



Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

On representations of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $\widehat{GT}$ and $\text{Aut}(\widehat{F}_2)$ Frauke M. Bleher^{a,*}, Ted Chinburg^b, Alexander Lubotzky^c^a Department of Mathematics, University of Iowa, 14 MacLean Hall, Iowa City, IA 52242-1419, USA^b Department of Mathematics, University of Pennsylvania, Philadelphia, PA 19104-6395, USA^c Einstein Institute of Mathematics, Hebrew University, Givat Ram, Jerusalem 91904, Israel

ARTICLE INFO

Article history:

Received 20 January 2021

Available online 8 June 2021

Communicated by Robert Guralnick

In memory of Jan Saxl

MSC:

primary 14G32

secondary 20F34, 14H30

Keywords:

Belyi map

Galois group

Grothendieck-Teichmüller group

Representations

Automorphism groups

Free profinite groups

ABSTRACT

By work of Belyi [2], the absolute Galois group $G_{\mathbb{Q}} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of the field $\mathbb{Q}$ of rational numbers can be embedded into $A = \text{Aut}(\widehat{F}_2)$, the automorphism group of the free profinite group $\widehat{F}_2$ on two generators. The image of $G_{\mathbb{Q}}$ lies inside $\widehat{GT}$, the Grothendieck-Teichmüller group. While it is known that every abelian representation of $G_{\mathbb{Q}}$ can be extended to $\widehat{GT}$, Lochak and Schneps [13] put forward the challenge of constructing irreducible non-abelian representations of $\widehat{GT}$. We do this virtually, namely by showing that a rich class of arithmetically defined representations of $G_{\mathbb{Q}}$ can be extended to finite index subgroups of $\widehat{GT}$. This is achieved, in fact, by extending these representations all the way to finite index subgroups of $A = \text{Aut}(\widehat{F}_2)$. We do this by developing a profinite version of the work of Grunewald and Lubotzky [7], which provided a rich collection of representations for the discrete group $\text{Aut}(F_d)$.

© 2021 Elsevier Inc. All rights reserved.

* Corresponding author.

E-mail addresses: frauke-bleher@uiowa.edu (F.M. Bleher), ted@math.upenn.edu (T. Chinburg), alex.lubotzky@mail.huji.ac.il (A. Lubotzky).

1. Introduction

Let $G_{\mathbb{Q}} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group of the field $\mathbb{Q}$ of rational numbers. Let $A = \text{Aut}(\widehat{F}_2)$ be the automorphism group of the free profinite group $\widehat{F}_2$ on two generators. Belyĭ showed in [2] that there is a canonical embedding ι of $G_{\mathbb{Q}}$ into A (see §3 for details). In [3], Drinfel'd defined the so-called Grothendieck-Teichmüller group whose profinite version $\widehat{GT}$ is a certain subgroup of A that contains the image of $G_{\mathbb{Q}}$ under ι . For background on $\widehat{GT}$ and on variants of this group, see [8,17] and [13]. Thus $\iota(G_{\mathbb{Q}}) \leq \widehat{GT} \leq A$, and much effort has been dedicated to understanding the connection between $G_{\mathbb{Q}}$ and $\widehat{GT}$. It is known that every homomorphism from $G_{\mathbb{Q}}$ to an abelian group can be extended to $\widehat{GT}$ (see, for example, [17, §1.4(6)]) but no similar result is known for non-abelian quotients. In [13, p. 179], Lochak and Schneps wrote that “no irreducible non-abelian representation of any version of (the Grothendieck-Teichmüller group) has been constructed to date.” The goal of this paper is to address this challenge. Our main results will show that many naturally constructed representations of $G_{\mathbb{Q}}$ can be extended to $\widehat{GT}$, at least virtually, i.e. to a finite index subgroup. The main point of our work is that instead of trying to extend a representation from $G_{\mathbb{Q}}$ to $\widehat{GT}$, we extend it further all the way to a representation of a finite index subgroup of $A = \text{Aut}(\widehat{F}_2)$, and thus in particular to a finite index subgroup of $\widehat{GT}$. What makes this possible is adapting, to the profinite world, the work of Grunewald and Lubotzky in [7]. They constructed many linear representations of the discrete group $\text{Aut}(F_d)$ and showed that these provide surjections of $\text{Aut}(F_d)$ onto various arithmetic groups. It turns out that the analogous profinite theory is easier than the discrete one (see below) and leads to stronger results. In particular, this approach works for $A = \text{Aut}(\widehat{F}_2)$, while the discrete theory has given interesting results for $\text{Aut}(F_d)$ only when $d \geq 3$. As an illustrative example, we will show the following result in connection with the challenge of Lochak and Schneps:

Theorem 1.1. *Suppose $t > 1$ is an odd integer. Let ζ be a primitive t^{th} root of unity, and let E_{ζ} be the elliptic curve with affine equation*

$$y^2 = x(x-1)(x-\zeta).$$

There is a number field F over which E_{ζ} is defined, with the following property for every prime ℓ . The action of the finite index subgroup $G_F = \text{Gal}(\overline{\mathbb{Q}}/F)$ of $G_{\mathbb{Q}}$ on the ℓ -adic Tate module $T_{\ell}(E_{\zeta})$ can be extended to an action of a finite index subgroup $A_{E_{\zeta}}$ of A that contains the image of G_F under the Belyĭ embedding $\iota : G_{\mathbb{Q}} \rightarrow A$. Let $\tau_{\zeta,\ell} : A_{E_{\zeta}} \rightarrow \text{GL}(\mathbb{Q}_{\ell} \otimes_{\mathbb{Z}_{\ell}} T_{\ell}(E_{\zeta}))$ be the associated representation of $A_{E_{\zeta}}$ over $\mathbb{Q}_{\ell}$. Suppose the value $\phi(t)$ of Euler's phi function on t is larger than 24. Then the restriction of $\tau_{\zeta,\ell}$ to any subgroup between $A_{E_{\zeta}}$ and $\iota(G_F)$ is absolutely irreducible and non-abelian. This is true, in particular, for the restriction of $\tau_{\zeta,\ell}$ to the finite index subgroup $\widehat{GT} \cap A_{E_{\zeta}}$ of $\widehat{GT}$.

We now state a more general result concerning arbitrary smooth projective curves X defined over $\overline{\mathbb{Q}}$. By a theorem of Belyĭ [1, Theorem 4], X can be realized as a cover $\lambda : X \rightarrow \mathbb{P}_{\overline{\mathbb{Q}}}^1$ that is unramified outside $\{0, 1, \infty\}$. Suppose F is a number field over which X , the points in $\lambda^{-1}(\{0, 1, \infty\})$ and the generalized Jacobian $J_\lambda(X)$ of X with respect to $\lambda^{-1}(\{0, 1, \infty\})$ are defined. Let $T_{\ell, \lambda}(X)$ denote the ℓ -adic Tate module of $J_\lambda(X)$. This is a $\mathbb{Z}_\ell$ -module of rank $2 \text{genus}(X) + |\lambda^{-1}(\{0, 1, \infty\})| - 1$. The finite index subgroup $G_F = \text{Gal}(\overline{\mathbb{Q}}/F)$ of $G_{\overline{\mathbb{Q}}}$ acts naturally on $T_{\ell, \lambda}(X)$ and on the adelic Tate module

$$T_\lambda(X) := \prod_{\ell \text{ prime}} T_{\ell, \lambda}(X)$$

of $J_\lambda(X)$. This gives rise to Galois representations, which we denote by

$$\rho_{X, \ell} : G_F \rightarrow \text{GL}(T_{\ell, \lambda}(X)) \quad \text{and} \quad \rho_X : G_F \rightarrow \text{GL}(T_\lambda(X)).$$

Theorem 1.2. *There is a representation $\tilde{\rho}_X : A_X \rightarrow \text{GL}(T_\lambda(X))$ of a finite index subgroup A_X of A that agrees with ρ_X on the finite index subgroup $G_F \cap \iota^{-1}(A_X)$ of G_F . In particular, the same holds for every $\rho_{X, \ell}$ that is extended to $\tilde{\rho}_{X, \ell} : A_X \rightarrow \text{GL}(T_{\ell, \lambda}(X))$.*

To prove Theorem 1.2, let us recall the results in [7], which are not needed here, but which were the inspiration for the current work. In that paper, the following situation was studied. Let $F = F_d$ be the free group on $d \geq 2$ generators and let $\pi : F_d \rightarrow H$ be an epimorphism onto a finite group H , with $\mathcal{R} = \text{Ker}(\pi)$. Let $\mathcal{A} = \text{Aut}(F_d)$ and $\mathcal{A}(\pi) = \{\alpha \in \mathcal{A} : \pi \circ \alpha = \pi\}$. The finite index subgroup $\mathcal{A}(\pi)$ of $\mathcal{A}$ preserves $\mathcal{R}$. Hence, we get a linear representation $\rho_\pi : \mathcal{A}(\pi) \rightarrow \text{GL}(\overline{\mathcal{R}})$, where $\overline{\mathcal{R}} = \mathcal{R}/[\mathcal{R}, \mathcal{R}]$ is a $\mathbb{Z}$ -module of rank $|H|(d-1)+1$. The image of ρ_π is inside the arithmetic group of all the H -module automorphisms of $\overline{\mathcal{R}}$. The main result of [7] is the claim that **under some technical condition on π** (“ π is redundant”) $\rho_\pi(\mathcal{A}(\pi))$ is, after projectivization, an arithmetic group. This provides a rich class of arithmetic virtual quotients of $\mathcal{A} = \text{Aut}(F_d)$.

In §2, we develop the analogous profinite theory for all $d \geq 1$. Let π now be a continuous epimorphism $\pi : \widehat{F}_d \rightarrow H$, and let $A(\pi) = \{\alpha \in \text{Aut}(\widehat{F}_d) : \pi \circ \alpha = \pi\}$. Let $R = \text{Ker}(\pi)$. Then $\overline{R} = R/[R, R]$ is a $\widehat{\mathbb{Z}}[H]$ -module giving rise to $\rho : A(\pi) \rightarrow \text{GL}(\overline{R})$. The result here is stronger than in the discrete case and without any assumption:

Theorem 1.3. *For every $d \geq 1$ and every such π , the image $\rho(A(\pi))$ equals the subgroup $\text{Aut}_{H, \beta}(\overline{R})$ of all $\widehat{\mathbb{Z}}[H]$ -module automorphisms of $\overline{R}$ preserving the extension class β of the short exact sequence*

$$1 \rightarrow \overline{R} \rightarrow \widehat{F}_d/[R, R] \xrightarrow{\overline{\pi}} H \rightarrow 1 \tag{1.1}$$

where $\overline{\pi}$ is induced by π .

See Theorem 2.1 below for an even more general result. This theorem is deduced from a powerful lemma of Gaschütz which holds for (pro)finite groups but not for discrete groups. This explains why Theorem 1.3 does not hold in general for discrete groups; see also [7, Prop. 9.7].

Theorems 1.2 and 1.3 are connected with each other because of Belyĭ's theorem. Let H be the Galois group of the normal closure $\tilde{\lambda} : Y \rightarrow \mathbb{P}_{\mathbb{Q}}^1$ of a Belyĭ cover $\lambda : X \rightarrow \mathbb{P}_{\mathbb{Q}}^1$, and let $\mathcal{J}$ be the Galois group of Y over X . The étale fundamental group of $\mathbb{P}_{\mathbb{Q}}^1 - \{0, 1, \infty\}$ with respect to a geometric base point is naturally isomorphic to the free profinite group $\widehat{F}_2$. Letting $\pi : \widehat{F}_2 \rightarrow H$ be the homomorphism associated to $\tilde{\lambda}$, we get from Theorem 1.3 a lift to a finite index subgroup of $A(\pi)$ of the action of a subgroup of finite index in $G_{\mathbb{Q}}$ on $T_{\tilde{\lambda}}(Y)$. Taking $\mathcal{J}$ -coinvariants of this lift and then dividing by the finite torsion subgroup of these coinvariants leads to Theorem 1.2; see Theorem 4.1 for details.

One natural question is whether similar results hold if one replaces the adelic Tate module $T_{\lambda}(X)$ of the generalized Jacobian of X with respect to the ramification locus of $\lambda : X \rightarrow \mathbb{P}_{\mathbb{Q}}^1$ with the adelic Tate module $T(X)$ of the Jacobian of X . Using Theorem 1.2, we will give in §5 a sufficient condition for the lift of the action on $T_{\lambda}(X)$ which we construct to descend to an action on $T(X)$; see Theorem 5.1. If $X = Y$ then this condition is also necessary. The condition is not always satisfied, but it is if, for example, the Galois group H of the normal closure of λ is abelian. Theorem 1.1 is proved by applying Theorem 5.1 to a suitable Belyĭ cover when $X = E_C$.

Theorem 1.3 gives the precise image of $A(\pi)$ in $\mathrm{GL}(\overline{R})$ and hence also in $\mathrm{GL}(T_{\lambda}(X))$. It is of interest to compare it with the image of G_F in $\mathrm{GL}(T_{\lambda}(X))$. In §6 we analyze the case in which X has genus 1 and $\lambda : X \rightarrow \mathbb{P}_{\mathbb{Q}}^1$ is Galois.

We end this introduction with some comments and questions. The main open question concerning the Grothendieck-Teichmüller group $\widehat{GT}$ is whether there is a variant of this group that is equal to the image of $G_{\mathbb{Q}}$ under the Belyĭ embedding $\iota : G_{\mathbb{Q}} \rightarrow A$. If this is true then every linear representation of $G_{\mathbb{Q}}$ must lift to the variant of $\widehat{GT}$. In view of Theorems 1.1 and 1.2 above, it would be interesting to find other natural representations of finite index subgroups of $G_{\mathbb{Q}}$ that lift to representations of finite index subgroups of A . For example, the Galois representations provided by the adelic Tate modules of the Jacobians of modular curves arise in the theory of modular forms of weight two for congruence subgroups of $\mathrm{PSL}_2(\mathbb{Z})$; see, for example, [20] and [10]. It would be interesting if other Galois representations provided by modular forms of other weights, and more generally by Λ -adic modular forms, have lifts to finite index subgroups of A . At a minimum, one would like to check whether such representations can be lifted to finite index subgroups of the Grothendieck-Teichmüller group $\widehat{GT}$. For related questions of this kind, see the end of [13, §1].

Acknowledgments. The first and second authors would like to thank the Hebrew University in Jerusalem for its support and hospitality during work on this paper. The first author was supported in part by NSF FRG Grant No. DMS-1360621 and by NSF Grant No. DMS-1801328. The second author was supported in part by NSF FRG Grant

No. DMS-1360767, NSF SaTC Grants No. CNS-1513671 and CNS-1701785, and Simons Foundation Grant No. 338379. The third author is indebted for support from the NSF (Grant No. DMS-1700165) and the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program (Grant No. 692854). This material is based upon work supported by a grant from the Institute for Advanced Study.

