math. Sci. Univ. Tokyo* **1** (1994), 71-136.

[S] J-P. Serre, Deux lettres sur la cohomologie non abélienne, this volume.

[T] J. Thompson, Some finite groups which appear as Gal $L/K$, where $K \subset \mathbb{Q}(\mu_n)$, *J. Algebra* **89** (1984), 437-499.