Explicit computation of a Galois representation attached to an eigenform over SL_3 from the $\mathrm{H}^2_{\text{ét}}$ of a surface

Nicolas Mascot*

AUB, Beirut, Lebanon

June 10, 2019

Abstract

We sketch a method to compute mod ℓ Galois representations contained in the $\mathrm{H}^2_{\text{ét}}$ of surfaces. We apply this method to the case of a representation with values in $\mathrm{GL}_3(\mathbb{F}_9)$ attached to an eigenform over a congruence subgroup of SL_3. We obtain in particular a polynomial with Galois group isomorphic to the simple group $\mathrm{PSU}_3(\mathbb{F}_9)$ and ramified at 2 and 3 only.

Acknowledgements

The author thanks Jean-Marc Couveignes for his suggestion to apply the *dévissage* principle to the case of the $\mathrm{H}^2_{\text{ét}}$ of surfaces, and in particular on the example presented in this article; François Brunault for his help with the details of the proof of theorem 2.3; Bert van Geemen for pointing out the possibility to read the monodromy around the bad fibres of an elliptic surface off their Kodaira types; and the anonymous referee for providing the explanation why the representation has unitary image.

The computer algebra packages used for the computations presented in this article were [Pari/GP] and [Magma]. The computations were carried out on the Warwick mathematics institute computer cluster provided by the EPSRC Programme Grant EP/K034383/1 "LMF: L-Functions and Modular Forms".

Keywords: Galois representation, algorithm, étale cohomology, dévissage, surface, automorphic form, GL_3, unitary group.

2010 *Mathematics subject classification:* 11Y40, 11F80, 14F20, 11F55, 11Y70, 14Q10, 14Q05.

*nm116@aub.edu.lb

1 Introduction

Several techniques (such as [CE11], [Mas18b], and [Mas18c]) have recently been developed to compute explicitly mod ℓ Galois representations afforded in the torsion of Jacobians of curves. However, many "interesting" representations (e.g. in view of the Langlands program) are not naturally found in Jacobians, but rather in higher étale cohomology spaces of higher-dimensional varieties. They are thus inaccessible to the aforementioned methods, and, to the author's knowledge, computational methods to deal with these representations have not yet been developed apart from the case of modular forms over GL_2.

The purpose of this article is to sketch such a method, thus answering the conjecture made in the second-to-last point of the epilogue of [CE11]. Although our method is still at an experimental stage, it is already sufficiently advanced for us to be able to prove our concept by giving a concrete example of application, which we also present in this article.

Remark 1.1. Very general algorithms to compute with étale cohomology are presented in [MO15] and [PTvL15] (cf. also [Jin17] for a more explicit approach in the case of curves); however, as far as we know these algorithms are not really practical and have never been implemented. Our purpose is to present a method which is completely explicit and really practical on a moderately simple case, and ought to be generalizable to other similar cases.

The concrete example that we have chosen comes from [GT94], where B. van Geemen and J. Top give evidence towards a conjecture of L. Clozel's . They exhibit a Hecke eigenform u over a congruence subgroup of $\mathrm{SL}_3(\mathbb{Z})$ of level $128 = 2^7$ whose Hecke eigenvalues lie in $\mathbb{Z}[2\sqrt{-1}]$, and an algebraic surface S over $\mathbb{Q}$ equipped with an automorphism ϕ_S of order 4 defined over $\mathbb{Q}$, such that for all primes $\ell \in \mathbb{N}$, the ℓ-adic H^2 of S (equipped with the $\mathbb{Q}_\ell(\sqrt{-1})$-vector space structure induced by ϕ_S) contains a Galois-submodule affording the quadratic twist by -2 of the ℓ-adic representation

$$\widetilde{\rho}_{u,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_3\left(\mathbb{Q}_\ell(\sqrt{-1})\right)$$

attached to u.

Remark 1.2. At the time when [GT94] was published, representations attached to this kind of modular forms were not even known to exist, especially when, like $\widetilde{\rho}_{u,\ell}$, they are not self-dual. The existence of these representations was established recently independently by [HLTT16] and [Sch15], and the fact that $\widetilde{\rho}_{u,\ell}$ is indeed afforded by the ℓ-adic H^2 of S is proved in [IKM18].

According to [GT94, 2.4] and to the first paragraph of section 4 of [IKM18], the ℓ-adic representation $\widetilde{\rho}_{u,\ell}$ is unramified away from[1] 2 and ℓ, and for each unramified prime $p \in \mathbb{N}$, the characteristic polynomial of $\widetilde{\rho}_{u,\ell}(\mathrm{Frob}_p)$ is

$$\chi_p(x) = x^3 - a_p x^2 + p\overline{a_p} x - p^3 \in \mathbb{Q}_\ell(\sqrt{-1})[x], \tag{1.3}$$

where $a_p \in \mathbb{Z}[2\sqrt{-1}]$ is the corresponding Hecke eigenvalue of u, and $\overline{a_p}$ is the image of a_p under complex conjugation. In particular, the determinant of this representation is the cube of the ℓ-adic cyclotomic character, and the value of a_p can be recovered as the trace of the Frobenius.

Remark 1.4. Since a_p lies in $\mathbb{Z}[2\sqrt{-1}]$ for all p, the characteristic polynomial $\chi_p(x)$ is always congruent to $(x-1)^3$ mod 2. This shows that the mod 2 representation is trivial (up to semi-simplification). Therefore, we have chosen to consider the more interesting (and challenging) case $\ell = 3$.

[1] This also follows of course from the fact that S has good reduction away from 2.

The purpose of this article is thus to explain how we have almost certainly succeeded to compute explicitly the mod 3 representation

$$\rho_{u,3} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_3(\mathbb{F}_9)$$

found up to twist in $\mathrm{H}^2_{\text{ét}}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}/3\mathbb{Z})$.

Here and in the rest of the article, by *computing explicitly a mod ℓ Galois representation*, we mean computing a polynomial whose roots are permuted by Galois in the same way as the vectors in the space of the representation (so that its splitting field agrees with the field cut out by the representation), as well as extra data making it possible to determine for any unramified prime $p \in \mathbb{N}$ the image of the the Frobenius at p up to conjugacy. In our case, this implies in particular that our computations allow us to determine mod 3 the eigenvalue a_p of u for all $p \geqslant 5$. For instance, we can compute in four seconds that if $p = 10^{1000} + 453$ is the first prime after 10^{1000}, then $a_p \equiv -1 \bmod 3\mathbb{Z}[\sqrt{-1}]$. As a bonus, the Galois group of the polynomial that we thus obtain, which is by construction the image of $\rho_{u,3}$, turns out to be a particularly interesting subgroup of $\mathrm{GL}_3(\mathbb{F}_9)$ (cf. section 5).

Remark 1.5. Unfortunately, because of the reason given in remark 4.1, we are unable to certify rigorously that the results of our computations are correct. However, the fact that we are eventually able to recover the values of the a_p mod 3 from the representation (cf. section 6) shows that our results are correct beyond reasonable doubt.

The central idea making this computation possible, which we owe to J.-M. Couveignes, is a method to construct by *dévissage* a curve C (depending on ℓ) such that the reduction mod ℓ of $\widetilde{\rho}_{u,\ell}$ is contained in the ℓ-torsion of the Jacobian of C. The point is that once we have obtained an explicit model for C, we are able (at least in theory) to compute the representation, thanks to our technique presented in [Mas18c]. In principle, this *dévissage* technique could be iterated to construct a curve whose Jacobian contains a given representation found in the $\mathrm{H}^d_{\text{ét}}$ of a variety of dimension d.