2. A construction of linear representations of $\text{Aut}(\widehat{F}_d)$

Let $\pi : \widehat{F}_d \rightarrow H$ be a continuous epimorphism from $\widehat{F}_d$ to a finite group H , and let R be the kernel of π . Define $\overline{R} = R/[R, R]$ to be the maximal abelian quotient of R . Then $\overline{R}$ is isomorphic to $\widehat{\mathbb{Z}}^{|H|(d-1)+1}$ where $\widehat{\mathbb{Z}}$ is the profinite completion of $\mathbb{Z}$. We consider surjections $R \rightarrow \tilde{R}$ whose kernel $\tilde{I}$ is a closed normal subgroup of $\widehat{F}_d$ containing $[R, R]$, so that $\tilde{R}$ is a quotient of $\overline{R}$. We will be interested in constructing large linear representations of the group

$$A(\pi, \tilde{I}) = \{\alpha \in \text{Aut}(\widehat{F}_d) : \pi \circ \alpha = \pi \quad \text{and} \quad \alpha(\tilde{I}) = \tilde{I}\} \quad (2.1)$$

where we set $A(\pi) = A(\pi, [R, R])$. Since $\widehat{F}_d$ is finitely generated as a profinite group, there are finitely many surjections $\widehat{F}_d \rightarrow H$, and $A(\pi)$ is of finite index in $\text{Aut}(\widehat{F}_d)$. In general, $A(\pi, \tilde{I})$ need not have finite index in $\text{Aut}(\widehat{F}_d)$, but it will if $\tilde{I}$ is a characteristic subgroup of R .

We have an exact sequence

$$1 \rightarrow \tilde{R} \rightarrow \widehat{F}_d/\tilde{I} \rightarrow H \rightarrow 1 \quad (2.2)$$

with some extension class $\beta \in H^2(H, \tilde{R})$. Since $\tilde{R}$ is abelian and profinite, there is a well-defined continuous action of H on $\tilde{R}$. This gives rise to a linear representation $\rho : A(\pi, \tilde{I}) \rightarrow \text{GL}(\tilde{R})$.

Let $\text{Aut}_H(\tilde{R})$ be the group of continuous automorphisms of $\tilde{R}$ that commute with the action of H . Each element of $\text{Aut}_H(\tilde{R})$ induces an automorphism of $H^2(H, \tilde{R})$. We define

$$\text{Aut}_{H,\beta}(\tilde{R}) = \{\gamma \in \text{Aut}_H(\tilde{R}) : \gamma_*(\beta) = \beta\}. \quad (2.3)$$

Since $\tilde{R}$ is a quotient of a finitely generated $\widehat{\mathbb{Z}}$ -module, $H^2(H, \tilde{R})$ is finite, and $\text{Aut}_{H,\beta}(\tilde{R})$ has finite index in $\text{Aut}_H(\tilde{R})$.

We will prove the following result, which implies Theorem 1.3.

Theorem 2.1. *For every $d \geq 1$ and every π and $\tilde{I}$, the image $\rho(A(\pi, \tilde{I}))$ equals $\text{Aut}_{H,\beta}(\tilde{R})$. In other words, the action of $A(\pi, \tilde{I})$ on $\tilde{R}$ gives a surjection*

$$A(\pi, \tilde{I}) \rightarrow \text{Aut}_{H,\beta}(\tilde{R}). \quad (2.4)$$

This construction is the profinite analog of the one used in [7] to construct linear representations of $\text{Aut}(F_d)$. Note, though, that Theorem 2.1 shows that in the profinite case the representation is surjective. In the discrete case this may not be true; see [7, Prop. 9.7]. Here is a concrete example.

Example 2.2. Let H be a cyclic group of prime order p , and let $k = \mathbb{Q}(\zeta_p)$ for a primitive p^{th} root of unity ζ_p in $\overline{\mathbb{Q}}$. Suppose $\pi : F_d \rightarrow H$ is a surjection with kernel $\mathcal{R}$. In this case, $\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{R}/[\mathcal{R}, \mathcal{R}]$ is isomorphic to $\mathbb{Q}[H]^{d-1} \oplus \mathbb{Q}$ as a $\mathbb{Q}[H]$ -module, i.e. to $k^{d-1} \oplus \mathbb{Q}^d$ (see, for example, [6, §2]). Theorem 1.4 of [7] implies that if $d \geq 3$, the finite index subgroup $\mathcal{A}(\pi)$ of $\mathcal{A} = \text{Aut}(F_d)$ has a “large” image in the H -module automorphism group of $k^{d-1} \oplus \mathbb{Q}^d$ in the following sense. After choosing a suitable basis for $\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{R}/[\mathcal{R}, \mathcal{R}] \cong k^{d-1} \oplus \mathbb{Q}^d$, the $\mathbb{Z}[H]$ submodule $\mathcal{R}/[\mathcal{R}, \mathcal{R}]$ is commensurable with $\mathbb{Z}[\zeta_p]^{d-1} \oplus \mathbb{Z}^d$, where a chosen generator $h \in H$ acts on $\mathbb{Z}[\zeta_p]$ by multiplication by ζ_p and h acts trivially on $\mathbb{Z}$. The intersection of $\rho_{\pi}(\mathcal{A}(\pi))$ with $\text{GL}_{d-1}(\mathbb{Z}[\zeta_p]) \times \text{GL}_d(\mathbb{Z})$ has finite index in $\rho_{\pi}(\mathcal{A}(\pi))$, and the intersection $\rho_{\pi}(\mathcal{A}(\pi)) \cap (\text{SL}_{d-1}(\mathbb{Z}[\zeta_p]) \times \text{SL}_d(\mathbb{Z}))$ is of finite index in $\text{SL}_{d-1}(\mathbb{Z}[\zeta_p]) \times \text{SL}_d(\mathbb{Z})$. This way it is shown in [7] that $\text{Aut}(F_d)$ has many arithmetic subgroups as quotients. It was left open in [7] whether the image $\rho_{\pi}(\mathcal{A}(\pi))$ is of finite index even in $\text{GL}_{d-1}(\mathbb{Z}[\zeta_p]) \times \text{GL}_d(\mathbb{Z})$. This is the question “(SL) or not (SL)?” discussed in [7, §8]. By using the recently proved result that $\text{Aut}(F_d)$ has Kazhdan property (T) for $d \geq 4$ (see [12], [11], [15]), so that the abelianization of each finite index subgroup is finite, it follows that (at least when $d \geq 4$), the answer to the “(SL) or not (SL)?” question is (SL). In other words, the image there is always commensurable with the SL group. So it is of infinite index in $\text{GL}_{d-1}(\mathbb{Z}[\zeta_p]) \times \text{GL}_d(\mathbb{Z})$ if $p > 3$.

Theorem 2.1 gives a more precise and stronger result in the category of profinite groups. As remarked above, $\overline{R} = R/[R, R] \cong \widehat{\mathbb{Z}}^{(d-1)p} \oplus \widehat{\mathbb{Z}}$. Concerning the action of H , we can prove a more precise statement if we divide $\overline{R}$ by its pro- p Sylow subgroup $\overline{R}(p)$ (i.e. by the $\mathbb{Z}_p$ -factors). Let $\tilde{I}$ be the inverse image of $\overline{R}(p)$ under the natural map $R \rightarrow \overline{R}$. Define

$$\widehat{\mathbb{Z}}_{(p)} = \widehat{\mathbb{Z}}/\mathbb{Z}_p \cong \prod_{\ell \neq p} \mathbb{Z}_{\ell}.$$

Then $\tilde{R} = \overline{R}/\overline{R}(p) = R/\tilde{I}$ is isomorphic to $\widehat{\mathbb{Z}}_{(p)}^{|H|(d-1)+1}$ but this time we can say that $\tilde{R}$ is isomorphic to $\widehat{\mathbb{Z}}_{(p)}[H]^{d-1} \oplus \widehat{\mathbb{Z}}_{(p)} \cong \widehat{\mathbb{Z}}_{(p)}[\zeta_p]^{d-1} \oplus \widehat{\mathbb{Z}}_{(p)}^d$ as an H -module since $|H|$ is a unit in $\widehat{\mathbb{Z}}_{(p)}$. Theorem 2.1 implies that $A(\pi, \tilde{I})$, which is a finite index subgroup of $\text{Aut}(\widehat{F}_d)$, is mapped **onto** $\text{GL}_{d-1}(\widehat{\mathbb{Z}}_{(p)}[\zeta_p]) \times \text{GL}_d(\widehat{\mathbb{Z}}_{(p)})$. (Note that $\text{SL}_{d-1}(\widehat{\mathbb{Z}}_{(p)}[\zeta_p]) \times \text{SL}_d(\widehat{\mathbb{Z}}_{(p)})$ is of infinite index in $\text{GL}_{d-1}(\widehat{\mathbb{Z}}_{(p)}[\zeta_p]) \times \text{GL}_d(\widehat{\mathbb{Z}}_{(p)})$.)

More examples of this kind can be worked out by considering the various examples studied in [7]. The advantage of Theorem 2.1 over [7, Theorem 4.1] is that it gives the exact image (and not only up to a finite index subgroup as in [7], and only under some additional assumptions on H and π). It implies that the question “(SL) or not (SL)?”

from [7, §8] has a clear answer here: it is never just SL. Moreover, a careful look at Example 2.2 shows that not only $\text{Aut}(\widehat{F}_d)$ has an infinite abelianization, since it clearly surjects onto $\text{GL}_d(\widehat{\mathbb{Z}})$ and hence onto $\widehat{\mathbb{Z}}^*$, but that also $\text{Aut}^1(\widehat{F}_d)$, which is defined as the preimage of $\text{SL}_d(\widehat{\mathbb{Z}})$, has a finite index subgroup with an infinite abelianization. This implies (at least for $d \geq 4$) that $\text{Aut}^1(F_d)$ is not dense in $\text{Aut}^1(\widehat{F}_d)$, since the former has property (T).

To prove Theorem 2.1 we need the following well-known result of Gaschütz; see [5] and [4, Lemma 17.7.2].

Lemma 2.3. *Suppose $\psi : G_1 \rightarrow G_2$ is a continuous surjective group homomorphism of profinite groups. Suppose S_2 is a finite set of generators of G_2 with $|S_2| = d$, and that the minimal number of generators of G_1 is less than or equal to d . Then there exists a set of generators S_1 of G_1 such that $\psi(S_1) = S_2$.*

This lemma has the following easy corollary (compare to [14, §2]).

Corollary 2.4. *If N is a closed normal subgroup of $\widehat{F}_d$, then every automorphism of $\widehat{F}_d/N$ can be lifted to an automorphism of $\widehat{F}_d$ preserving N . In particular, this holds for $N = R$.*

The identification of second group cohomology classes with equivalence classes of group extensions shows the following result.

Lemma 2.5. *Assume B is an abelian H -module and that there is a short exact sequence*

$$1 \longrightarrow B \longrightarrow \widetilde{H} \longrightarrow H \longrightarrow 1. \quad (2.5)$$

Let $\widetilde{\beta} \in H^2(H, B)$ be the extension class of this sequence. Let $\gamma : B \rightarrow B$ be an H -module automorphism. Then γ fixes $\widetilde{\beta}$ if and only if there is a diagram of automorphisms

$$\begin{array}{ccccccc} 1 & \longrightarrow & B & \longrightarrow & \widetilde{H} & \longrightarrow & H \longrightarrow 1 \\ & & \downarrow \gamma & & \downarrow \widetilde{\gamma} & & \parallel \\ 1 & \longrightarrow & B & \longrightarrow & \widetilde{H} & \longrightarrow & H \longrightarrow 1 \end{array} \quad (2.6)$$

in which the right vertical isomorphism is the identity map on H .

Proof of Theorem 2.1. An element of $A(\pi, \widetilde{I}) = \{\alpha \in \text{Aut}(\widehat{F}_d) : \pi \circ \alpha = \pi \text{ and } \alpha(\widetilde{I}) = \widetilde{I}\}$ induces an automorphism of the sequence (2.2) which is the identity on H . Therefore, Lemma 2.5 implies that the restriction of this element to $\widetilde{R}$ lies in $\text{Aut}_{H, \beta}(\widetilde{R})$. We now suppose that γ is an element of $\text{Aut}_{H, \beta}(\widetilde{R})$. By Lemma 2.5, there is an automorphism $\widetilde{\gamma}$ of $\widehat{F}_d/\widetilde{I}$ that fits in a diagram of automorphisms

$$\begin{array}{ccccccc}
 1 & \longrightarrow & \tilde{R} & \longrightarrow & \hat{F}_d/\tilde{I} & \longrightarrow & H \longrightarrow 1 \\
 & & \downarrow \gamma & & \downarrow \tilde{\gamma} & & \parallel \\
 1 & \longrightarrow & \tilde{R} & \longrightarrow & \hat{F}_d/\tilde{I} & \longrightarrow & H \longrightarrow 1.
 \end{array} \tag{2.7}$$

By Corollary 2.4, we can lift $\tilde{\gamma}$ to an automorphism α of $\hat{F}_d$. This lift will lie in $A(\pi, \tilde{I})$, which shows that the homomorphism in Theorem 2.1 is surjective. $\square$

3. Belyĭ's construction of an injection $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{Aut}(\hat{F}_2)$

In this section, we review a construction of Belyĭ in [1,2,8] of an injection $\iota : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{Aut}(\hat{F}_2)$ which is essential to our work. An explicit description of this construction is needed, in particular, to show that on passing to a finite index subgroup, it is compatible with the actions of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $\text{Aut}(\hat{F}_2)$ on the generalized Jacobians of curves.

We will identify $\mathbb{Q}(\mathbb{P}_{\mathbb{Q}}^1)$ with $\mathbb{Q}(t)$ for a fixed choice of affine parameter t . Then $\overline{\mathbb{Q}}(\mathbb{P}_{\mathbb{Q}}^1)$ is identified with $\overline{\mathbb{Q}}(t)$. Let $\overline{\mathbb{Q}}(t)^{\text{cl}}$ be a fixed algebraic closure of $\overline{\mathbb{Q}}(\mathbb{P}_{\mathbb{Q}}^1) = \overline{\mathbb{Q}}(t)$. We have an exact sequence of étale fundamental groups

$$1 \longrightarrow \pi_1(\mathbb{P}_{\mathbb{Q}}^1 - \{0, 1, \infty\}, \eta) \longrightarrow \pi_1(\mathbb{P}_{\mathbb{Q}}^1 - \{0, 1, \infty\}, \eta) \longrightarrow \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow 1 \tag{3.1}$$

when $\eta : \text{Spec}(\overline{\mathbb{Q}}(t)^{\text{cl}}) \longrightarrow \mathbb{P}_{\mathbb{Q}}^1 - \{0, 1, \infty\}$ is the geometric point determined by $\overline{\mathbb{Q}}(t)^{\text{cl}}$. This gives a homomorphism $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{Out}(\pi_1(\mathbb{P}_{\mathbb{Q}}^1 - \{0, 1, \infty\}, \eta))$. Belyĭ showed in [1,2] how one can lift this homomorphism to an injection

$$\iota : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{Aut}(\pi_1(\mathbb{P}_{\mathbb{Q}}^1 - \{0, 1, \infty\}, \eta)) \tag{3.2}$$

in the following way.

Let L be the maximal extension of $\overline{\mathbb{Q}}(t)$ contained in $\overline{\mathbb{Q}}(t)^{\text{cl}}$ that is unramified outside $\{0, 1, \infty\}$. Define

$$\Gamma_{\overline{\mathbb{Q}}} = \text{Gal}(L/\overline{\mathbb{Q}}(t)) = \pi_1(\mathbb{P}_{\mathbb{Q}}^1 - \{0, 1, \infty\}, \eta).$$

Let x and y be topological generators of decomposition groups in $\Gamma_{\overline{\mathbb{Q}}}$ over 0 and 1. These decomposition groups correspond to projective systems $\{P_{i,0}\}_i$ and $\{P_{i,1}\}_i$ of discrete valuations over 0 and 1, respectively, in a countable cofinal system indexed by i of finite extensions of $\overline{\mathbb{Q}}(t)$ in L . The topological fundamental group of $\mathbb{P}^1(\mathbb{C}) - \{0, 1, \infty\}$ is the free group generated by loops around 0 and 1. It follows that the group $\Gamma_{\overline{\mathbb{Q}}}$ is the profinite completion $\widehat{\langle x, y \rangle}$ of the free group generated by x and y .

For $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we lift σ canonically to an element of $\text{Gal}(\overline{\mathbb{Q}}(t)/\mathbb{Q}(t))$ by letting σ fix t . Choose a further lift $\tilde{\sigma}$ of σ to $\text{Aut}(L/\mathbb{Q}(t)) \subset \text{Aut}(L/\mathbb{Q})$. There is a transitive

action of $\Gamma_{\overline{\mathbb{Q}}}$ on the discrete valuations of any finite Galois extension of $\overline{\mathbb{Q}}(t)$ in L that lie over the discrete valuation of $\overline{\mathbb{Q}}(t)$ associated to the point 0. It follows that there is an element $\gamma \in \text{Gal}(L/\overline{\mathbb{Q}}(t))$ such that $\gamma(\{P_{i,0}\}_i) = \tilde{\sigma}(\{P_{i,0}\}_i)$. Then conjugation by $\gamma^{-1}\tilde{\sigma}$ takes the profinite group $\widehat{\langle x \rangle}$ generated by x back to itself.

Define

$$\Gamma_{\mathbb{Q}} = \text{Gal}(L/\mathbb{Q}(t))$$

and let $[\Gamma_{\overline{\mathbb{Q}}}, \Gamma_{\overline{\mathbb{Q}}}]$ be the commutator subgroup of $\Gamma_{\overline{\mathbb{Q}}} \subset \Gamma_{\mathbb{Q}}$. When we set

$$\tilde{\Gamma}_{\mathbb{Q}} = \frac{\Gamma_{\mathbb{Q}}}{[\Gamma_{\overline{\mathbb{Q}}}, \Gamma_{\overline{\mathbb{Q}}}]}$$

we have an exact sequence

$$1 \longrightarrow \Gamma_{\overline{\mathbb{Q}}}^{\text{ab}} \longrightarrow \tilde{\Gamma}_{\mathbb{Q}} \longrightarrow \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow 1 \quad (3.3)$$

where

$$\Gamma_{\overline{\mathbb{Q}}}^{\text{ab}} = \Gamma_{\overline{\mathbb{Q}}} / [\Gamma_{\overline{\mathbb{Q}}}, \Gamma_{\overline{\mathbb{Q}}}] = \widehat{\langle x, y \rangle}^{\text{ab}} \cong \widehat{\langle x \rangle} \times \widehat{\langle y \rangle}$$

and we have identified $\text{Gal}(\overline{\mathbb{Q}}(t)/\mathbb{Q}(t))$ with $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Let $D(y)$ be the subgroup of $\Gamma_{\mathbb{Q}}$ which fixes the projective system $\{P_{i,1}\}_i$ of points lying over 1. Since the residue field of the point 1 on $\mathbb{P}_{\mathbb{Q}}^1$ is $\mathbb{Q}$, we have an exact sequence

$$1 \longrightarrow \widehat{\langle y \rangle} \longrightarrow D(y) \longrightarrow \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow 1.$$

We have an injective homomorphism $\widehat{\langle y \rangle} \longrightarrow \Gamma_{\overline{\mathbb{Q}}}^{\text{ab}}$ induced by the inclusion of $\widehat{\langle y \rangle}$ into $\Gamma_{\overline{\mathbb{Q}}}$. It follows that the homomorphism $D(y) \longrightarrow \tilde{\Gamma}_{\mathbb{Q}}$ induced by $D(y) \subset \Gamma_{\mathbb{Q}}$ is injective; let $\overline{D}(y)$ be the image of this homomorphism. For simplicity we will identify $\widehat{\langle x \rangle}$ and $\widehat{\langle y \rangle}$ with their images in $\Gamma_{\overline{\mathbb{Q}}}^{\text{ab}}$.

We now claim that $\widehat{\langle x \rangle}$ is a set of representatives for the left cosets $z\overline{D}(y)$ of $\overline{D}(y)$ in $\tilde{\Gamma}_{\mathbb{Q}}$. First, these cosets are disjoint, since if $z\overline{D}(y) = z'\overline{D}(y)$ for some $z, z' \in \widehat{\langle x \rangle}$ then $z^{-1}z'$ is in the intersection of $\overline{D}(y)$ with the kernel of $\tilde{\Gamma}_{\mathbb{Q}} \longrightarrow \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. This intersection is

$$\overline{D}(y) \cap \Gamma_{\overline{\mathbb{Q}}}^{\text{ab}} = \widehat{\langle y \rangle} \subset \Gamma_{\overline{\mathbb{Q}}}^{\text{ab}} = \widehat{\langle x \rangle} \times \widehat{\langle y \rangle}.$$

The only element of $\widehat{\langle x \rangle}$ lying in this intersection is the identity element, so $z = z'$. We must now show that every element ψ of $\tilde{\Gamma}_{\mathbb{Q}}$ lies in some coset $z\overline{D}(y)$ with $z \in \widehat{\langle x \rangle}$. To show this, first note that we can find $d \in \overline{D}(y)$ with the same image under $\tilde{\Gamma}_{\mathbb{Q}} \longrightarrow$

$\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ as ψ . Then $\psi d^{-1} \in \Gamma_{\overline{\mathbb{Q}}}^{\text{ab}} = \langle \widehat{x} \rangle \times \langle \widehat{y} \rangle$, so $\psi d^{-1} \in z \langle \widehat{y} \rangle$ for some $z \in \langle \widehat{x} \rangle$. Hence, $\psi \in z \langle \widehat{y} \rangle d \subset z \overline{D}(y)$ and we are done.

We now return to the element $\gamma^{-1}\tilde{\sigma}$ of $\Gamma_{\overline{\mathbb{Q}}}$. The image of this element in $\tilde{\Gamma}_{\overline{\mathbb{Q}}}$ lies in a coset $\nu \overline{D}(y)$ for a unique $\nu \in \langle \widehat{x} \rangle$. Therefore, $\nu^{-1}\gamma^{-1}\tilde{\sigma} \in \Gamma_{\overline{\mathbb{Q}}}$ has the same image in $\tilde{\Gamma}_{\overline{\mathbb{Q}}}$ as an element μ of $D(y)$, and μ is unique since ν was unique and the map $D(y) \rightarrow \overline{D}(y)$ is an isomorphism. Hence, $\nu^{-1}\gamma^{-1}\tilde{\sigma} = \lambda \cdot \mu$ for a unique λ in the commutator subgroup $[\Gamma_{\overline{\mathbb{Q}}}, \Gamma_{\overline{\mathbb{Q}}}]$ of $\Gamma_{\overline{\mathbb{Q}}}$. Since ν was uniquely determined by $\gamma^{-1}\tilde{\sigma}$, both λ and μ are as well. The intersection of $[\Gamma_{\overline{\mathbb{Q}}}, \Gamma_{\overline{\mathbb{Q}}}]$ with $D(y)$ is trivial. It follows that $\sigma' = \nu^{-1}\gamma^{-1}\tilde{\sigma} = \lambda \cdot \mu$ is a lift of σ to $\text{Gal}(L/\mathbb{Q}(t)) = \Gamma_{\overline{\mathbb{Q}}}$ that has these properties:

- i. Conjugation by σ' takes $\langle \widehat{x} \rangle$ to itself, so $\sigma' \cdot x \cdot (\sigma')^{-1} = x^a$ for some $a \in \widehat{\mathbb{Z}}^*$.
- ii. Conjugation by σ' takes $\langle \widehat{y} \rangle$ to a conjugate $\lambda \langle \widehat{y} \rangle \lambda^{-1} = (\lambda \mu) \langle \widehat{y} \rangle (\lambda \mu)^{-1}$ of $\langle \widehat{y} \rangle$ by an element λ of the commutator subgroup $[\Gamma_{\overline{\mathbb{Q}}}, \Gamma_{\overline{\mathbb{Q}}}]$. Thus $\sigma' \cdot y \cdot (\sigma')^{-1} = (\lambda \cdot y \cdot \lambda^{-1})^b$ for some $b \in \widehat{\mathbb{Z}}^*$.

By considering the action of σ' by conjugation on $\Gamma_{\overline{\mathbb{Q}}}^{\text{ab}}$, one sees by Kummer theory that $a = b = \chi_{\text{cyc}}(\sigma)$ where χ_{cyc} is the standard cyclotomic character. Belyĭ shows that $\langle \widehat{x} \rangle$ and $\langle \widehat{y} \rangle$ are their own centralizers in $\Gamma_{\overline{\mathbb{Q}}}$, from which it follows that σ' is uniquely determined by σ . Belyĭ denotes λ by f_{σ} , and the Belyĭ lift

$$\iota : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{Aut}(\Gamma_{\overline{\mathbb{Q}}}) = \text{Aut}(\langle \widehat{x, y} \rangle)$$

is defined by letting $\iota(\sigma)$ be conjugation by σ' .

For later use, we will describe one consequence of this construction. Suppose F is a number field and that $Y \rightarrow \mathbb{P}_{\overline{\mathbb{Q}}}^1$ is an irreducible finite Galois H -cover of smooth projective irreducible curves that is unramified outside $\{0, 1, \infty\}$. Suppose Y and the action of H on Y are defined over F , and that F is algebraically closed in the function field $F(Y)$. We will furthermore require that the points over 0, 1 and ∞ on Y are defined over F . Recall that η corresponds to the choice of an algebraic closure $\overline{\mathbb{Q}}(t)^{\text{cl}}$ of $\overline{\mathbb{Q}}(t)$. We fix an embedding of $F(Y)$ into $\overline{\mathbb{Q}}(t)^{\text{cl}}$.

Lemma 3.1. *We can find a finite extension $F^{\dagger}$ of F so that if $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/F^{\dagger})$ then the element σ' in the Belyĭ construction of $\iota(\sigma)$ lies in $\text{Gal}(L/F^{\dagger}(Y))$.*

Proof. If $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ lies in the finite index subgroup $\text{Gal}(\overline{\mathbb{Q}}/F)$, we can extend σ in a unique way to an element of $\text{Gal}(\overline{\mathbb{Q}}(Y)/F(Y))$. We can thus choose the first lift $\tilde{\sigma} \in \text{Aut}(L/\mathbb{Q})$ in Belyĭ's construction so that $\tilde{\sigma} \in \text{Gal}(L/F(Y))$. Recall that $\{P_{i,0}\}_i$ was a cofinal system of points over 0 in a cofinal system of finite covers of $\mathbb{P}_{\overline{\mathbb{Q}}}^1$ that are unramified outside 0, 1 and ∞ . We can assume that Y is one of the covers in this system, and that all the covers in the system are in fact covers of Y . Let 0_Y be the point of Y lying over 0 which appears in the system $\{P_{i,0}\}_i$. Since $\tilde{\sigma}$ fixes Y and 0_Y , we see that $\{\tilde{\sigma}(P_{i,0})\}_i$ is a system of points over 0 which all lie over 0_Y . It follows that the first element

$\gamma \in \text{Gal}(L/\overline{\mathbb{Q}}(t))$ in Belyi's construction can be chosen to lie in $\text{Gal}(L/\overline{\mathbb{Q}}(Y))$. However, we cannot say that the next element ν in Belyi's construction lies in $\text{Gal}(L/\overline{\mathbb{Q}}(Y))$. We now indicate some further hypotheses that will force this to be the case.

Let s be the exponent of the finite group H , i.e. the smallest positive integer such that every element of H has order dividing s . There is an abelian cover U of $\mathbb{P}_{\overline{\mathbb{Q}}}^1$ that is unramified outside $\{0, 1, \infty\}$ and whose Galois group over $\mathbb{P}_{\overline{\mathbb{Q}}}^1$ is isomorphic to the group $\mathbb{Z}/s \times \mathbb{Z}/s$. Any automorphism in $\text{Gal}(L/\overline{\mathbb{Q}}(U))$ then has image in $\text{Gal}(L/\overline{\mathbb{Q}}(t))^{\text{ab}} = \widehat{\langle x, y \rangle}^{\text{ab}} \cong \widehat{\langle x \rangle} \times \widehat{\langle y \rangle}$ which is an s^{th} power. Let $F^\dagger$ be a finite extension of F with the following properties. The composite of $\overline{\mathbb{Q}}(U)$ and $\overline{\mathbb{Q}}(Y)$ in L is the function field of a smooth projective irreducible curve $Y^\dagger$ that is defined over $F^\dagger$. The action of $H^\dagger = \text{Gal}(\overline{\mathbb{Q}}(Y^\dagger)/\overline{\mathbb{Q}}(t))$ is defined over $F^\dagger$. The points of $Y^\dagger$ over $\{0, 1, \infty\}$ are defined over $F^\dagger$, and $F^\dagger$ is the constant field of $F^\dagger(Y^\dagger)$. Then $Y^\dagger$ is a cover of Y and H is a quotient of $H^\dagger$. Running Belyi's construction now with Y replaced by $Y^\dagger$ and F replaced by $F^\dagger$, we arrive at a lift $\tilde{\sigma} \in \text{Gal}(L/F^\dagger(Y^\dagger))$ and an element $\gamma \in \text{Gal}(L/\overline{\mathbb{Q}}(Y^\dagger))$.