We will sketch this construction in section 2, after which we will apply it to $\rho_{u,3}$ in section 3. Next, we will explain in section 4 how we used the curve thus obtained to compute a polynomial corresponding to $\rho_{u,3}$, after what we use this polynomial to determine the image of $\rho_{u,3}$ in section 5. Finally, we will show in section 6 how to compute the image of Frobenius elements.

2 Dévissage

Suppose we are given a surface S defined over $\mathbb{Q}$ as well as a prime $\ell \in \mathbb{N}$ such that $\mathrm{H}^2_{\text{ét}}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$ contains a Galois-submodule affording a mod ℓ Galois representation ρ that we wish to compute. We are going to show how to construct a curve C whose Jacobian will also contain ρ (up to twist) in its ℓ-torsion. Of course, this curve C will depend on ℓ. This construction is an example of the *dévissage* method summarized in [SGA4$\frac{1}{2}$, 3.4].

Let μ_ℓ be the Galois module formed by the ℓ-th roots of unity. Given a Galois module M and an integer $n \in \mathbb{Z}$, we will denote by $M(n)$ the twist of M by the n-th power of the mod ℓ cyclotomic character. Thus $\mu_\ell = (\mathbb{Z}/\ell\mathbb{Z})(1)$ for instance. We will sometimes write $\mu_\ell^\vee$ for $(\mathbb{Z}/\ell\mathbb{Z})(-1)$. Finally, we will also denote by μ_ℓ and $(\mathbb{Z}/\ell\mathbb{Z})(n)$ the corresponding constant sheaves on the étale site of a variety.

Recall [MilEC, 14.2] that when X is a complete, connected and non-singular curve over $\overline{\mathbb{Q}}$, we have canonical (and hence Galois-equivariant) identifications

$$\mathrm{H}^r_{\text{ét}}(X, \mu_\ell) \simeq \begin{cases} \mu_\ell & \text{if } r = 0, \\ J[\ell] & \text{if } r = 1, \\ \mathbb{Z}/\ell\mathbb{Z} & \text{if } r = 2, \end{cases}$$

where $J = \mathrm{Jac}(X)$ is the Jacobian of X. By tensoring out μ_ℓ, we deduce the identifications

$$\mathrm{H}^r_{\text{ét}}(X, \mathbb{Z}/\ell\mathbb{Z}) \simeq \begin{cases} \mathbb{Z}/\ell\mathbb{Z} & \text{if } r = 0, \\ J[\ell](-1) & \text{if } r = 1, \\ \mu_\ell^\vee & \text{if } r = 2. \end{cases} \tag{2.1}$$

If we let U be X with finitely many points deleted, which is thus still a non-singular connected curved but is no longer complete, then we obtain

$$\mathrm{H}^r_{\text{ét}}(U, \mathbb{Z}/\ell\mathbb{Z}) \simeq \begin{cases} \mathbb{Z}/\ell\mathbb{Z}, & \text{if } r = 0, \\ J[\ell](-1) \text{ extended by copies of } \mu_\ell^\vee & \text{if } r = 1, \\ 0 & \text{if } r = 2, \end{cases} \tag{2.2}$$

where the first case is obvious, and the last two follow respectively from corollary 16.2 and proposition 14.12 of [MilEC].

Suppose now that we have a proper regular surface S, equipped with a proper dominant morphism $\pi : S \longrightarrow B$ to a non-singular complete curve B, with S, B, and π defined over $\mathbb{Q}$.

Let $Z \subset B$ be a nonempty[2] finite subset containing the image of the bad fibres of π, and let $Y = \pi^{-1}(Z) \subset S$. Define $B' = B \setminus Z$, and $S' = S \setminus Y$, so that the fibre $S_b = S' \times_{B'} b$ at any $b \in B'$ of the induced map $\pi : S' \longrightarrow B'$ is a smooth proper curve. The representability of the relative Picard functor [BLR90, 9.4.4] thus guarantees the existence of a cover $\psi : C' \longrightarrow B'$ whose fibre at $b \in B'$ is $C'_b = \mathrm{Jac}(S_b)[\ell]$.

The closed subscheme Y of S is made up of curves, possibly with multiplicities, and intersecting in some way. Define Y' to be the scheme obtained from Y by first passing to the reduced scheme structure, and then deleting the singular points. Thus Y' is a disjoint union of smooth curves defined over $\mathbb{Q}$. Its geometrically irreducible components are therefore permuted by Galois; let

$$\eta = \prod_{\text{Components of } Y'} \mathbb{F}_\ell$$

be the corresponding mod ℓ permutation representation, and denote by $\eta(-1) = \eta \otimes \mu_\ell^\vee$ its twist by the inverse of mod ℓ cyclotomic character.

With this notation, we can prove that the "interesting" Galois representations which lie in $\mathrm{H}^2_{\text{ét}}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$ are also afforded in $\mathrm{H}^1_{\text{ét}}(C'_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$:

Theorem 2.3. *Suppose ρ is a mod ℓ Galois representation contained in $\mathrm{H}^2_{ét}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$ (up to semi-simplification). Assume that ρ has no Jordan-Hölder components of the form $(\mathbb{Z}/\ell\mathbb{Z})(n)$ for any $n \in \mathbb{Z}$, and no component in common with $\eta(-1)$. Then the twist of ρ by the mod ℓ cyclotomic character is also contained (up to semi-simplification) in $\mathrm{H}^1_{ét}(C'_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$.*

Remark 2.4. The number field cut out by $\eta(-1)$ is contained in the compositum of the ℓ-th cyclotomic field and of the fields of definition of the geometric components of the bad fibres

[2] We insist that Z must not be empty because we will need B' to be affine later.

of π. In general, we expect this field to be considerably smaller than that cut out by ρ if ρ is an "interesting" representation. For instance, for the surface considered in section 3 below, the field cut out by η is merely $\mathbb{Q}(\sqrt{2})$ (cf. remark 3.5). Therefore, the requirement that ρ have no common component with $\eta(-1)$ ought to be harmless for "interesting" representations ρ.

Proof. Let us first show that ρ is also contained in $\mathrm{H}^2_{\text{ét}}(S'_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$, so that the bad fibres of π will no longer be a nuisance. The localization exact sequence [MilEC, 9.4] shows that the kernel of $\mathrm{H}^2_{\text{ét}}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z}) \longrightarrow \mathrm{H}^2_{\text{ét}}(S'_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$ is a quotient of $\mathrm{H}^2_{\text{ét},Y}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$. Étale cohomology with coefficients in $(\mathbb{Z}/\ell\mathbb{Z})(n)$ satisfies the Bloch-Ogus axioms [BO74], so in particular the Poincaré duality axiom [Jan90, 6.1.j] shows that

$$\mathrm{H}^2_{\text{ét},Y}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z}) \simeq \mathrm{H}_2\big(Y_{\overline{\mathbb{Q}}}, (\mathbb{Z}/\ell\mathbb{Z})(2)\big).$$

Applying [Jan90, 6.1.f] twice shows that $\mathrm{H}_2\big(Y_{\overline{\mathbb{Q}}}, (\mathbb{Z}/\ell\mathbb{Z})(2)\big) \simeq \mathrm{H}_2\big(Y'_{\overline{\mathbb{Q}}}, (\mathbb{Z}/\ell\mathbb{Z})(2)\big)$, and since Y' is a disjoint union of smooth curves, applying Poincaré duality [Jan90, 6.1.j] and then (2.1) or (2.2) component-wise reveals that

$$\mathrm{H}_2\big(Y'_{\overline{\mathbb{Q}}}, (\mathbb{Z}/\ell\mathbb{Z})(2)\big) \simeq \eta(-1).$$

Our assumptions on ρ thus show that it must be contained in $\mathrm{H}^2_{\text{ét}}(S'_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$ as claimed.