We now recall that ν is the unique element of $\widehat{\langle x \rangle}$ such that the image of $\gamma^{-1}\tilde{\sigma}$ in $\tilde{\Gamma}_{\overline{\mathbb{Q}}} = \Gamma_{\overline{\mathbb{Q}}} / [\Gamma_{\overline{\mathbb{Q}}}, \Gamma_{\overline{\mathbb{Q}}}]$ lies in the image in $\tilde{\Gamma}_{\overline{\mathbb{Q}}}$ of the coset $\nu D(y)$ of the decomposition group $D(y)$ of the inverse system of points $\{P_{i,1}\}_i$ over 1. We can assume that the inverse system of covers used to define $\{P_{i,1}\}_i$ includes U and Y and $Y^\dagger$. Since we have arranged that $\gamma^{-1}\tilde{\sigma}$ fixes $F^\dagger(Y^\dagger)$ and that the points over $\{0, 1, \infty\}$ on $Y^\dagger$ are defined over $F^\dagger$, the action of $\gamma^{-1}\tilde{\sigma}$ fixes the point $P_{U,1}$ of the cover U over 1 in the above inverse system. Now, U is an abelian cover of $\mathbb{P}_{\overline{\mathbb{Q}}}^1$ and $\gamma^{-1}\tilde{\sigma}$ has the same image in $\tilde{\Gamma}_{\overline{\mathbb{Q}}}$ as νz for some z in $D(y)$. Since $D(y)$ fixes the inverse system $\{P_{i,1}\}_i$, we conclude that $\nu \in \widehat{\langle x \rangle}$ must fix $P_{U,1}$ because $\gamma^{-1}\tilde{\sigma}$ does. Therefore, the image of $\nu \in \widehat{\langle x \rangle} \subset \Gamma_{\overline{\mathbb{Q}}}$ in $\text{Gal}(\overline{\mathbb{Q}}(U)/\overline{\mathbb{Q}}(t)) = \mathbb{Z}/s \times \mathbb{Z}/s$ is in the inertia group of a point $P_{U,0}$ over 0 in U as well as in the inertia group of the point $P_{U,1}$. These inertia subgroups of $\text{Gal}(\overline{\mathbb{Q}}(U)/\overline{\mathbb{Q}}(t))$ have trivial intersection, so $\nu \in \widehat{\langle x \rangle}$ has trivial image in $\text{Gal}(\overline{\mathbb{Q}}(U)/\overline{\mathbb{Q}}(t))$. This forces ν to be the s^{th} power of an element of $\widehat{\langle x \rangle}$. Since s was the exponent of H , we conclude that ν has trivial image in $H = \text{Gal}(\overline{\mathbb{Q}}(Y)/\overline{\mathbb{Q}}(t))$. Therefore, $\sigma' = \nu^{-1}\gamma^{-1}\tilde{\sigma}$ lies in $\text{Gal}(L/F^\dagger(Y))$ and we are done. $\square$

4. Galois representations

Let X be a smooth projective irreducible curve defined over $\overline{\mathbb{Q}}$. By Belyi's Theorem [1, Theorem 4], there is a non-constant morphism $\lambda : X \rightarrow \mathbb{P}_{\overline{\mathbb{Q}}}^1$ which is unramified outside $\{0, 1, \infty\}$. Let H be the Galois group of the Galois closure $\tilde{\lambda} : Y \rightarrow \mathbb{P}_{\overline{\mathbb{Q}}}^1$ of λ . We will identify $\widehat{F}_2$ with the étale fundamental group $\pi_1(\mathbb{P}_{\overline{\mathbb{Q}}}^1 - \{0, 1, \infty\}, \eta)$ appearing in (3.2) by the choices described in the previous section. We will also view $G_{\overline{\mathbb{Q}}} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ as a subgroup of $\text{Aut}(\widehat{F}_2)$ via the injection ι of (3.2). Let $\pi : \widehat{F}_2 \rightarrow H$ be the homomorphism associated to $\tilde{\lambda}$ and the choice of a geometric point of Y over η . Fix $d = 2$ and let

$$\rho : A(\pi) \rightarrow \text{Aut}_{H,\beta}(\overline{R})$$

be the surjective homomorphism defined in Theorem 1.3.

We will prove the following result, which implies Theorem 1.2.

Theorem 4.1. *The group $\overline{R}$ is isomorphic to the Galois group of the maximal abelian cover of Y that is unramified outside the ramification locus $\tilde{\lambda}^{-1}(\{0, 1, \infty\})$. This Galois group is isomorphic to the adelic Tate module $T_{\tilde{\lambda}}(Y)$ of the generalized Jacobian $J_{\tilde{\lambda}}(Y)$ of Y with respect to $\tilde{\lambda}^{-1}(\{0, 1, \infty\})$. Let $\mathcal{J} \subset H$ be the Galois group of Y over X . The coinvariants $\overline{R}_{\mathcal{J}}$ of $\overline{R}$ with respect to $\mathcal{J}$ have finite torsion, and the quotient $\overline{R}_{\mathcal{J}}^{\text{cotor}}$ of $\overline{R}_{\mathcal{J}}$ by this torsion subgroup is naturally identified with a subgroup of finite index in the Galois group of the maximal abelian cover of X that is unramified outside the ramification locus $\lambda^{-1}(\{0, 1, \infty\})$. The latter Galois group is $T_{\lambda}(X)$. There is an H -equivariant action of $A(\pi)$ on $T_{\tilde{\lambda}}(Y)$, and there is a finite index subgroup $A_X(\pi)$ of $A(\pi)$ that acts on $T_{\lambda}(X)$.*

There is a finite extension F of $\mathbb{Q}$ over which X , Y , $J_{\lambda}(X)$, $J_{\tilde{\lambda}}(Y)$ and the action of H on Y are defined. There is a natural action of $G_F = \text{Gal}(\overline{\mathbb{Q}}/F)$ on $T_{\tilde{\lambda}}(Y)$ and $T_{\lambda}(X)$. There are finite index normal subgroups A_Y of $A(\pi)$ and A_X of $A_X(\pi)$ such that the action of $G_F \cap \iota^{-1}(A_Y)$ (resp. $G_F \cap \iota^{-1}(A_X)$) on $T_{\tilde{\lambda}}(Y)$ (resp. $T_{\lambda}(X)$) agrees with the action of A_Y (resp. A_X) under Belyi's embedding $G_F \xrightarrow{\iota} \text{Aut}(\widehat{F}_2)$.

Proof. The identification of $\overline{R}$ with $T_{\tilde{\lambda}}(Y)$ is shown by Serre in [19, §I.2]. Let L be the maximal abelian extension of $\overline{\mathbb{Q}}(Y)$ that is Galois over $\overline{\mathbb{Q}}(X)$, unramified outside $\tilde{\lambda}^{-1}(\{0, 1, \infty\})$ and for which $\text{Gal}(L/\overline{\mathbb{Q}}(Y))$ is central in $\text{Gal}(L/\overline{\mathbb{Q}}(X))$. Then L contains the maximal abelian extension L' of $\overline{\mathbb{Q}}(X)$ that is unramified outside $\lambda^{-1}(\{0, 1, \infty\})$. Furthermore, $\text{Gal}(L/\overline{\mathbb{Q}}(Y)) = T_{\tilde{\lambda}}(Y)_{\mathcal{J}}$ and there is a central extension of groups

$$1 \longrightarrow T_{\tilde{\lambda}}(Y)_{\mathcal{J}} \longrightarrow \text{Gal}(L/\overline{\mathbb{Q}}(X)) \longrightarrow \mathcal{J} \longrightarrow 1.$$

Letting these groups act trivially on $\mathbb{Q}/\mathbb{Z}$, the Hochschild-Serre spectral sequence gives an exact sequence of low degree terms

$$\begin{aligned} 0 \longrightarrow H^1(\mathcal{J}, \mathbb{Q}/\mathbb{Z}) &\longrightarrow H^1(\text{Gal}(L/\overline{\mathbb{Q}}(X)), \mathbb{Q}/\mathbb{Z}) \longrightarrow H^1(T_{\tilde{\lambda}}(Y)_{\mathcal{J}}, \mathbb{Q}/\mathbb{Z}) \\ &\longrightarrow H^2(\mathcal{J}, \mathbb{Q}/\mathbb{Z}). \end{aligned}$$

Here $H^i(\mathcal{J}, \mathbb{Q}/\mathbb{Z})$ is finite for $i \geq 1$. The maximal abelian quotient of $\text{Gal}(L/\overline{\mathbb{Q}}(X))$ is $\text{Gal}(L'/\overline{\mathbb{Q}}(X)) = T_{\lambda}(X)$ and

$$H^1(\text{Gal}(L/\overline{\mathbb{Q}}(X)), \mathbb{Q}/\mathbb{Z}) = \text{Hom}(\text{Gal}(L'/\overline{\mathbb{Q}}(X)), \mathbb{Q}/\mathbb{Z}).$$

Moreover,

$$H^1(T_{\tilde{\lambda}}(Y)_{\mathcal{J}}, \mathbb{Q}/\mathbb{Z}) = \text{Hom}(T_{\tilde{\lambda}}(Y)_{\mathcal{J}}, \mathbb{Q}/\mathbb{Z}).$$

Since $T_{\tilde{\lambda}}(Y)_{\mathcal{J}}$ is abelian, we obtain that $T_{\tilde{\lambda}}(Y)_{\mathcal{J}}$ maps with finite kernel and cokernel to $\text{Gal}(L'/\overline{\mathbb{Q}}(X)) = T_{\lambda}(X)$. Because $T_{\lambda}(X)$ is torsion free, we conclude that $T_{\tilde{\lambda}}(Y)_{\mathcal{J}}$

has finite torsion, and the quotient $T_{\tilde{\lambda}}(Y)_{\mathcal{J}}^{\text{cotor}}$ of $T_{\tilde{\lambda}}(Y)_{\mathcal{J}}$ by its torsion subgroup is isomorphic to a subgroup of finite index in $T_{\lambda}(X)$.

We now identify $T_{\tilde{\lambda}}(Y)$ with $\overline{R}$ and apply Theorem 1.3. This shows that there is an H -equivariant action of $A(\pi)$ on $T_{\tilde{\lambda}}(Y)$. In particular, this action descends to an action of $A(\pi)$ on $T_{\tilde{\lambda}}(Y)_{\mathcal{J}}^{\text{cotor}}$. Let m be the index of $T_{\tilde{\lambda}}(Y)_{\mathcal{J}}^{\text{cotor}}$ in $T_{\lambda}(X)$. We have a sequence of inclusions

$$m T_{\tilde{\lambda}}(Y)_{\mathcal{J}}^{\text{cotor}} \subset m T_{\lambda}(X) \subset T_{\tilde{\lambda}}(Y)_{\mathcal{J}}^{\text{cotor}}.$$

Since $A(\pi)$ acts on the finite group $T_{\tilde{\lambda}}(Y)_{\mathcal{J}}^{\text{cotor}}/m T_{\tilde{\lambda}}(Y)_{\mathcal{J}}^{\text{cotor}}$, there exists a finite index subgroup $A_X(\pi)$ of $A(\pi)$ such that $A_X(\pi)$ acts trivially on $T_{\tilde{\lambda}}(Y)_{\mathcal{J}}^{\text{cotor}}/m T_{\tilde{\lambda}}(Y)_{\mathcal{J}}^{\text{cotor}}$. Therefore, $A_X(\pi)$ preserves $m T_{\lambda}(X)$ and hence $A_X(\pi)$ acts on $T_{\lambda}(X)$.

It remains to show that we can shrink $A(\pi)$ and $A_X(\pi)$ to smaller finite index normal subgroups A_Y and A_X , respectively, if necessary, so that the action of $G_F \cap \iota^{-1}(A_Y)$ (resp. $G_F \cap \iota^{-1}(A_X)$) on $T_{\tilde{\lambda}}(Y)$ (resp. $T_{\lambda}(X)$) agrees with the action of A_Y and A_X under Belyi's embedding $\iota : G_F \rightarrow \text{Aut}(\widehat{F}_2)$. We will use the description of ι given in §3.

In the arguments below, we will need to enlarge F to a finite extension $F^{\dagger}$ of F . Since $\iota : G_F \rightarrow \text{Aut}(\widehat{F}_2)$ is a continuous injective homomorphism of profinite groups, it follows from [16, Prop. 2.1.5] that ι is a homeomorphism onto its image when the image is given the topology induced by that of $\text{Aut}(\widehat{F}_2)$. Therefore, there are finite index normal subgroups of $A(\pi)$ and $A_X(\pi)$ with the property that their intersection with $\iota(G_F)$ is contained in $\iota(G_{F^{\dagger}})$. Thus in what follows we are free to enlarge F by a finite extension in order to prove the existence of finite index subgroups A_Y and A_X with the desired properties.

By Lemma 3.1, we can now replace F by a larger finite extension $F^{\dagger}$ to be able to assume that if $\sigma \in G_F$ then $\iota(\sigma)$ is conjugation by an element $\sigma' \in \text{Gal}(L/F(Y))$ which restricts to σ on $\overline{\mathbb{Q}} \subset L$. We have a tower of fields $F(Y) \subset \overline{\mathbb{Q}}(Y) \subset \overline{\mathbb{Q}}(Y)^{\text{ab}} \subset L$ in which $\overline{\mathbb{Q}}(Y)^{\text{ab}}$ is the largest abelian extension of $\overline{\mathbb{Q}}(Y)$ inside L . By [19, §I.2], $\text{Gal}(\overline{\mathbb{Q}}(Y)^{\text{ab}}/\overline{\mathbb{Q}}(Y))$ is naturally isomorphic to the adelic Tate module $T_{\tilde{\lambda}}(Y)$, and the action of σ on $T_{\tilde{\lambda}}(Y)$ corresponds to the conjugation action of any lift $\widehat{\sigma}$ of σ to an element of $\text{Gal}(\overline{\mathbb{Q}}(Y)^{\text{ab}}/F(Y))$. Note that this conjugation action does not depend on the choice of the lift $\widehat{\sigma}$ because $\text{Gal}(\overline{\mathbb{Q}}(Y)^{\text{ab}}/\overline{\mathbb{Q}}(Y))$ is an abelian normal subgroup of $\text{Gal}(\overline{\mathbb{Q}}(Y)^{\text{ab}}/F(Y))$. However, we know that the action of $\iota(\sigma)$ on $\text{Gal}(\overline{\mathbb{Q}}(Y)^{\text{ab}}/\overline{\mathbb{Q}}(Y))$ is via the conjugation action by $\sigma' \in \text{Gal}(L/F(Y))$, so the action of $\iota(\sigma)$ on $\text{Gal}(\overline{\mathbb{Q}}(Y)^{\text{ab}}/\overline{\mathbb{Q}}(Y))$ agrees with the conjugation action of $\widehat{\sigma}$. This shows that the action of $\iota(\sigma)$ on $T_{\tilde{\lambda}}(Y)$ agrees with the natural action of σ . $\square$

Remark 4.2. The statements in Theorem 4.1 hold if one replaces $T_{\tilde{\lambda}}(Y)$ and $T_{\lambda}(X)$ by their maximal pro- ℓ quotients $T_{\ell, \tilde{\lambda}}(Y)$ and $T_{\ell, \lambda}(X)$, the latter being the ℓ -adic Tate modules of the generalized Jacobians of Y and X with respect to $\tilde{\lambda}^{-1}(\{0, 1, \infty\})$ and $\lambda^{-1}(\{0, 1, \infty\})$, respectively.

We obtain the following consequence of Theorem 4.1.

Corollary 4.3. *Assume the notation from Theorem 4.1. Suppose $\tilde{I}$ is a (closed) normal subgroup of $\hat{F}_2$ such that $[R, R] \subset \tilde{I} \subset R$, and let $\tilde{R} = R/\tilde{I}$. Then $\tilde{R}$ is a quotient module of $\bar{R} = T_{\tilde{\lambda}}(Y)$ and there is an H -equivariant action of $A(\pi, \tilde{I}) \subset \text{Aut}(\hat{F}_2)$ on $\tilde{R}$. The kernel of the surjection $\bar{R} \rightarrow \tilde{R}$ has stabilizer $G_{F'}$ in G_F for some extension F' of F in $\bar{\mathbb{Q}}$.*

- i. *There is a finite index normal subgroup $A_{Y, \tilde{I}}$ of $A(\pi, \tilde{I})$ such that the action of $G_{F'} \cap \iota^{-1}(A_{Y, \tilde{I}})$ on $\tilde{R}$ agrees with the action of $A_{Y, \tilde{I}}$ under Belyi's embedding $G_{F'} \xrightarrow{\iota} \text{Aut}(\hat{F}_2)$.*
- ii. *There is a finite extension F'' of F' in $\bar{\mathbb{Q}}$ such that the action of $G_{F''} \cap \iota^{-1}(A(\pi, \tilde{I}))$ agrees with the action of $A(\pi, \tilde{I})$ under Belyi's embedding $G_{F''} \xrightarrow{\iota} \text{Aut}(\hat{F}_2)$.*

Proof. The first statement follows by letting $A_{Y, \tilde{I}}$ be the intersection of $A(\pi, \tilde{I})$ with the subgroup A_Y appearing in the last sentence of the statement of Theorem 4.1. For the second, observe that since $A_{Y, \tilde{I}}$ has finite index in $A(\pi, \tilde{I})$, the kernel of the homomorphism $G_{F'} \cap \iota^{-1}(A(\pi, \tilde{I})) \rightarrow A(\pi, \tilde{I})/A_{Y, \tilde{I}}$ induced by ι has finite index in $G_{F'} \cap \iota^{-1}(A(\pi, \tilde{I}))$. Therefore, this kernel equals $G_{F''} \cap \iota^{-1}(A(\pi, \tilde{I}))$ for some finite extension F'' of F' . $\square$

Example 4.4. Assume the notation from Corollary 4.3. If $\bar{I}$ is a subgroup of $\bar{R}$ that is stabilized by the action of H on $\bar{R}$, then $\bar{I} = \tilde{I}/[R, R]$ for a normal subgroup $\tilde{I}$ of $\hat{F}_2$. Fix a prime number p . If $\bar{I}_p$ is the subgroup of $\bar{R} = \hat{\mathbb{Z}}^{1+|H|}$ generated by all factors isomorphic to $\mathbb{Z}_p$, then $\bar{I}_p = \tilde{I}_p/[R, R]$ for a normal subgroup $\tilde{I}_p$ of $\hat{F}_2$. Moreover, the action of G_F on $\bar{R}$ preserves $\bar{I}_p$.

Suppose now that we take $\tilde{R} = R/\tilde{I}$ to be the quotient of $\bar{R} = \hat{\mathbb{Z}}^{1+|H|}$ by the subgroup generated by all $\bar{I}_p$ for primes p dividing $|H|$. Then $\tilde{I}$ is a normal subgroup of $\hat{F}_2$, and the kernel of $\bar{R} \rightarrow \tilde{R}$ is stable under all of G_F . The action of $A(\pi)$ on $\bar{R}$ is $\hat{\mathbb{Z}}$ -linear, so $A(\pi)$ acts on $\tilde{R}$ and $A(\pi, \tilde{I}) = A(\pi)$. If $\mathcal{L}'_H$ is the set of all primes ℓ not dividing $|H|$, then

$$\tilde{R} = \prod_{\ell \in \mathcal{L}'_H} T_{\ell, \tilde{\lambda}}(Y).$$

The extension class $\beta \in H^2(H, \tilde{R})$ corresponding to (2.2) is zero for this choice of $\tilde{R}$. Therefore, it follows from Theorem 2.1 that the image of the action of $A(\pi, \tilde{I}) = A(\pi)$ on $\tilde{R}$ is $\text{Aut}_H(\tilde{R})$. Define

$$\hat{\mathbb{Z}}' = \frac{\hat{\mathbb{Z}}}{\prod_{p \notin \mathcal{L}'_H} \mathbb{Z}_p} \cong \prod_{\ell \in \mathcal{L}'_H} \mathbb{Z}_\ell.$$

Then $\tilde{R}$ is isomorphic to $\widehat{\mathbb{Z}}'[H] \oplus \widehat{\mathbb{Z}}'$ as an H -module since $|H|$ is a unit in $\widehat{\mathbb{Z}}'$ (see [6, §2]). Note that $\widehat{\mathbb{Z}}'[H] = \widehat{\mathbb{Z}}' \oplus M$ as H -module, where M is the augmentation ideal of $\widehat{\mathbb{Z}}'[H]$. Hence, $\text{Aut}_H(\tilde{R}) \cong \text{GL}_2(\widehat{\mathbb{Z}}') \times \text{Aut}_H(M)$. The right multiplication action of $\widehat{\mathbb{Z}}'[H]$ identifies the endomorphism ring $\text{End}_{\widehat{\mathbb{Z}}'[H]}(M)$ with the quotient ring of the opposite ring $\widehat{\mathbb{Z}}'[H]^{\text{op}}$ of $\widehat{\mathbb{Z}}'[H]$ modulo the ideal generated by the central idempotent $\frac{1}{|H|} \sum_{\sigma \in H} \sigma$. Recall that the inversion $\sigma \mapsto \sigma^{-1}$ on H extends to a ring isomorphism of $\widehat{\mathbb{Z}}'[H]^{\text{op}}$ with $\widehat{\mathbb{Z}}'[H]$. In other words,

$$\text{Aut}_H(\tilde{R}) \cong \text{GL}_2(\widehat{\mathbb{Z}}') \times \text{GL}_1 \left(\frac{\widehat{\mathbb{Z}}'[H]}{\widehat{\mathbb{Z}}'[H] \cdot (\sum_{\sigma \in H} \sigma)} \right)$$

since $|H|$ is a unit in $\widehat{\mathbb{Z}}'$. Corollary 4.3 says that there is a finite index normal subgroup $A_{Y, \tilde{I}}$ of $A(\pi, \tilde{I}) = A(\pi)$ such that the action of $G_F \cap \iota^{-1}(A_{Y, \tilde{I}})$ on $\tilde{R}$ extends to an action of $A_{Y, \tilde{I}}$ under ι .

5. Actions on the Jacobian versus the generalized Jacobian

Theorems 1.2 and 4.1 show that the action of the absolute Galois group $G_{\mathbb{Q}} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the adelic Tate module of the generalized Jacobian can be virtually extended to an action of $\text{Aut}(\widehat{F}_2)$. In this section, we show that, in general, one indeed needs the full structure of the adelic Tate module of the generalized Jacobian and that the action of $G_{\mathbb{Q}}$ on the adelic Tate module of the Jacobian cannot be virtually extended to $\text{Aut}(\widehat{F}_2)$. Moreover, we give a sufficient condition to distinguish between these two possibilities, which is also necessary when we have a Belyĭ cover that is Galois.

We use the notation from §3 and §4. In particular, we identify $\widehat{F}_2$ with the étale fundamental group $\pi_1(\mathbb{P}_{\mathbb{Q}}^1 - \{0, 1, \infty\}, \eta)$, and we view $G_{\mathbb{Q}}$ as a subgroup of $\text{Aut}(\widehat{F}_2)$ via the injection ι of (3.2). As in §4, let $\lambda : X \rightarrow \mathbb{P}_{\mathbb{Q}}^1$ be a Belyĭ cover, i.e. X is a smooth projective curve over $\overline{\mathbb{Q}}$ and λ is a non-constant morphism which is unramified outside $\{0, 1, \infty\}$. Let H be the Galois group of the Galois closure $\tilde{\lambda} : Y \rightarrow \mathbb{P}_{\mathbb{Q}}^1$ of λ . Let $\pi : \widehat{F}_2 \rightarrow H$ be the homomorphism associated to $\tilde{\lambda}$ and the choice of a geometric point of Y over η .

Let $\mathcal{J} \subset H$ be the Galois group of Y over X , let $\mathcal{W}$ be the normalizer of $\mathcal{J}$ in H , and let $Z = Y/\mathcal{W}$. We can factor $\lambda = \kappa \circ \delta$ where $\delta : X \rightarrow Z$ is a Galois cover with Galois group $\mathcal{D} = \mathcal{W}/\mathcal{J}$ and $\kappa : Z \rightarrow \mathbb{P}_{\mathbb{Q}}^1$ is a Belyĭ cover. For each point $j \in \kappa^{-1}(\{0, 1, \infty\})$ let j_X be a point over j in X and let d_{j_X} be a generator for the inertia group of j_X in $\mathcal{D}$.

Consider now the natural surjection $J_{\lambda}(X) \rightarrow J(X)$ from the generalized Jacobian of X with respect to $\lambda^{-1}(\{0, 1, \infty\})$ to the Jacobian of X . Recall that the points of $J_{\lambda}(X)$ over $\overline{\mathbb{Q}}$ are divisors of degree zero on X prime to $\lambda^{-1}(\{0, 1, \infty\})$ modulo divisors of the form $\text{div}(f)$ for rational functions $f \in \overline{\mathbb{Q}}(X)^*$ such that $f(x) = 1$ if $x \in \lambda^{-1}(\{0, 1, \infty\})$. The principal divisor group of X is isomorphic to $\overline{\mathbb{Q}}(X)^*/\overline{\mathbb{Q}}^*$. Consider the homomor-

phism from the group of elements $g \in \overline{\mathbb{Q}}(X)^*$ that have no zeros or poles in $\lambda^{-1}(\{0, 1, \infty\})$ to the product $\prod_{x \in \lambda^{-1}(\{0, 1, \infty\})} \overline{\mathbb{Q}}^*$ which sends g to the element of the product with component $g(x)$ at x . This homomorphism induces an isomorphism between the algebraic group that is the kernel of $J_\lambda(X) \rightarrow J(X)$ and the split torus

$$T := \frac{\prod_{x \in \lambda^{-1}(\{0, 1, \infty\})} \mathbb{G}_m}{\text{diag}(\mathbb{G}_m)}.$$

The exact sequence

$$1 \rightarrow T \rightarrow J_\lambda(X) \rightarrow J(X) \rightarrow 1$$

gives an exact sequence of ℓ -adic Tate modules

$$0 \rightarrow \frac{\prod_{x \in \lambda^{-1}(\{0, 1, \infty\})} \mathbb{Z}_\ell(1)}{\text{diag}(\mathbb{Z}_\ell(1))} \rightarrow T_{\ell, \lambda}(X) \rightarrow T_\ell(X) \rightarrow 0. \quad (5.1)$$

This sequence is exact as a sequence of G_F -modules once F is a number field over which X , $J(X)$, $J_\lambda(X)$ and the action of $\mathcal{D}$ on X are defined.

The set $\lambda^{-1}(\{0, 1, \infty\}) = \delta^{-1}(\kappa^{-1}(\{0, 1, \infty\}))$ is the $\mathcal{D}$ -set formed by the disjoint union of the orbits of the j_X as j ranges over $\kappa^{-1}(\{0, 1, \infty\})$. We find that the tensor product of the left term in the sequence (5.1) with $\mathbb{Q}_\ell$ over $\mathbb{Z}_\ell$ is isomorphic to

$$\frac{\bigoplus_{j \in \kappa^{-1}(\{0, 1, \infty\})} \mathbb{Q}_\ell[\mathcal{D}/\langle d_{j_X} \rangle]}{\mathbb{Q}_\ell} \quad (5.2)$$

as a $\mathbb{Q}_\ell[\mathcal{D}]$ -module, where the denominator here is embedded into the numerator by sending $1 \in \mathbb{Q}_\ell$ to the sum of all the cosets of $\langle d_{j_X} \rangle$ as j ranges over $\kappa^{-1}(\{0, 1, \infty\})$. When we tensor the middle term of (5.1) with $\mathbb{Q}_\ell$ over $\mathbb{Z}_\ell$, we get the $\mathbb{Q}_\ell[\mathcal{D}]$ -module that is the group of $\mathcal{J}$ -coinvariants of $\mathbb{Q}_\ell \oplus \mathbb{Q}_\ell[H]$ by Gaschütz's theorem (see [6, §2]).

Let $A_X(\pi)$ be the finite index subgroup of $A(\pi)$ from the statement of Theorem 4.1, so we have a well-defined action of $A_X(\pi)$ on $T_{\ell, \lambda}(X)$ as in Remark 4.2. Let A_1 be a finite index subgroup of $A_X(\pi)$. We will say that the action of A_1 on $T_{\ell, \lambda}(X)$ descends to an action on the Tate module $T_\ell(X)$ if the action of A_1 respects the terms of the sequence (5.1). We now give a sufficient condition for this to occur which is also necessary when $X = Y$. In the latter case, $A_X(\pi) = A(\pi)$ and $\lambda = \tilde{\lambda}$.

Theorem 5.1. *Let A_1 be a finite index subgroup of $A_X(\pi)$. A sufficient condition for the action of A_1 on $T_{\ell, \lambda}(X)$ to descend to an action on $T_\ell(X)$ is that for every irreducible representation V of $\mathcal{D}$ over $\overline{\mathbb{Q}}$,*

$$n_V := -\dim_{\overline{\mathbb{Q}}}(V^{\mathcal{D}}) + \sum_{j \in \kappa^{-1}(\{0, 1, \infty\})} \dim_{\overline{\mathbb{Q}}}(V^{\langle d_{j_X} \rangle})$$

is equal to either 0 or

$$m_V := \dim_{\overline{\mathbb{Q}}}(V^{\mathcal{D}}) + [H : \mathcal{W}] \cdot \dim_{\overline{\mathbb{Q}}}(V).$$

This condition for V holds if and only if $\overline{\mathbb{Q}}_{\ell} \otimes_{\overline{\mathbb{Q}}} V$ occurs in exactly one of the $\overline{\mathbb{Q}}_{\ell}[\mathcal{D}]$ -modules that result from tensoring either the left or right term of (5.1) with $\overline{\mathbb{Q}}_{\ell}$ over $\mathbb{Z}_{\ell}$. If $X = Y$, then $\mathcal{D} = H = \mathcal{W}$ and the above sufficient condition is also necessary. Furthermore, if $X = Y$, then the condition holds for all V of dimension 1.