Consider now the Leray spectral sequence [MilEC, 12.7]

$$E_2^{p,q} = \mathrm{H}^p_{\text{ét}}(B'_{\overline{\mathbb{Q}}}, R^q\pi_*\mathbb{Z}/\ell\mathbb{Z}) \Rightarrow \mathrm{H}^{p+q}_{\text{ét}}(S'_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$$

attached to $\pi : S' \longrightarrow B'$. We know by proper base change [MilEC, 17.7] that

$$R^q\pi_*\mathbb{Z}/\ell\mathbb{Z} = \mathrm{H}^q_{\text{ét}}(S_b, \mathbb{Z}/\ell\mathbb{Z}),$$

where by abuse of notation we denote by $\mathcal{M}_b$ instead of $\mathcal{M}$ the sheaf on B' whose stalk at b is $\mathcal{M}_b$. Besides, the base B' and the fibres S_b are non-singular connected curves, so $E_2^{p,q} = 0$ unless $0 \leqslant p, q \leqslant 2$. Therefore $E_2^{p,q} = E_\infty^{p,q}$ for all p, q such that $p + q = 1$, which means that $H^2(S_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$ admits a filtration with components

- $\mathrm{H}^2_{\text{ét}}(B'_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z}) = 0$ by (2.2),
- $\mathrm{H}^0_{\text{ét}}\big(B'_{\overline{\mathbb{Q}}}, H^2(S_b, \mathbb{Z}/\ell\mathbb{Z})\big) = \mathrm{H}^0_{\text{ét}}(B'_{\overline{\mathbb{Q}}}, \mu_\ell^\vee) = \mu_\ell^\vee$ by (2.1) and (2.2),
- and $\mathrm{H}^1_{\text{ét}}(B'_{\overline{\mathbb{Q}}}, \mathcal{F})$,

where $\mathcal{F}$ is the sheaf on B' with stalks

$$\mathcal{F}_b = \mathrm{H}^1_{\text{ét}}(S_b, \mathbb{Z}/\ell\mathbb{Z}) = C'_b(-1)$$

by (2.1) and the definition $C'_b = \mathrm{Jac}(S_b)[\ell]$. Our assumptions on ρ thus show that it must be contained in $\mathrm{H}^1_{\text{ét}}(B'_{\overline{\mathbb{Q}}}, \mathcal{F})$.

Similarly, the Leray spectral sequence

$$\mathrm{H}^p_{\text{ét}}(B'_{\overline{\mathbb{Q}}}, R^q\psi_*\mathbb{Z}/\ell\mathbb{Z}) \Rightarrow \mathrm{H}^{p+q}_{\text{ét}}(C'_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$$

attached to $\psi : C' \longrightarrow B'$ shows that $\mathrm{H}^1_{\text{ét}}(C'_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z}) = \mathrm{H}^1_{\text{ét}}(B'_{\overline{\mathbb{Q}}}, \mathcal{G})$, where

$$\mathcal{G}_b = \mathrm{H}^0_{\text{ét}}(C'_b, \psi_*\mathbb{Z}/\ell\mathbb{Z}) = {\mathbb{F}_\ell}^{C'_b}.$$

Since $C'_b = \mathrm{Jac}(S_b)[\ell]$ is an Abelian ℓ-torsion group, there is a natural surjection

$$\begin{array}{rcl} \mathcal{G}_b = \mathbb{F}_\ell{}^{C'_b} & \longrightarrow & C'_b = \mathcal{F}_b(1) \\ \lambda & \longmapsto & \sum_{c \in C'_b} \lambda_c \, c \end{array}$$

which, after twisting, yields an epimorphism $\mathcal{G}(-1) \twoheadrightarrow \mathcal{F}$. Let $\mathcal{K}$ by its kernel, so that we have the short exact sequence

$$0 \longrightarrow \mathcal{K} \longrightarrow \mathcal{G}(-1) \longrightarrow \mathcal{F} \longrightarrow 0$$

of sheaves on $B'_{\overline{\mathbb{Q}}}$. The associated long exact sequence contains

$$\cdots \longrightarrow \mathrm{H}^1_{\text{ét}}\big(B'_{\overline{\mathbb{Q}}}, \mathcal{G}(-1)\big) \longrightarrow \mathrm{H}^1_{\text{ét}}(B'_{\overline{\mathbb{Q}}}, \mathcal{F}) \longrightarrow \mathrm{H}^2_{\text{ét}}(B'_{\overline{\mathbb{Q}}}, \mathcal{K}) \longrightarrow \cdots,$$

and as $\mathrm{H}^2_{\text{ét}}(B'_{\overline{\mathbb{Q}}}, \mathcal{K}) = 0$ by [SGA4$\frac{1}{2}$, 1.3.3.6.ii], we conclude that since ρ is contained in $\mathrm{H}^1_{\text{ét}}(B'_{\overline{\mathbb{Q}}}, \mathcal{F})$, it also appears in

$$\mathrm{H}^1_{\text{ét}}\big(B'_{\overline{\mathbb{Q}}}, \mathcal{G}(-1)\big) = \mathrm{H}^1_{\text{ét}}(C'_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})(-1).$$

□

The curve C' constructed in theorem 2.3 will not, in general, be connected, because of the zero section $0 \in \mathrm{Jac}(S_b)[\ell] = C'_b$. However, we can modify the definition of C' so that

$$C'_b = \mathrm{Jac}(S_b)[\ell] \setminus \{0\}.$$

The curve thus redefined has now a good chance of being geometrically connected, and will contain[3] ρ in its $\mathrm{H}^1_{\text{ét}}$. Assuming that C' is indeed connected, let C be the smooth proper model of C' over $\mathbb{Q}$; as $\mathrm{H}^1_{\text{ét}}(C'_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$ is an extension of $\mathrm{H}^1_{\text{ét}}(C_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$ by copies of $\mu_\ell^\vee$ according to (2.2), we conclude by (2.1) that the twist of ρ by a power of the cyclotomic character will be contained in $\mathrm{Jac}(C)[\ell]$ up to semi-simplification.

This leads to the following plan of attack to compute $\rho \subset \mathrm{H}^2_{\text{ét}}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$:

1. Compute the Galois representations afforded by the ℓ-torsion of the Jacobian of the fibre S_b of π for various $b \in B$,
2. Interpolate to glue these data into an explicit model of the cover $C \longrightarrow B$,
3. Catch a twist of ρ in the ℓ-torsion of the Jacobian of C.

The first and last steps require one to be able to compute explicitly the representations afforded by the torsion of the Jacobian of any smooth curve, which we can do thanks to the method presented in [Mas18c]. In fact, this is the reason why we invented this method in the first place.