Proof. It follows from Theorem 4.1 and Remark 4.2 that $\mathbb{Q}_{\ell} \otimes_{\mathbb{Z}_{\ell}} T_{\ell, \lambda}(X)$ is isomorphic to the coinvariants $(\mathbb{Q}_{\ell} \otimes_{\mathbb{Z}_{\ell}} T_{\ell, \tilde{\lambda}}(Y))_{\mathcal{J}}$. By Gaschütz's theorem (see [6, §2]), $\mathbb{Q}_{\ell} \otimes_{\mathbb{Z}_{\ell}} T_{\ell, \tilde{\lambda}}(Y)$ is isomorphic to $\mathbb{Q}_{\ell} \oplus \mathbb{Q}_{\ell}[H]$ as a $\mathbb{Q}_{\ell}[H]$ -module. Therefore, $\mathbb{Q}_{\ell} \otimes_{\mathbb{Z}_{\ell}} T_{\ell, \lambda}(X)$ is isomorphic to $\mathbb{Q}_{\ell} \oplus \mathbb{Q}_{\ell}[\mathcal{D}]^{[H: \mathcal{W}]}$ as a $\mathbb{Q}_{\ell}[\mathcal{D}]$ -module.

Let V be an arbitrary irreducible representation of $\mathcal{D}$ over $\overline{\mathbb{Q}}$. Then m_V is the multiplicity of V as a direct summand of $\overline{\mathbb{Q}} \oplus \overline{\mathbb{Q}}[\mathcal{D}]^{[H: \mathcal{W}]}$. By Frobenius reciprocity and (5.2), n_V is the multiplicity of $\overline{\mathbb{Q}}_{\ell} \otimes_{\overline{\mathbb{Q}}} V$ as a direct summand of the tensor product of the left term of (5.1) with $\overline{\mathbb{Q}}_{\ell}$ over $\mathbb{Z}_{\ell}$. Therefore, Theorem 5.1 is equivalent to the statement that the action of A_1 respects the sequence (5.1) if

$$n_V \in \{0, m_V\} \quad \text{for every irreducible representation } V \text{ of } \mathcal{D} \text{ over } \overline{\mathbb{Q}}, \quad (5.3)$$

and if $X = Y$ then (5.3) is also necessary for A_1 to respect the sequence (5.1).

Suppose first that the action of A_1 does not respect the sequence (5.1). Since the terms of (5.1) are free $\mathbb{Z}_{\ell}$ -modules, the action of A_1 does not respect the terms of the sequence obtained by tensoring (5.1) with $\overline{\mathbb{Q}}_{\ell}$ over $\mathbb{Z}_{\ell}$. Hence, we obtain a non-zero $\overline{\mathbb{Q}}_{\ell}[\mathcal{D}]$ -module homomorphism from the tensor product with $\overline{\mathbb{Q}}_{\ell}$ over $\mathbb{Z}_{\ell}$ of the left term of (5.1) to $\overline{\mathbb{Q}}_{\ell} \otimes_{\mathbb{Z}_{\ell}} T_{\ell}(X)$. Since the irreducible representations of $\mathcal{D}$ over $\overline{\mathbb{Q}}_{\ell}$ are all defined over $\overline{\mathbb{Q}}$, this means that there exists an irreducible representation V of $\mathcal{D}$ over $\overline{\mathbb{Q}}$ such that $0 < n_V < m_V$, so (5.3) does not hold.

Now suppose that $X = Y$, so that $\mathcal{J}$ is the trivial subgroup of H , and hence $\mathcal{W} = H$ and $\mathcal{D} = H$. We suppose that the action of A_1 respects the terms of the sequence (5.1), and we must show that (5.3) holds. The action of A_1 preserves the terms of the sequence that results from tensoring (5.1) with $\overline{\mathbb{Q}}_{\ell}$ over $\mathbb{Z}_{\ell}$. Since $T_{\ell, \lambda}(X) = T_{\ell, \tilde{\lambda}}(Y)$ is the maximal pro- ℓ quotient of $\overline{R} = T_{\tilde{\lambda}}(Y)$, we can write $T_{\ell, \lambda}(X) = R/\tilde{I}_{\ell}$ for a characteristic subgroup $\tilde{I}_{\ell}$ of R . By Theorem 2.1, it follows that the image of the action of $A_X(\pi) = A(\pi, \tilde{I}_{\ell})$ on $T_{\ell, \lambda}(X) = R/\tilde{I}_{\ell}$ consists of all H -equivariant automorphisms of $T_{\ell, \lambda}(X)$ that preserve a certain extension class. Since this extension class is annihilated by ℓ^a for a sufficiently large integer $a > 0$, it follows that if $f : T_{\ell, \lambda}(X) \rightarrow T_{\ell, \lambda}(X)$ is any $\mathbb{Z}_{\ell}[H]$ -module endomorphism of $T_{\ell, \lambda}(X)$ and $\text{id}_{T_{\ell, \lambda}(X)}$ is the identity automorphism of $T_{\ell, \lambda}(X)$, then $\text{id}_{T_{\ell, \lambda}(X)} + \ell^a f$ is induced by the action of an element of $A_X(\pi)$. The kernel A_2 of the left multiplication action of $A_X(\pi)$ on the finitely many left cosets of A_1 in $A_X(\pi)$ is a finite index normal subgroup of $A_X(\pi)$ contained in A_1 . Let $n = [A_X(\pi) : A_2]$. Then for

all sufficiently large $a > 0$, the binomial theorem shows that there is an endomorphism f_1 of $T_{\ell,\lambda}(X)$ with the following property. The map

$$\frac{1}{\ell^a} \left((\text{id}_{T_{\ell,\lambda}(X)} + \ell^a f)^n - \text{id}_{T_{\ell,\lambda}(X)} \right) = n f + \ell^a f_1$$

is an endomorphism of $T_{\ell,\lambda}(X)$ lying in the $\mathbb{Q}_\ell$ -subalgebra B of $\text{End}_{\mathbb{Q}_\ell[H]}(\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_{\ell,\lambda}(X))$ generated by automorphisms arising from the action of $A_2 \subset A_1$ on $T_{\ell,\lambda}(X)$. Taking the limit as $a \rightarrow \infty$ and using the fact that B is a closed $\mathbb{Q}_\ell$ -subspace of a finite dimensional $\mathbb{Q}_\ell$ -vector space, we see that B is all of $\text{End}_{\mathbb{Q}_\ell[H]}(\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_{\ell,\lambda}(X))$. Therefore, every element of $\text{End}_{\mathbb{Q}_\ell[H]}(\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_{\ell,\lambda}(X))$ preserves the tensor product of the left term of (5.1) with $\mathbb{Q}_\ell$ over $\mathbb{Z}_\ell$. It follows that every element of $\text{End}_{\overline{\mathbb{Q}_\ell}[H]}(\overline{\mathbb{Q}_\ell} \otimes_{\mathbb{Z}_\ell} T_{\ell,\lambda}(X))$ preserves the tensor product of the left term of (5.1) with $\overline{\mathbb{Q}_\ell}$ over $\mathbb{Z}_\ell$. But this implies the statement (5.3) since the irreducible representations of H over $\overline{\mathbb{Q}_\ell}$ are all defined over $\overline{\mathbb{Q}_\ell}$. $\square$

Remark 5.2. Let $\mathcal{D}_1$ be a subgroup of $\mathcal{D}$. Suppose V is an irreducible representation of $\mathcal{D}$ over $\overline{\mathbb{Q}}$ for which the sufficient criterion described in Theorem 5.1 does not hold. Let V_1 be any irreducible representation of $\mathcal{D}_1$ over $\overline{\mathbb{Q}}$ that occurs in the restriction of V to $\mathcal{D}_1$. Then $\overline{\mathbb{Q}_\ell} \otimes_{\overline{\mathbb{Q}}} V_1$ occurs in both of the restrictions to $\mathcal{D}_1$ of the $\overline{\mathbb{Q}_\ell}[\mathcal{D}]$ -modules that result from tensoring either the left or right term of (5.1) with $\overline{\mathbb{Q}_\ell}$ over $\mathbb{Z}_\ell$. This implies that if for some subgroup $\mathcal{D}_1$ of $\mathcal{D}$ the counterpart of the criterion in Theorem 5.1 holds for all irreducible representations of $\mathcal{D}_1$ over $\overline{\mathbb{Q}}$, then this criterion holds for $\mathcal{D}$. This forces the action of every finite index subgroup A_1 of $A_X(\pi)$ to descend to $T_\ell(X)$.

We now give an example in which $X = Y$ and the action of no finite index subgroup A_1 of $A_X(\pi) = A(\pi)$ descends to an action on $T_\ell(X)$.

Example 5.3. Suppose $X = Y$ and that $\mathcal{D} = H$ is the alternating group A_5 of order 60 on the letters $\{a_1, a_2, a_3, a_4, a_5\}$. Recall that d_{0_X} and d_{1_X} are generators of inertia groups of points of $X = Y$ over 0 and 1. It follows that they generate $\mathcal{D} = H$ and that $d_{\infty_X} = (d_{0_X} d_{1_X})^{-1}$. Suppose d_{0_X} is the three-cycle (a_1, a_2, a_3) in $\mathcal{D}$ and d_{1_X} is the five-cycle $(a_1, a_2, a_3, a_4, a_5)$, so that $d_{\infty_X} = (d_{0_X} d_{1_X})^{-1}$ is a five-cycle. Define A_4 to be the alternating group of order 12 on the letters $\{a_1, a_2, a_3, a_4\}$. The induction $\mathbb{Q}[A_5/A_4]$ of the trivial representation of A_4 to A_5 is then isomorphic to the direct sum of one copy of the trivial representation $\mathbb{Q}$ of A_5 with a four-dimensional absolutely irreducible representation V of A_5 . It is easy to check that the invariants $V^{(d_{j_X})}$ are trivial for $j = 1, \infty$. On the other hand, the three-cycle d_{0_X} has eigenvalues $1, 1, \zeta_3$ and ζ_3^2 on V , so $\dim_{\mathbb{Q}}(V^{(d_{0_X})}) = 2$. It follows by Theorem 5.1 that no finite index subgroup A_1 of $A_X(\pi) = A(\pi)$ respects the terms of the sequence (5.1). Therefore, while the Galois action of some finite index subgroup G_F of $G_{\mathbb{Q}}$ on the ℓ -adic Tate module $T_{\ell,\lambda}(X)$ can be extended to an action of $A(\pi)$, the same cannot be said for the ℓ -adic Tate module $T_\ell(X)$.

We next give an example to show that the sufficient condition in Theorem 5.1 is not in general necessary for the action of $A_X(\pi)$ on $T_{\ell,\lambda}(X)$ to descend to an action on $T_\ell(X)$.

Example 5.4. Let E be the elliptic curve with affine equation $y^3 = t(t-1)$, and let $\kappa : E \rightarrow \mathbb{P}_{\mathbb{Q}}^1$ be the Belyĭ cover defined by $(t, y) \mapsto t$ in affine coordinates. Then κ is a Galois cover and $\text{Gal}(E/\mathbb{P}_{\mathbb{Q}}^1) = \mu_3$ is a cyclic group of order 3, corresponding to the action of cube roots of unity on E via the complex multiplication of E . Suppose $p \neq 3$ is a prime and that $\mathcal{J}$ is a cyclic subgroup of the p -torsion $E(\overline{\mathbb{Q}})[p]$ that is not stable under the action of $\text{Gal}(E/\mathbb{P}_{\mathbb{Q}}^1)$. Define $Y = E$ and let $\tilde{\lambda} : Y \rightarrow \mathbb{P}_{\mathbb{Q}}^1$ be the Belyĭ Galois cover that is the composition of multiplication by p with κ . Define X to be the quotient $Y/\mathcal{J}$. Then there is an isogeny $\delta : X \rightarrow E$ such that the multiplication by p map $Y \rightarrow E$ is the composition of the quotient morphism $Y \rightarrow X$ with δ . The composition of δ with κ is a Belyĭ cover $\lambda : X \rightarrow \mathbb{P}_{\mathbb{Q}}^1$. The Galois group $H = \text{Gal}(Y/\mathbb{P}_{\mathbb{Q}}^1)$ is the semi-direct product $E(\overline{\mathbb{Q}})[p] \rtimes \mu_3$, and the normalizer of $\mathcal{J} = \text{Gal}(Y/X)$ in H is $\mathcal{W} = E(\overline{\mathbb{Q}})[p]$. Thus $\mathcal{D} = \mathcal{W}/\mathcal{J} = \text{Gal}(X/E)$ is the cyclic order p group associated to the isogeny δ . Each of the points $0, 1, \infty \in \mathbb{P}_{\mathbb{Q}}^1$ are totally ramified with respect to $\kappa : E \rightarrow \mathbb{P}_{\mathbb{Q}}^1$, and the points over them are split under $\delta : X \rightarrow E$. Thus if V is the trivial one-dimensional representation of $\mathcal{D}$, then

$$n_V = -\dim_{\overline{\mathbb{Q}}}(V^{\mathcal{D}}) + \sum_{j \in \kappa^{-1}(\{0,1,\infty\})} \dim_{\overline{\mathbb{Q}}}(V^{(d_{jX})}) = -1 + 3 = 2$$

and

$$m_V = \dim_{\overline{\mathbb{Q}}}(V^{\mathcal{D}}) + [H : \mathcal{W}] \cdot \dim_{\overline{\mathbb{Q}}}(V) = 1 + 3 = 4.$$

Hence it is not true that n_V is either 0 or m_V , and the condition in Theorem 5.1 does not hold. Let us now check that nevertheless the action of $A_X(\pi)$ descends to $T_\ell(X)$, i.e. that this action preserves the terms of (5.1). For this we use that the p -isogeny $\delta : X \rightarrow E$ is induced by the trace element of the group ring $\mathbb{Z}_\ell[\mathcal{D}]$ and induces a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \frac{\prod_{x \in \lambda^{-1}(\{0,1,\infty\})} \mathbb{Z}_\ell(1)}{\text{diag}(\mathbb{Z}_\ell(1))} & \longrightarrow & T_{\ell,\lambda}(X) & \longrightarrow & T_\ell(X) \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \frac{\prod_{x \in \kappa^{-1}(\{0,1,\infty\})} \mathbb{Z}_\ell(1)}{\text{diag}(\mathbb{Z}_\ell(1))} & \longrightarrow & T_{\ell,\kappa}(E) & \longrightarrow & T_\ell(E) \longrightarrow 0. \end{array} \quad (5.4)$$

Since the actions of $A_X(\pi)$ and $\mathcal{D}$ on $T_{\ell,\lambda}(X)$ commute, the middle vertical arrow in (5.4) is equivariant for the action of $A_X(\pi)$. Suppose that the terms of the top row of (5.4) are not stable under the action of $A_X(\pi)$. Then there exists $\alpha \in A_X(\pi)$ and there exists

$c \in T_{\ell,\lambda}(X)$ with non-zero image in $T_\ell(X)$ such that $\alpha \cdot c$ has trivial image in $T_\ell(X)$. The right vertical arrow in (5.4) is injective, since the elements of $\mathcal{D}$ act by translations on the elliptic curve X and thus they act trivially on the torsion free module $T_\ell(X)$. Therefore, the image c' of c under the middle vertical arrow in (5.4) is an element of $T_{\ell,\kappa}(E)$ with non-zero image in $T_\ell(E)$ such that $\alpha \cdot c'$ has trivial image in $T_\ell(E)$. This means that the terms of the bottom row of (5.4) are not respected by the action of $A_X(\pi)$. However, we can now apply Theorem 5.1 to the cyclic morphism $\kappa : E \rightarrow \mathbb{P}_{\overline{\mathbb{Q}}}^1$ with Galois group μ_3 . Since κ is Galois and all the irreducible characters of μ_3 over $\overline{\mathbb{Q}}$ have dimension 1, the condition in Theorem 5.1 is automatically satisfied. Hence the action of $A_X(\pi)$ respects the terms in the bottom row of (5.4), which is a contradiction. In other words, the action of $A_X(\pi)$ on $T_{\ell,\lambda}(X)$ descends to an action on $T_\ell(X)$.