The "interpolation" part of the second step, as presented here, is quite vague. Fortunately, this will not be a problem for the example that we have in mind, because the fibres S_b will be elliptic curves. We have not yet studied how to treat the general case.

[3] Unless ρ comes from $\mathrm{H}^1_{\text{ét}}(B_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$, but in this case we could compute it in the Jacobian of B in view of (2.1).

3 Computation of a nice model of C

We now apply the method presented in the previous section to the case of the representation $\rho_{u,3}$ introduced in section 1. According to [GT94, 3.10], for all ℓ, the mod ℓ representation $\rho_{u,\ell}\otimes\left(\frac{-2}{\cdot}\right)$ is contained in $\mathrm{H}^2_{\text{ét}}(S_{\overline{\mathbb{Q}}},\mathbb{Z}/\ell\mathbb{Z})$, where S is the minimal regular model of the projective closure of the surface over $\mathbb{Q}$ of equation

$$z^2 = xy(x^2-1)(y^2-1)(x^2-y^2+2xy). \tag{3.1}$$

In order to apply the method presented in the previous section to this surface, we need to choose a non-constant map $\pi : S \longrightarrow B$, where B is a curve. We choose $B = \mathbb{P}^1$ with coordinate λ, and π the map sending (x, y, z) to $\lambda = y/x$.

Remark 3.2. Although π is only a rational map from the surface defined by equation (3.1) to $\mathbb{P}^1$, it becomes a morphism once we blow up this surface in order to obtain a regular model. In fact, π is the canonical map of S (cf. [GT94, 3.2]).

The fibre of π at λ is obtained by setting $y = \lambda x$ in (3.1). The locus of bad fibres is

$$Z = \{0, \pm 1, 1 \pm \sqrt{2}, \infty\} \subset B,$$

and for $\lambda \notin Z$, the fibre is an elliptic curve E_λ over $\mathbb{Q}$. These E_λ define an elliptic curve over $\mathbb{Q}(\lambda)$ isomorphic to

$$y^2 = \lambda(\lambda^2-2\lambda-1)(x-2\lambda)(x+2\lambda)(x+\lambda^2+1), \tag{3.3}$$

whose j-invariant is $2^4\dfrac{(\lambda^4+14\lambda^2+1)^3}{\lambda^2(\lambda^2-1)^4}$.

Remark 3.4. Equation (3.3) reveals that $E_\lambda[2]$ is already defined over $\mathbb{Q}(\lambda)$. This reflects the fact that the mod 2 representation $\rho_{u,2}$ attached to u is trivial (up to semi-simplification), as we noted in remark 1.4.

The ℓ-division polynomial $\psi_{\ell,\lambda}(x)$ of E_λ is easily computed thanks to [Pari/GP]. By definition, for each λ, the Galois action on the roots of $\psi_{\ell,\lambda}(x)$ describes the Galois action on the x-coordinates of the points of $E_\lambda[\ell]$. We then compute $R_{\ell,\lambda}(y)$, the resultant in x of $\psi_{\ell,\lambda}(x)$ and of the Weierstrass equation (3.3) of E_λ, which yields a polynomial describing the Galois action on the y-coordinates of $E_\lambda[\ell]$. For $\ell = 3$, the y-coordinate happens to be injective on $E_\lambda[\ell]$ for generic λ; indeed, $R_{3,\lambda}(y)$ is squarefree for $\lambda = 2$.

We have thus computed the mod 3 Galois representation afforded by the Jacobian of the fibre of π in terms of λ. Substituting x for λ, we obtain the following rather ugly plane model for C:

$$\begin{aligned}
&-256x^{56}+6144x^{55}-62464x^{54}+333824x^{53}-859648x^{52}-120832x^{51}+7252992x^{50}-16046080x^{49}-9891072x^{48}+90136576x^{47}\\
&-73076736x^{46}-237805568x^{45}+420485120x^{44}+341843968x^{43}-1165840384x^{42}-192667648x^{41}+2178936320x^{40}-238563328x^{39}\\
&-3063240704x^{38}+639488000x^{37}+3412593664x^{36}-639488000x^{35}-3063240704x^{34}+238563328x^{33}+2178936320x^{32}+192667648x^{31}\\
&-1165840384x^{30}-341843968x^{29}+(-288y^4+420485120)x^{28}+(3456y^4+237805568)x^{27}+(-14400y^4-73076736)x^{26}\\
&+(14976y^4-90136576)x^{25}+(56160y^4-9891072)x^{24}+(-142848y^4+16046080)x^{23}+(-52992y^4+7252992)x^{22}+(400896y^4+120832)x^{21}\\
&+(-55872y^4-859648)x^{20}+(-624384y^4-333824)x^{19}+(134784y^4-62464)x^{18}+(624384y^4-6144)x^{17}+(-55872y^4-256)x^{16}\\
&+(16y^6-400896y^4)x^{15}+(-96y^6-52992y^4)x^{14}+(-384y^6+142848y^4)x^{13}+(3232y^6+56160y^4)x^{12}+(-5424y^6-14976y^4)x^{11}\\
&+(960y^6-14400y^4)x^{10}-3456y^4x^9+(960y^6-288y^4)x^8+5424y^6x^7+3232y^6x^6+384y^6x^5-96y^6x^4-16y^6x^3+27y^8=0.
\end{aligned}$$

A [Magma] session still manages to reveal in a few seconds that C is geometrically integral and has (geometric) genus $g = 7$. This is good news, as our method [Mas18c] probably cannot reasonably cope with genera beyond 20 or 30.

Remark 3.5. We can easily do the same computation for other values of ℓ, and thus get plane models of curves C that contain a twist of $\rho_{u,\ell}$ in their Jacobian. However, already for $\ell = 5$, the model we get is so terrible that [Magma] is unable to determine its genus (the computation was interrupted after 5 days, because it was using more than 400GB of RAM).

We can still compute this genus, by exploiting the fact that $\pi : S \longrightarrow B$ is an elliptic surface. Indeed, since $B = \mathbb{P}^1_\lambda$ has genus 0, Riemann-Hurewicz tells us that if C is connected, then its genus is

$$g = 1 - d + \frac{1}{2}\sum_{c\in C}(e_c - 1),$$

where $d = \ell^2 - 1$ is the degree of the projection $\psi : C \longrightarrow B$ induced by π, and the e_c are its ramification indices.

Rewrite

$$\sum_{c\in C}(e_c - 1) = \sum_{\lambda\in B}\sum_{\psi(c)=\lambda}(e_c - 1),$$

and notice that for each λ, we have

$$\sum_{\psi(c)=\lambda}(e_c - 1) = \sum_{\psi(c)=\lambda} e_c - \sum_{\psi(c)=\lambda} 1 = d - \#\psi^{-1}(\lambda).$$

Besides, the ramification of ψ can only come from the bad fibres of π, so this expression is 0 for $\lambda \notin Z$.