We end this section by proving Theorem 1.1 of the introduction.

Proof of Theorem 1.1. As in the statement of the theorem, suppose $t > 1$ is an odd integer. Let ζ be a primitive t^{th} root of unity, and let $E = E_\zeta$ be the elliptic curve with affine equation

$$y^2 = x(x-1)(x-\zeta).$$

Let $\lambda : E \rightarrow \mathbb{P}_{\overline{\mathbb{Q}}}^1$ be the Belyĭ cover defined by $(x, y) \mapsto x^t$ in affine coordinates. Then λ factors as $\lambda = \kappa \circ \delta$ where $\delta : E \rightarrow \mathbb{P}_{\overline{\mathbb{Q}}}^1$ is given by $(x, y) \mapsto x$, and $\kappa : \mathbb{P}_{\overline{\mathbb{Q}}}^1 \rightarrow \mathbb{P}_{\overline{\mathbb{Q}}}^1$ is given by $x \mapsto x^t$, both in affine coordinates. Over $\overline{\mathbb{Q}}$, κ is a cyclic cover of order t . Since $\delta : E \rightarrow \mathbb{P}_{\overline{\mathbb{Q}}}^1$ is quadratic, the Galois group H of the Galois closure $\tilde{\lambda} : Y \rightarrow \mathbb{P}_{\overline{\mathbb{Q}}}^1$ of λ is a semi-direct product of a cyclic group $\mathbb{Z}/t$ of order t with a normal elementary abelian 2-group G . The Galois group $\mathcal{J}$ of the natural morphism $z : Y \rightarrow E$ is an index two subgroup of G . We can identify G with the Galois group of the morphism $\delta \circ z : Y \rightarrow \mathbb{P}_{\overline{\mathbb{Q}}}^1$, where $\tilde{\lambda} = \kappa \circ \delta \circ z$. Note that G is contained in the normalizer $\mathcal{W}$ of $\mathcal{J}$ in H . As before, we let $\pi : \widehat{F}_2 \rightarrow H$ be the surjective homomorphism associated to $\tilde{\lambda}$.

We now apply Theorem 4.1 and Remark 4.2 to $X = E$. We obtain a finite index subgroup $A_E(\pi)$ of $A(\pi)$ so that $A_E(\pi)$ acts on the ℓ -adic Tate module $T_{\ell,\lambda}(E)$. Let $F_1 \supset \mathbb{Q}(\zeta)$ be a number field over which $E = E_\zeta$, Y , $J_\lambda(E)$, $J_{\tilde{\lambda}}(Y)$ and the action of H on Y are defined. Then there exists a finite index normal subgroup A_E of $A_E(\pi)$ such that the action of $G_{F_1} \cap \iota^{-1}(A_E)$ on $T_{\ell,\lambda}(E)$ agrees with the action of A_E under Belyĭ's embedding $G_{F_1} \xrightarrow{\iota} \text{Aut}(\widehat{F}_2)$. Since $G_{F_1} \cap \iota^{-1}(A_E)$ is a finite index subgroup of G_{F_1} , there exists a number field F containing F_1 such that $G_F = G_{F_1} \cap \iota^{-1}(A_E)$. In other words, A_E contains the image of G_F under ι .

We next use the criterion of Theorem 5.1 and Remark 5.2 to show that the action of $A_E(\pi)$, and hence the action of A_E , on $T_{\ell,\lambda}(E)$ descends to an action on $T_\ell(E)$. Let $\mathcal{D}_1$ be the order two subgroup $G/\mathcal{J}$ of $\mathcal{D} = \mathcal{W}/\mathcal{J}$. Let V_1 be an irreducible representation of $\mathcal{D}_1$ over $\overline{\mathbb{Q}}$. Then the character of V_1 is either the trivial character or the order two character of $\mathcal{D}_1$. By Remark 5.2, it suffices to show that $\overline{\mathbb{Q}}_\ell \otimes_{\overline{\mathbb{Q}}} V_1$ occurs in at most one

of the restrictions to $\mathcal{D}_1$ of the $\overline{\mathbb{Q}}_\ell[\mathcal{D}]$ -modules that result from tensoring either the left or right term of (5.1) with $\overline{\mathbb{Q}}_\ell$ over $\mathbb{Z}_\ell$. Here the action of $\mathcal{D}_1$ on these terms results from the elliptic involution associated to $\delta : E \rightarrow \mathbb{P}_{\overline{\mathbb{Q}}}^1$. This involution acts trivially on each of the points in $\lambda^{-1}(\{0, 1, \infty\}) \subset E$, so it acts trivially on the left term of (5.1). On the other hand, the elliptic involution $(x, y) \mapsto (x, -y)$ on E acts as multiplication by -1 on $T_\ell(E)$. Therefore, each V_1 can occur in only one of the above restrictions, which implies that $A_E(\pi)$ acts on $T_\ell(E)$.

Finally, suppose that the value $\phi(t)$ of Euler's phi function on t is larger than 24. Let $\tau_\ell : A_E \rightarrow \mathrm{GL}(\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(E))$ be the representation of A_E over $\mathbb{Q}_\ell$ that is associated to the action of A_E on $T_\ell(E)$. It remains to check that the restriction of τ_ℓ to any subgroup between A_E and $\iota(G_F)$ is absolutely irreducible and non-abelian. For this it will suffice to show these properties for the representation of G_F over $\mathbb{Q}_\ell$ that is associated to the action of G_F on $T_\ell(E)$. By a result of Serre (see [18, Chapter IV]), this will be true as long as E does not have complex multiplication. Using the formula for the j -invariant of $E = E_\zeta$ in [21, Prop. III.1.7], we see that

$$j(E) = 256 \frac{(\zeta^2 - \zeta + 1)^3}{\zeta^2(\zeta - 1)^2}.$$

In particular, $j(E)$ lies in $\mathbb{Q}(\zeta) \subset F$. If E has complex multiplication then $j(E)$ lies in the Hilbert class field of an imaginary quadratic field, which is a dihedral extension of $\mathbb{Q}$. However, the maximal abelian quotient of such a dihedral group has order 4. Therefore, we only need to ensure that $j(E)$ generates an extension of $\mathbb{Q}$ of degree larger than 4. However, this is the case provided the minimal polynomial of ζ has degree greater than 24, which happens if and only if $\phi(t) > 24$. This completes the proof of Theorem 1.1. $\square$

6. The case of elliptic curves that are Galois covers of $\mathbb{P}_{\overline{\mathbb{Q}}}^1 - \{0, 1, \infty\}$

Suppose X is a Galois H -cover of $\mathbb{P}_{\overline{\mathbb{Q}}}^1$ that is unramified outside $\{0, 1, \infty\}$ and associated to a surjection $\pi : \widehat{F}_2 \rightarrow H$. Theorem 5.1 shows that the action of a finite index subgroup of $G_{\overline{\mathbb{Q}}}$ on the adelic Tate module of the Jacobian of X cannot, in general, be extended to an action of the finite index subgroup $A(\pi)$ of $\mathrm{Aut}(\widehat{F}_2)$. In this section, we will show that such an extension does always exist when X has genus 1, and that all such X must be CM elliptic curves. We will also show that when $\iota : G_{\overline{\mathbb{Q}}} \rightarrow \mathrm{Aut}(\widehat{F}_2)$ is the Belyi embedding, the action of $\iota(G_{\overline{\mathbb{Q}}}) \cap A(\pi)$ on the adelic Tate module of the generalized Jacobian of X has infinite index in the group of automorphisms generated by $A(\pi)$, while the corresponding index is finite if we replace the generalized Jacobian by the Jacobian of X .

Throughout this section we will make the following hypothesis:

Hypothesis 6.1. The morphism $\lambda : X \rightarrow \mathbb{P}_{\overline{\mathbb{Q}}}^1$ is an H -cover unramified outside $\{0, 1, \infty\}$, associated to a surjection $\pi : \widehat{F}_2 \rightarrow H$ and an embedding of $\overline{\mathbb{Q}}(X)$ into an algebraic

closure of $\overline{\mathbb{Q}}(t) = \overline{\mathbb{Q}}(\mathbb{P}_{\overline{\mathbb{Q}}}^1)$. The genus of X is 1. There are points 0_X , 1_X and ∞_X of X over 0, 1 and ∞ on $\mathbb{P}_{\overline{\mathbb{Q}}}^1$ such that the corresponding inertia groups I_{0_X} , I_{1_X} and I_{∞_X} satisfy $|I_{0_X}| \geq |I_{1_X}| \geq |I_{\infty_X}|$.

Note that we can always arrange for the last property to hold by composing λ with an automorphism of $\mathbb{P}_{\overline{\mathbb{Q}}}^1$ which permutes $\{0, 1, \infty\}$. In the notation of the previous two sections, we are assuming that $X = Y$ is its own Galois closure over $\mathbb{P}_{\overline{\mathbb{Q}}}^1$ and that $\lambda = \tilde{\lambda}$, which implies that $A_X(\pi) = A(\pi)$.

Here are some examples which are easily checked using Hurwitz's theorem (see [9, §IV.2]).

Example 6.2. Let $d \in \{3, 6, 4\}$. Suppose (a, b, d) is a triple of integers in the set

$$\{(1, 1, 3), (2, 2, 3), (1, 2, 6), (5, 4, 6), (1, 1, 4), (3, 3, 4)\}.$$

Let X be the curve with affine equation $y^d = t^a(t-1)^b$ and let $\lambda_{a,b,d} : X \rightarrow \mathbb{P}_{\overline{\mathbb{Q}}}^1$ be the map sending (y, t) to t . Fix a root of unity ζ_d of order d in $\overline{\mathbb{Q}}$. Then Hypothesis (6.1) holds with $\lambda = \lambda_{a,b,d}$ and the generator 1 of $H_{a,b,d} = \mathbb{Z}/d$ sending y to $\zeta_d y$. Note that the isomorphism class of X as an $H_{a,b,d}$ -cover of $\mathbb{P}_{\overline{\mathbb{Q}}}^1$ depends on the choice of ζ_d . There is a unique point 0_X over 0 on X , and $I_{0_X} = H_{a,b,d}$. The ordered pair $(|I_{1_X}|, |I_{\infty_X}|)$ equals $(3, 3)$ if $d = 3$, $(3, 2)$ if $d = 6$ and $(4, 2)$ if $d = 4$. The elliptic curve X with origin 0_X is isomorphic to an elliptic curve over $\overline{\mathbb{Q}}$ with complex multiplication by the ring of integers $\mathbb{Z}[\zeta_d]$ of $\mathbb{Q}(\zeta_d)$, and all such elliptic curves are isomorphic.

Proposition 6.3. Let X be as in Hypothesis 6.1, so that X is an elliptic curve with origin 0_X . Then λ can be factored as a finite étale isogeny $\lambda_1 : X \rightarrow X$ followed by one of the morphisms $\lambda_{a,b,d} : X \rightarrow \mathbb{P}_{\overline{\mathbb{Q}}}^1$ defined in Example 6.2. The group H is the semi-direct product of $H_{a,b,d} = \mathbb{Z}/d$ with the kernel $\mathcal{J}$ of λ_1 . We can identify $\mathcal{J}$ with an $H_{a,b,d}$ -stable submodule of the torsion points of X as an elliptic curve. Conversely, any such finite $H_{a,b,d}$ -stable subgroup of torsion points can be taken to be the kernel of a λ_1 of the above kind, leading to a cover $\lambda : X \rightarrow \mathbb{P}_{\overline{\mathbb{Q}}}^1$ as in Hypothesis 6.1. The action of $H_{a,b,d}$ on torsion points agrees with the action of $\langle \zeta_d \rangle$ when we identify the Kummer action of the generator 1 of $H_{a,b,d}$ with complex multiplication by ζ_d .

Proof. By Hurwitz's Theorem,

$$0 = 2g(X) - 2 = |H| \cdot (-2) + \sum_{j=0,1,\infty} [H : I_{j_X}] \cdot (|I_{j_X}| - 1).$$

It follows that

$$1 = \sum_{j=0,1,\infty} 1/|I_{j_X}|. \quad (6.1)$$

This forces $|I_{j_X}| \geq 3$ for some j , so $d = |I_{0_X}| \geq 3$ since I_{0_X} has the largest order of any inertia group. Fix an identification of I_{0_X} with $\mathbb{Z}/d$. The generator 1 of I_{0_X} then acts on X via complex multiplication by a root of unity ζ_d of order d . This forces $d \in \{3, 6, 4\}$. Now (6.1) together with the inequalities $d = |I_{0_X}| \geq |I_{1_X}| \geq |I_{\infty_X}|$ force $(|I_{1_X}|, |I_{\infty_X}|)$ to be $(3, 3)$ if $d = 3$, $(3, 2)$ if $d = 6$, and $(4, 2)$ if $d = 4$. If $d = 6$ or $d = 4$, the group I'_{0_X} of automorphisms of X fixing 0_X is equal to I_{0_X} . If $d = 3$, I'_{0_X} is cyclic of order 6 and generated by I_{0_X} together with the multiplication by -1 map $z : X \rightarrow X$.