Our surface S is the minimal proper regular model of E_λ/B, so we can analyse its bad fibres thanks to Tate's algorithm. It reveals that at $\lambda = 0$ and ∞, the special fibre is of Kodaira type I_2^*, which, according to Table 6 of [BHPvV, V.10], implies that the monodromy around λ acts on the homology of the fibre of π by $T = -\left[\begin{smallmatrix}1 & 2\\ 0 & 1\end{smallmatrix}\right]$. If ℓ is an odd prime, this means that $\#\psi^{-1}(\lambda)$, which is the number of orbits of T acting on ${\mathbb{F}_\ell}^2 \setminus \{0\}$, is $\frac{1}{2\ell}\big(1(\ell^2-1) + (\ell-1)(\ell-1)\big) = 2\ell - 2$ by Burnside's formula. Similarly, at $\lambda = \pm 1$, the special fibre is of type I_4, whence $T = \left[\begin{smallmatrix}1 & 4\\ 0 & 1\end{smallmatrix}\right]$ and $\#\psi^{-1}(\lambda) = 2\ell - 2$; whereas at $\lambda = 1 \pm \sqrt{2}$, the special fibre is of type I_0^*, whence $T = -\left[\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right]$ and $\#\psi^{-1}(\lambda) = \frac{\ell^2-1}{2}$.

As a result, we find that if ℓ is an odd prime and if C is connected, then its genus is

$$g = \frac{3}{2}\ell^2 - 3\ell + \frac{5}{2}.$$

In particular, we recover $g = 7$ for $\ell = 3$, and we find that $g = 25$ for $\ell = 5$ and that $g = 55$ for $\ell = 7$. This means that our method [Mas18c] could probably manage to compute the mod 5 representation $\rho_{u,5}$ if we could find a decent enough model for C for $\ell = 5$ and if we were patient enough, whereas $\ell \geqslant 7$ seems out of our reach.

Let us get back to the case $\ell = 3$ and to our curve C of genus 7. The model that we have just obtained has degree 56, and therefore arithmetic genus 1485. We do not want to work with such a badly singular model, so we attempt to eliminate the worst of the singularities by having [Magma] determine the canonical image of C in $\mathbb{P}^6$ and project it on a plane. This yields the already more appealing model

$$\begin{aligned}(&-374594220y^6 + 148459311y^5 - 20961720y^4 + 1285362y^3 - 35100y^2 + 351y)x^4\\ &+ (-61958809438y^8 + 12030741624y^7 - 574743724y^6 - 5928484y^5 + 27600y^4 + 129884y^3 - 8516y^2 + 216y - 2)x^2\\ &+ (15790199962940y^{10} - 5854413418867y^9 + 927447207596y^8 - 81010188948y^7 + 4049824636y^6 - 100135334y^5\\ &\qquad - 48724y^4 + 70252y^3 - 1664y^2 + 13y) = 0.\end{aligned}$$

We check that this model still has genus 7, which by Riemann-Hurwitz ensures that it is birational to the previous one, as opposed to being a quotient of it.

By projecting the canonical image onto another plane, we also find that C is a cover of degree 2 (simply given by $x \mapsto x^2$ on our new model) of a curve E of genus 1, which turns out to be an elliptic curve isomorphic to the modular curve $X_0(24)$. We learn from the [LMFDB] that this curve has rank 0; after careful back-tracking, this allows us to determine the complete list of rational points of C in our new model.

In order to further simplify our model for C, we turn to a trial-and-error manual shifting and rescaling process based on the shape of the rational points thus obtained and on the observation of the p-adic valuations of the coefficients of our model for small primes p. After a few attempts, we obtain the quite satisfying model

$$\begin{aligned}(3y^5 - 6y^3 + 3y)x^4 + (2y^8 - 8y^7 + 4y^6 + 12y^5 + 12y^3 - 4y^2 - 8y - 2)x^2 \\ + (9y^9 - 36y^8 - 36y^7 + 36y^6 + 18y^5 - 36y^4 - 36y^3 + 36y^2 + 9y) = 0. \quad (3.6)\end{aligned}$$

Remark 3.7. The whole process to obtain a nice model for C was rather rustic. Most computer algebra systems include algorithms that, given a complicated polynomial defining a number field, are able to find a much simpler polynomial defining the same field (when it exists); it would be nice to have similar algorithms for curves!

Remark 3.8. The automorphism ϕ_S of order 4 of S mentioned in section 1 is given by $(x, y, z) \mapsto (y, -x, z)$ on the model (3.1) according to [GT94, 3.4]. It naturally induces an automorphism ϕ_C of C, which still has order 4 since it defines the $\mathbb{F}_9 = \mathbb{F}_3(\sqrt{-1})$-vector space structure on the piece of the 3-torsion of the Jacobian of C that affords $\rho_{u,3}$. Although is not too difficult to determine that ϕ_S is given by

$$(x, y, \lambda) \mapsto \left(-2\frac{x + 2\lambda^2 - 2\lambda + 2}{\lambda(x + 2\lambda)}, \left(\frac{2(\lambda - 1)}{\lambda^2(x + 2\lambda)}\right)^2 y, -\frac{1}{\lambda}\right)$$

on (3.3), it is arduous to determine explicitly the action of ϕ_C on (3.6) because of the method by which we have obtained this model. Fortunately, it is simple enough that [Magma] is able to inform us that the automorphism group of C happens to be cyclic of order 4, and to provide us with an explicit generator, which must therefore coincide with ϕ_C or its inverse. We thus find that the action of ϕ_C on (3.6) is simply given by $(x, y) \mapsto (\pm x/y, -1/y)$; in particular, the map $x \mapsto x^2$ mentioned above is actually the quotient by ϕ_C^2. However, we will see in remark 4.3 below that knowing the action of ϕ_C explicitly does not really help to speed up our computations. We still note that if we homogenize (3.6) and then dehomogenize with respect to x, then ϕ_C becomes a mere rotation of angle $\pi/2$ around the origin; it may be that for general ℓ, simple models of C could be obtained by looking for ones such that ϕ_C acts in a similarly simple way.

The arguments of the previous section show that the 3-torsion of the Jacobian of (3.6) contains the representation contained in $\mathrm{H}^2_{\text{ét}}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}/3\mathbb{Z})$ up to twist by the mod 3 cyclotomic character χ_3, which agrees with the quadratic character $\left(\frac{-3}{\cdot}\right)$. Since this representation was already the twist of the representation $\rho_{u,3}$ we are interested in by $\left(\frac{-2}{\cdot}\right)$, this is just an extra twist.

In order to confirm this, we can check that the characteristic polynomials match at a few primes p. Indeed, let $\rho'_{u,3}$ be the $\mathrm{GL}_6(\mathbb{F}_3)$-valued representation obtained by restricting the scalars from the $\mathrm{GL}_3(\mathbb{F}_9)$-valued representation $\rho_{u,3}$. On the one hand, we know that for $p \neq 2, 3$, the characteristic polynomial of $\rho'_{u,3}(\mathrm{Frob}_p)$ is

$$\chi'_p(x) = \chi_p(x)\overline{\chi_p(x)} = (x^3 - a_p x^2 + p\overline{a_p}x - p^3)(x^3 - \overline{a_p}x^2 + pa_p x - p^3) \in \mathbb{F}_3[x],$$

the norm from $\mathbb{F}_9$ to $\mathbb{F}_3$ of the polynomial $\chi_p(x)$ given in (1.3), and furthermore [GT94, 2.5] provides us with the values of the Hecke eigenvalues a_p of u for $p \leqslant 67$. On the other hand, we can determine the characteristic polynomial $L_p(x) \in \mathbb{Z}[x]$ of the Frobenius at p acting on the Jacobian of C (which is the local factor at p of its L function) by counting the $\mathbb{F}_{p^a}$-points of C for $a \leqslant g$, where $g = 7$ is the genus of C; in practice, [Magma] can do this in reasonable time for $p \leqslant 19$. We then check that for $5 \leqslant p \leqslant 19$, $L_p(x)$ mod 3 is divisible by the characteristic polynomial $\chi'_p(\epsilon x)$ of the image of Frob_p by $\rho'_{u,3} \otimes \left(\frac{6}{\cdot}\right)$, where $\epsilon = \left(\frac{6}{p}\right) = \pm 1$. This corroborates the fact that the Jacobian J of C contains $\rho'_{u,3} \otimes \left(\frac{6}{\cdot}\right)$ in its 3-torsion.

Remark 3.9. Since $g = 7$, the degree of $L_p(x)$ is 14. We actually observe that for all the primes $5 \leqslant p \leqslant 19$ that we can test, $L_p(x)$ is congruent mod 3 to the product

$$\chi_{E,p}(x)\, \chi'_p\big(\left(\tfrac{6}{p}\right)x\big)\, \chi'_p\big(\left(\tfrac{-2}{p}\right)x\big)$$

where the factors have respective degrees 2, 6, and 6, and are the characteristic polynomial of Frob_p for the mod 3 representation $\rho_{E,3}$ attached to the elliptic curve $E = X_0(24)$ exhibited above, the expected twist $\rho'_{u,3} \otimes \left(\frac{6}{\cdot}\right)$, and the twist $\rho'_{u,3} \otimes \left(\frac{-2}{\cdot}\right)$ originally contained in $\mathrm{H}^2_{\text{ét}}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}/3\mathbb{Z})$, respectively. The fact that we eventually managed to compute $\rho'_{u,3} \otimes \left(\frac{6}{\cdot}\right)$ from a piece of $J[3]$, whereas we were unable to do the same for $\rho'_{u,3} \otimes \left(\frac{-2}{\cdot}\right)$ (even after significantly increasing the p-adic accuracy in our computation, cf. the next section), leads us to guess that the Galois-module $J[3]$ decomposes as

$$J[3] \sim \begin{bmatrix} \rho_{E,3} & & \\ & \rho'_{u,3} \otimes \left(\frac{6}{\cdot}\right) & * \\ & & \rho'_{u,3} \otimes \left(\frac{-2}{\cdot}\right) \end{bmatrix},$$

where $*$ is non-trivial. In other words, the twist $\rho'_{u,3} \otimes \left(\frac{-2}{\cdot}\right)$ originally contained in $\mathrm{H}^2_{\text{ét}}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}/3\mathbb{Z})$ seems to show up as *quotient* of $J[3]$.

4 Computation of the representation in J

Now that we have obtained a reasonable model for C, we are going to use our method [Mas18c] to compute the representation $\rho'_{u,3} \otimes \left(\frac{6}{\cdot}\right)$ afforded by a Galois submodule T of the 3-torsion of the Jacobian J of C. This method requires us to pick a prime p of good reduction for which the local L factor

$$L_p(x) = \det(x - \mathrm{Frob}_p \,|J) \in \mathbb{Z}[x]$$

and the characteristic polynomial

$$\chi'_p\big(\left(\tfrac{6}{p}\right)x\big) = \det(x - \mathrm{Frob}_p \,|T) \in \mathbb{F}_3[x]$$

are known, and such that $\chi'_p\big(\left(\frac{6}{p}\right)x\big)$ is coprime to its cofactor $L_p(x)/\chi'_p\big(\left(\frac{6}{p}\right)x\big)$. We choose $p = 11$, which satisfies these assumptions. Besides, we then have

$$\chi'_p\big(\left(\tfrac{6}{p}\right)x\big) = \sum_{k=0}^{6} x^k \in \mathbb{F}_3[x],$$

which is irreducible; this fact will be useful on two occasions below.

Our method performs by generating points of $J[3]$ over an appropriate extension of $\mathbb{F}_{11}$ and projecting them onto T thanks to the action of Frob_{11} until we get a basis of T, to lift this

basis 11-adically, and then to evaluate a Galois-equivariant rational map α from J to $\mathbb{A}^1$ at the points of T. If the 11-adic accuracy is sufficient, then we will be able to identify the coefficients of the polynomial

$$F(x) = \prod_{\substack{t \in T \\ t \neq 0}} \big(x - \alpha(t)\big)$$

as rational numbers; if furthermore α is injective on T, we will thus have obtained a polynomial whose roots are permuted under Galois just as the non-zero points of T are.

Here, the fact that the characteristic polynomial of Frob_{11} is squarefree implies that Frob_{11} is a cyclic endomorphism of the $\mathbb{F}_3$-vector space T, which means that we can afford to lift only one point of T and recover a basis by applying Frob_{11} repeatedly (cf. section 6.4 of [Mas18c]).

Remark 4.1. The fact that we identify the coefficients of $F(x)$ from their p-adic approximations is the reason why we cannot rigorously certify that our computation results are correct. Nevertheless, we will give in section 6 below very strong evidence that these results are correct beyond reasonable doubt.

In order to be able to compute in J, we need to fix an effective divisor D_0 on C of degree $d_0 \geqslant 2g+1 = 15$ for which we can explicitly compute the corresponding Riemann-Roch space. In order to construct the evaluation map α, we also need to pick two non-equivalent effective divisors E_1, E_2 of degree $d_0 - g$ such that we can also compute the Riemann-Roch spaces attached to $2D_0 - E_1$ and $2D_0 - E_2$ (the notations are the same as in [Mas18c]).

It is qualitatively clear that we should strive to choose D_0, E_1, and E_2 so that these three Riemann-Roch spaces are as "nice" as possible, since the values of α will then have smaller arithmetic height, so that the p-adic accuracy required to identify the coefficients of $F(x)$ will be lower and the computation will be more efficient. After a bit of experimentation with [Magma], we choose

$$d_0 = 16, \quad D_0 = 9P + 7Q, \quad E_1 = 6P + 3Q, \quad E_2 = 5P + 4Q,$$

where $P, Q \in C(\mathbb{Q})$ are points such that, in the model obtained at the end of the previous section, the divisors of poles of x and y are respectively

$$(x)_\infty = 3P + Q + R + M_1 + M_2 \text{ and } (y)_\infty = 2P + 2Q$$

where R has degree 1 and M_1 and M_2 both have degree 2.

Remark 4.2. It may happen that the $\mathbb{Q}$-basis of a Riemann-Roch space provided by [Magma] becomes linearly dependent when reduced mod p. Fortunately, this is easy to detect, because functions on C are represented internally in [Mas18c] as the vector of their values at a large enough set of fixed points of C. This is also easy to fix, by Gaussian elimination: given $s_1, \cdots, s_d \in \mathbb{Q}(C)$ forming the basis of a given Riemann-Roch space, if $\sum_i \lambda_i s_i \equiv 0 \bmod p$ for some $\lambda_i \in \mathbb{F}_p$ not all 0, it suffices to substitute $\frac{1}{p}\sum_i \widetilde{\lambda}_i s_i$ to s_j, where j is such that $\lambda_j \neq 0$ and the $\widetilde{\lambda}_i$ are lifts to $\mathbb{Z}$ of the λ_i. However, this complicates the basis of the Riemann-Roch space, which in turn increases the height of the values of the evaluation map α. Fortunately, this phenomenon does not occur with our choices of D_0, E_1, E_2 and p.