Let $\mathcal{T}$ be the group of elements of H which are translations $X \rightarrow X$ relative to the group law of X . Suppose h is an arbitrary element of H . Then $h(0_X) = t(0_X)$ for some translation $t : X \rightarrow X$, where we do not claim at this point that $t \in \mathcal{T}$. Moreover, $t^{-1} \circ h = \iota : X \rightarrow X$ is an automorphism of X which fixes 0_X . So ι is a unit in the endomorphism ring of X as an elliptic curve. If $d = 6$ or 4 , all such units are produced by powers of a generator of I_{0_X} , so it follows that $\iota \in I_{0_X}$ and $t \in \mathcal{T}$. Thus in this case, H is the semi-direct product of I_{0_X} with the normal subgroup $\mathcal{T}$ of H .

Suppose now that $d = 3$. Then $\iota \in I_{0_X}$ or $z^{-1} \circ \iota \in I_{0_X}$. We find that in this case, $h = t \circ \iota = \tilde{t} \circ \tilde{\iota}$ where either $t = \tilde{t} \in \mathcal{T}$ and $\iota = \tilde{\iota} \in I_{0_X}$, or $\tilde{t} = t \circ z$ and $\tilde{\iota} = z^{-1} \circ \iota \in I_{0_X}$. Suppose the alternative $\tilde{t} = t \circ z$ occurs. Then $\tilde{t} = t \circ z = h \circ \tilde{\iota}^{-1}$ lies in H . In this case there would be a point $\tau \in X$ such that $\tilde{t}(P) = -P + \tau$ for all $P \in X$. Hence, $\tilde{t}(\tau') = \tau'$ for all points $\tau' \in X$ satisfying $\tau' + \tau' = \tau$ with respect to the group law on X . Since $\tilde{t}^2$ is the identity, we would then have some points of X with inertia groups of even order, which we have shown does not occur when $d = 3$. So in fact, $h = t \circ \iota$ with $t \in \mathcal{T}$ and $\iota \in I_{0_X}$. This implies H is the semi-direct product of I_{0_X} with $\mathcal{T}$ in all cases.

Recall that the action of the generator 1 of $I_{0_X} = \mathbb{Z}/d$ on X defines the complex multiplication of X corresponding to ζ_d . Since $\mathcal{T}$ is stable under the conjugation action of I_{0_X} , $\mathcal{T}$ is the group of translations associated to a subgroup $\mathcal{J}(\mathcal{T})$ of torsion points on X which is stable under the action of $\mathbb{Z}[\zeta_d]$. We have a $\mathcal{T}$ -Galois isogeny $\lambda_1 : X \rightarrow X' = X/\mathcal{T} = X/\mathcal{J}(\mathcal{T})$, and X' is an elliptic curve over $\overline{\mathbb{Q}}$ with complex multiplication by $\mathbb{Z}[\zeta_d]$. Therefore X' is isomorphic to X . The morphism $\lambda_2 : X' = X/\mathcal{T} \rightarrow \mathbb{P}_{\overline{\mathbb{Q}}}^1$ induced by $\lambda : X \rightarrow \mathbb{P}_{\overline{\mathbb{Q}}}^1$ defines an $H/\mathcal{T}$ Galois cover of $\mathbb{P}_{\overline{\mathbb{Q}}}^1$ which is unramified outside $\{0, 1, \infty\}$. Furthermore the order of the inertia group of $H/\mathcal{T}$ at a point of X' over $j \in \{0, 1, \infty\}$ must be the same as the order of I_{j_X} since $\lambda_1 : X \rightarrow X'$ is étale. Since X' is isomorphic to X and $H/\mathcal{T}$ is isomorphic to I_{0_X} , Kummer theory shows that $\lambda_2 : X' \rightarrow \mathbb{P}_{\overline{\mathbb{Q}}}^1$ must be $H/\mathcal{T}$ -isomorphic to a unique $\mathbb{Z}/d$ -cover $\lambda_{a,b,d} : X \rightarrow \mathbb{P}_{\overline{\mathbb{Q}}}^1$ appearing in Example 6.2 when we identify $H/\mathcal{T}$ with I_{0_X} and I_{0_X} with $\mathbb{Z}/d$. The H -cover $X \rightarrow \mathbb{P}_{\overline{\mathbb{Q}}}^1$ we started with then results from the isogeny $X \rightarrow X' = X/\mathcal{T}$ followed by $\lambda_{a,b,d}$. $\square$

Theorem 6.4. *With the notation of Proposition 6.3, the action of $A(\pi)$ on the Tate module $T_{\lambda}(X)$ of the generalized Jacobian descends to an action of $A(\pi)$ on $T(X)$ which respects the action of $\mathbb{Z}[\zeta_d]$. Let F be a number field such that $\iota(G_{\mathbb{Q}}) \cap A(\pi) = \iota(G_F)$. The action of $\iota(G_{\mathbb{Q}}) \cap A(\pi)$ on $T_{\lambda}(X)$ defines an infinite index subgroup of the group of automorphisms of $T_{\lambda}(X)$ induced by $A(\pi)$. The action of $\iota(G_{\mathbb{Q}}) \cap A(\pi)$ on $T(X)$ defines a finite index subgroup of the group of automorphisms of $T(X)$ induced by $A(\pi)$.*

Proof. By Proposition 6.3, X is an elliptic curve with complex multiplication by $\mathbb{Z}[\zeta_d]$ for an integer $d \in \{3, 4, 6\}$. The group H is the semi-direct product of a group $\mathcal{T}$ of translations on X with a cyclic group I of order d , with a generator of I acting by complex multiplication by ζ_d . The action of $\mathcal{T}$ on the adelic Tate module $T(X)$ is trivial. So the action of H on $T(X)$ factors through $H/\mathcal{T} = I$ and corresponds to the action of complex multiplication. Therefore, in the sequence (5.1) the action of H on $\overline{\mathbb{Q}_\ell} \otimes_{\mathbb{Z}_\ell} T_\ell(X)$ gives two (non-trivial) one dimensional characters. Hence, by Theorem 5.1, the action of $A(\pi)$ on $T_\lambda(X)$ descends to an action on $T(X)$.

Therefore, we have an action of $A(\pi)$ on the submodule

$$\frac{\prod_{x \in \lambda^{-1}(\{0, 1, \infty\})} \mathbb{Z}_\ell(1)}{\text{diag}(\mathbb{Z}_\ell(1))}$$

of $T_{\ell, \lambda}(X)$ appearing in the sequence (5.1). This submodule contains the rank one $\mathbb{Z}_\ell$ -modules M_j with trivial action by H that are the images of $\mathbb{Z}_\ell(1)$ diagonally embedded in

$$\prod_{x \in \lambda^{-1}(j)} \mathbb{Z}_\ell(1)$$

for $j \in \{0, 1, \infty\}$. In particular, $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} M_0$ and $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} M_1$ define two distinct one-dimensional $\mathbb{Q}_\ell[H]$ -submodules of $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_{\ell, \lambda}(X)$ with trivial H -action. Since $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_{\ell, \lambda}(X) \cong \mathbb{Q}_\ell \oplus \mathbb{Q}_\ell[H]$, there exists a nilpotent $\mathbb{Q}_\ell[H]$ -module endomorphism f of $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_{\ell, \lambda}(X)$ that sends $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} M_0$ isomorphically to $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} M_1$ and that sends all other irreducible $\mathbb{Q}_\ell[H]$ -module summands of $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_{\ell, \lambda}(X)$ to zero. Multiplying f with a sufficiently large positive integer, say m_1 , we obtain that $m_1 \cdot f$ is a nilpotent $\mathbb{Z}_\ell[H]$ -module endomorphism of $T_{\ell, \lambda}(X)$ that sends M_0 to a non-zero submodule of M_1 . If m_2 is the largest power of ℓ dividing $|H|$, it then follows that $m_1 m_2 \cdot f$ is a nilpotent $\mathbb{Z}_\ell[H]$ -module endomorphism of $T_{\ell, \lambda}(X)$ that sends M_0 to a non-zero submodule of M_1 and that sends any extension class in $H^2(H, T_{\ell, \lambda}(X))$ to zero. Since $T_{\ell, \lambda}(X)$ is the maximal pro- ℓ quotient of $\overline{R} = T_\lambda(X)$, we can write $T_{\ell, \lambda}(X) = R/\tilde{I}_\ell$ for a characteristic subgroup $\tilde{I}_\ell$ of R . It follows from Theorem 2.1 that $\text{id}_{T_{\ell, \lambda}(X)} + m_1 m_2 \cdot f$ is an automorphism of $T_{\ell, \lambda}(X)$ that is induced by an element of $A(\pi) = A(\pi, \tilde{I}_\ell)$. Moreover, $\text{id}_{T_{\ell, \lambda}(X)} + m_1 m_2 \cdot f$ generates a subgroup of this automorphism group that is isomorphic to $\mathbb{Z}$ and every non-trivial element of this subgroup sends M_0 to a non-zero submodule of M_1 .

Since $A(\pi)$ is a finite index subgroup of $\text{Aut}(\widehat{F}_2)$, it follows that there exists a number field F such that $\iota(G_{\mathbb{Q}}) \cap A(\pi) = \iota(G_F)$. Since G_F cannot send points over 0 to points over 1 or ∞ , the action of $G_F = G_{\mathbb{Q}} \cap \iota^{-1}(A(\pi))$ on $T_{\ell, \lambda}(X)$ preserves M_0 and M_1 . By the above construction of $\text{id}_{T_{\ell, \lambda}(X)} + m_1 m_2 \cdot f$, this implies that the action of $\iota(G_{\mathbb{Q}}) \cap A(\pi)$ on $T_\lambda(X)$ defines an infinite index subgroup of the group of automorphisms of $T_\lambda(X)$ induced by $A(\pi)$.

We now compare the actions of G_F and $A(\pi)$ on $T(X)$. The action of $\mathbb{Z}[\zeta_d]$ on X by complex multiplication makes $T(X)$ a rank one free module for $\widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_d] = \widehat{\mathbb{Z}}[\zeta_d]$.

The action of $A(\pi)$ on $T(X)$ respects the action of H , and the action of H corresponds to the action of complex multiplication. On picking a basis for $T(X)$ as a rank one free module for $\widehat{\mathbb{Z}}[\zeta_d]$, we see that the action of $A(\pi)$ on $T(X)$ is defined by a homomorphism $\chi_A : A(\pi) \rightarrow \widehat{\mathbb{Z}}[\zeta_d]^*$. Similarly, the action of G_F on $T(X)$ is defined by a homomorphism $\chi_F : G_F \rightarrow \widehat{\mathbb{Z}}[\zeta_d]^*$. When $\iota : G_{\mathbb{Q}} \rightarrow \text{Aut}(\widehat{F}_2)$ is the Belyĭ embedding, we know by Corollary 4.3 that, after enlarging F by a finite extension, we have $\chi_F = \chi_A \circ \iota|_{G_F}$. Hence, the image of χ_F is contained in the image of χ_A . On the other hand, the main theorem of complex multiplication (see [20, Thm. 5.4]) shows that the image of χ_F has finite index in $\widehat{\mathbb{Z}}[\zeta_d]^*$. Therefore, the image of χ_F has finite index in the image of χ_A and the proof is complete. $\square$

References

- [1] G.V. Belyĭ, Galois extensions of a maximal cyclotomic field, *Izv. Akad. Nauk SSSR, Ser. Mat.* 43 (2) (1979) 267–276, English translation in *Math. USSR, Izv.* 14 (1980) 247–256.
- [2] G.V. Belyĭ, On extensions of the maximal cyclotomic field having a given classical Galois group, *J. Reine Angew. Math.* 341 (1983) 147–156.
- [3] V.G. Drinfel’d, On quasitriangular quasi-Hopf algebras and on a group that is closely connected with $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, *Algebra Anal.* 2 (4) (1990) 149–181.
- [4] M.D. Fried, M. Jarden, *Field Arithmetic*, second edition, *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge (A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics])*, vol. 11, Springer-Verlag, Berlin, 2005.
- [5] W. Gaschütz, Zu einem von B. H. und H. Neumann gestellten Problem, *Math. Nachr.* 14 (1956–1955) 249–252.
- [6] K.W. Gruenberg, *Relation Modules of Finite Groups*, *Conference Board of the Mathematical Sciences Regional Conference Series in Mathematics*, vol. 25, American Mathematical Society, Providence, RI, 1976.
- [7] F. Grunewald, A. Lubotzky, Linear representations of the automorphism group of a free group, *Geom. Funct. Anal.* 18 (5) (2009) 1564–1608.
- [8] D. Harbater, L. Schneps, Approximating Galois orbits of dessins, in: *Geometric Galois Actions, 1*, in: *London Math. Soc. Lecture Note Ser.*, vol. 242, Cambridge Univ. Press, Cambridge, 1997, pp. 205–230.
- [9] R. Hartshorne, *Algebraic Geometry*, *Graduate Texts in Mathematics*, vol. 52, Springer-Verlag, New York-Heidelberg, 1977.
- [10] H. Hida, *Modular Forms and Galois Cohomology*, *Cambridge Studies in Advanced Mathematics*, vol. 69, Cambridge University Press, Cambridge, 2000.
- [11] M. Kaluba, D. Kielak, P.W. Nowak, On property (T) for $\text{Aut}(F_n)$ and $\text{SL}_n(\mathbb{Z})$, *Ann. Math.* (2) 193 (2) (2021) 539–562.
- [12] M. Kaluba, P.W. Nowak, N. Ozawa, $\text{Aut}(\mathbb{F}_5)$ has property (T), *Math. Ann.* 375 (3–4) (2019) 1169–1191.
- [13] P. Lochak, L. Schneps, Open problems in Grothendieck-Teichmüller theory, in: *Problems on Mapping Class Groups and Related Topics*, in: *Proc. Sympos. Pure Math.*, vol. 74, Amer. Math. Soc., Providence, RI, 2006, pp. 165–186.
- [14] A. Lubotzky, Pro-finite presentations, *J. Algebra* 242 (2) (2001) 672–690.
- [15] M. Nitsche, Computer proofs for Property (T), and SDP duality, Preprint, arXiv:2009.05134, 2020.
- [16] L. Ribes, P. Zalesskii, *Profinite Groups*, second edition, *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge (A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics])*, vol. 40, Springer-Verlag, Berlin, 2010.
- [17] L. Schneps, The Grothendieck-Teichmüller group $\widehat{\text{GT}}$: a survey, in: *Geometric Galois Actions, 1*, in: *London Math. Soc. Lecture Note Ser.*, vol. 242, Cambridge Univ. Press, Cambridge, 1997, pp. 183–203.

- [18] J.-P. Serre, *Abelian l -Adic Representations and Elliptic Curves*. McGill University Lecture Notes Written with the Collaboration of Willem Kuyk and John Labute, W.A. Benjamin, Inc., New York-Amsterdam, 1968.
- [19] J.-P. Serre, *Algebraic Groups and Class Fields*, Graduate Texts in Mathematics, vol. 117, Springer-Verlag, New York, 1988, Translated from the French.
- [20] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kano Memorial Lectures, 1.
- [21] J.H. Silverman, *The Arithmetic of Elliptic Curves*, second edition, Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.