Now that we have made these choices, we are ready to launch the computations. After about 30 hours of CPU time (but only 1 hour of real time, thanks to parallelisation), we obtain a polynomial $F(x)$ of degree $3^6 - 1 = 728$ whose coefficients are rational numbers which all have (up to some small factors) the same denominator, a 191-digit integer. The p-adic precision used was $O(11^{1024})$.

The discriminant of $F(x)$ factors into a large power of 2 times a huge power of 3 times a large square, which indicates that its coefficients have probably been correctly identified from their p-adic approximations. The fact that discriminant is non-zero also shows that α is injective on T minus the origin, so that the roots of $F(x)$ represent faithfully the Galois action on T minus the origin, as desired.

Remark 4.3. Evaluating the map α at points of T with high 11-adic precision is computationally costly. As explained in [Mas18c, 6.4], we save a lot of time thanks to the fact that we are able to apply explicitly the Frobenius to the points of T: not only does this allow us to generate new points of T from old ones, but it also reduces the number of evaluations of the map α, since it commutes with the Frobenius. It is tempting (and not difficult, by the same method as in [Mas18c, 2.2.5]) to use the same idea with the automorphism of order 4 induced on J by ϕ_C; unfortunately, while this allows us to generate even more points of T from old ones, this does not reduce the number of evaluations of α, and therefore only saves a marginal amount of computation time.

5 The image of $\rho_{u,3}$

We find that the polynomial $F(x)$ computed in the previous section has three factors over $\mathbb{Q}$, of respective degrees 224, 252, and 252. This shows that the image of our representation does not act transitively on $\mathbb{F}_3^6$ minus the origin.

However, the degrees of these factors do not clearly indicate which subgroup of $\mathrm{GL}_6(\mathbb{F}_3)$ we are dealing with. In order to figure this out, we would like to determine the Galois groups of these factors; however, their degrees and heights are far too large for standard Galois group computation algorithms. We would therefore like to reduce these factors (in the sense of remark 3.7), but they are actually too large even for this!

As in [Mas18a, section 2], we circumvent this problem by considering the *projective* version of our representation, which has values in $\mathrm{PGL}_3(\mathbb{F}_9)$. We can obtain a polynomial corresponding to this representation by gathering the 11-adic roots $\alpha(t)$ of $F(x)$ along the $\mathbb{F}_9$-vector lines of T in a symmetric way (e.g. by summing or multiplying them). However, this requires us to understand the $\mathbb{F}_9$-structure of T, whereas we only know the $\mathbb{F}_3$-structure for now.

The most direct way to obtain this consists in using the action induced by the automorphism ϕ_C of order 4 of C, since it corresponds to multiplication by $i \in \mathbb{F}_9 = \mathbb{F}_3(i)$ on T; indeed, as explained in remark 4.3, it is not difficult to compute this action explicitly. However, there is also another method. Indeed, let $\Phi \in \mathrm{GL}(T)$ be the action of Frob_{11} on T. We know that $\mathbb{F}_9^\times$ acts on T by a cyclic subgroup of $\mathrm{GL}(T)$ of order 8 contained in the commutant of Φ, but luckily, Φ is cyclic, so its commutant is simply $\mathbb{F}_3[\Phi]$, which is a ring isomorphic to $\mathbb{F}_{3^6}$ since the characteristic polynomial of Φ is isomorphic over $\mathbb{F}_3$. In particular, there is a unique cyclic subgroup of order 8 in $\mathbb{F}_3[\Phi]^\times$, which must thus agree with the action of $\mathbb{F}_9^\times$.

Either way, we can thus compute as above a polynomial $F_0(x)$ of degree $\frac{1}{8}\deg F = 91$ describing the projective representation attached to $\rho_{u,3} \otimes \left(\frac{6}{\cdot}\right)$ (which is also that attached to $\rho_{u,3}$).

We can also be a bit more subtle, and consider all intermediate representations between the linear one and the projective one. Let us write $\mathbb{F}_9 = \mathbb{F}_3(i)$, where $i^2 = -1$. Then the subgroups of $\mathbb{F}_9^\times$ are, in decreasing order,

$$\mathbb{F}_9^\times \;\geqslant\; \{\pm 1, \pm i\} \;\geqslant\; \{\pm 1\} \;\geqslant\; \{1\}.$$

We can construct as above polynomials $F_0(x)$, $F_1(x)$, $F_2(x)$ and $F_3(x) = F(x)$ describing the corresponding quotients of $\rho_{u,3} \otimes \left(\frac{6}{\cdot}\right)$. These polynomials factor over $\mathbb{Q}$ as follows:

Quotient by	Degrees of factors
$\mathbb{F}_9^\times$	$28 + 63$
$\{\pm 1, \pm i\}$	$56 + 63 + 63$
$\{\pm 1\}$	$112 + 126 + 126$
$\{1\}$	$224 + 252 + 252.$

These degrees still do not clearly indicate what the image of the representation is. If anything, the fact that we have two factors for the projective representation that become three factors afterwards is rather mysterious.

Fortunately, one of the factors of $F_0(x)$ has degree 28, which is small enough that we can compute a much simpler polynomial defining the same number field, namely

$$\begin{aligned} x^{28} - 12x^{27} + 60x^{26} - 132x^{25} - 30x^{24} + 624x^{23} + 420x^{22} - 7704x^{21} \\ + 17118x^{20} - 9504x^{19} - 14424x^{18} + 10824x^{17} + 36492x^{16} - 64992x^{15} + 19488x^{14} \\ + 56064x^{13} - 89604x^{12} + 109296x^{11} - 88368x^{10} - 11472x^9 + 58488x^8 - 130176x^7 \\ + 34224x^6 - 58272x^5 - 39960x^4 + 32256x^3 + 24480x^2 - 352x - 1776. \end{aligned}$$

This polynomial is nice enough that [Magma] can rigorously determine its Galois group in less than a minute. This group turns out to be $\mathrm{PSU}_3(\mathbb{F}_9)$ (as we could have predicted, cf. remark 5.3 below), which explains all the observations made above!

Indeed, first of all one checks thanks to [Pari/GP] that the field defined by the factor of degree 63 of $F_0(x)$ is contained in the compositum of the field defined by that of degree 28 with itself, which shows that these factors have the same splitting field. Next, since there are no nontrivial cube roots of unity in characteristic 3, the quotient $\mathrm{SU}_3(\mathbb{F}_9) \longrightarrow \mathrm{PSU}_3(\mathbb{F}_9)$ is actually an isomorphism; in particular, it admits a section. This means that one twist of $\rho_{u,3}$ has image $\mathrm{SU}_3(\mathbb{F}_9)$ (and actually, this twist is the one by the mod 3 cyclotomic character $\chi_3 = \left(\frac{-3}{\cdot}\right)$ since we have seen that $\det \rho_{u,3} = \chi_3^3 = \chi_3$).

Let now H be a non-degenerate Hermitian form on the space $\mathbb{F}_{q^2}^n$, where q is a prime power and $n \in \mathbb{N}$, and let A_n (respectively B_n) be the number of elements $t \in \mathbb{F}_{q^2}^n$ such that $H(t) = 1$ (respectively, such that $H(t) = 0$). Since the norm between finite fields is surjective, A_n is also the number of elements $t \in \mathbb{F}_{q^2}^n$ such that $H(t)$ has prescribed value $y \in \mathbb{F}_q^\times$. From this fact, one easily determines a crossed recurrence relation satisfied by A_n and B_n, from which one deduces that

$$A_n = q^{2n-1} + (-q)^{n-1}, \quad B_n = q^{2n-1} - (q-1)(-q)^{n-1}.$$

For $n = 3$ and $q = 3$, one finds $A_n = 252$ and $B_n = 225$, which explains the shape $224+252+252$ of the factorization of $F_3(x)$: the first factor corresponds to the nonzero isotropic $t \in T$, and the other two correspond to the t such that $H(t) = 1$ (respectively, such that $H(t) = -1$).

Similarly, the Galois group of the factor of degree 28 of $F_0(x)$ is permutation-isomorphic to $\mathrm{PSU}_3(\mathbb{F}_9)$ acting on the isotropic lines of $\mathbb{F}_9^3$, whereas that of the factor of degree 63 corresponds to the action of $\mathrm{PSU}_3(\mathbb{F}_9)$ on non-isotropic lines.

Finally, the fact that the value of H is not well defined at a non-isotropic t known up to scaling by $\mathbb{F}_9^\times$, but becomes well-defined if we know t up to scaling by

$$\{\pm 1, \pm i\} = \mathrm{Ker}\,\mathrm{Norm} : \mathbb{F}_9^\times \to \mathbb{F}_3^\times,$$

explains why the factor of degree 63 of $F_0(x)$ yields two factors of degree 63 of $F_1(x)$ instead of one of degree 126.

Remark 5.1. We have also obtained a simpler polynomial of degree 63 defining the same number field as this factor of degree 63. This polynomial is available on the author's web page [Mas], and we do not reproduce it here. The polynomial of degree 28 displayed above and this polynomial of degree 63 thus solve the inverse Galois problem for the standard actions of the simple group $\mathrm{PSU}_3(\mathbb{F}_9)$ in respective degrees 28 and 63, and with controlled ramification (only at 2 and 3) to boost! The respective discriminants and signatures of the corresponding number fields are as follows:

Degree	Discriminant	Signature
28	$2^{76}3^{48}$	$(4, 12)$
63	$2^{166}3^{108}$	$(7, 28)$.

Remark 5.2. Since factors of the $F_i(x),\ 0 \leqslant i \leqslant 3$ correspond to towers of quadratic extensions, we can use the techniques presented in [Mas18a, section 2] to compute nice polynomials defining the same number fields as the factors of $F_3(x)$. This technique has the advantage of naturally producing even polynomials, such that the field automorphism induced by $x \mapsto -x$ corresponds to the action of $-1 \in \mathbb{F}_9^\times$. This means that given such a polynomial $f(x^2)$, the polynomial $f(Dx^2)$ corresponds to the twist of the representation by $\left(\frac{D}{\cdot}\right)$ for any $D \in \mathbb{Q}^\times$. By taking $D = -3$, we obtain polynomials corresponding to the representation $\rho_{u,3} \otimes \left(\frac{-3}{\cdot}\right)$ whose image is the simple group $\mathrm{SU}_3(\mathbb{F}_9) \simeq \mathrm{PSU}_3(\mathbb{F}_9)$, thus again solving the inverse Galois problem for the natural permutation representations of this group. These polynomials are also available on the author's web page [Mas].

Remark 5.3. As pointed out by an anonymous referee on a previous version of this article, the fact that the image of the representation is unitary is not a coincidence. Indeed, let $\ell \equiv -1 \bmod 4$ be a prime, identify $\mathbb{F}_{\ell^2}$ with $\mathbb{F}_\ell(i)$, $i^2 = -1$, and write H^r for $\mathrm{H}^r_{\text{ét}}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$ for brevity. The trace map [MilEC, 24.1.a] and the properness of S over $\mathbb{Q}$ provide us with a canonical isomorphism $\mathrm{H}^4 \simeq \mathbb{Z}/\ell\mathbb{Z}(-2)$, so in particular ϕ_S must act trivially on H^4. The cup product thus defines an alternating bilinear form

$$E : \mathrm{H}^2 \wedge \mathrm{H}^2 \longrightarrow \mathrm{H}^4 \simeq \mathbb{F}_\ell(-2)$$

satisfying

$$E(\phi_S u, \phi_S v) = E(u, v)$$

for all $u, v \in \mathrm{H}^2$, which may be extended into the bilinear form

$$\begin{array}{rccc} H : & \mathrm{H}^2 \times \mathrm{H}^2 & \longrightarrow & \mathbb{F}_\ell(i)(-2) \\ & (u, v) & \longmapsto & E(\phi_S u, v) + iE(u, v) \end{array}$$

which satisfies $\operatorname{Im} H = E$ and is Hermitian with respect to ϕ_S (exactly as a Riemann form corresponds to a Hermitian form). Therefore Galois acts on the Hermitian space H^2 by similarities of ratio given by the -2^{nd} power of the mod ℓ cyclotomic character, i.e.

$$H(\sigma u, \sigma v) = \chi_\ell(\sigma)^{-2} H(u, v)$$

for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $u, v \in \mathrm{H}^2$. In particular, for $\ell = 3$ the image of our Galois representation must be contained in the unitary group.

6 Computation of the image of Frob_p

Let L be a Galois number field, given as the splitting field of an irreducible polynomial $f(x) \in \mathbb{Q}[x]$. In [Dok13], the Dokchitsers show that if the action of $G = \mathrm{Gal}(L/\mathbb{Q})$ on the roots of $f(x)$ in L is known explicitly, then one can compute pairwise coprime resolvents $\Gamma_C(x) \in \mathbb{Q}[x]$ indexed by the conjugacy classes C of G, such that if the image of Frob_p in G lies in C, then the corresponding resolvent $\Gamma_C(x)$ vanishes at $x_p = \mathrm{Tr}_{\mathbb{F}_p}^{A_p}\left(a^p h(a)\right) \in \mathbb{F}_p$, where $A_p = \mathbb{F}_p[x]/f(x)$, a is the image of x in A_p, and $h(x) \in \mathbb{Z}[x]$ is a fixed parameter on which the $\Gamma_C(x)$ depend.

The point is that since the $\Gamma_C(x)$ are coprime, they remain coprime mod p for almost all p, so only one of them can vanish at x_p and we can tell in which class C the image of Frob_p lies. The finitely many p for which this is no longer true are usually quite small, and for these p be get not one but several C that may contain Frob_p. If the conjugacy class of Frob_p is really wanted for such a p, one should recompute the resolvents with another value of the parameter h.

Since the quotient $\mathrm{SU}_3(\mathbb{F}_9) \longrightarrow \mathrm{PSU}_3(\mathbb{F}_9)$ is actually an isomorphism, and as $\det \rho_{u,3} = \left(\frac{-3}{\cdot}\right)$ is known explicitly, for each prime p we can recover the image of Frob_p by $\rho_{u,3}$ from its image by the projective version of this representation. Namely, if the image of Frob_p by the projective representation is conjugate to $\overline{M} \in \mathrm{PSU}_3(\mathbb{F}_9)$, then $\rho_{u,3}(\mathrm{Frob}_p)$ is conjugate to $\left(\frac{-3}{p}\right)M$ in $\mathrm{U}_3(\mathbb{F}_9)$, where $M \in \mathrm{SU}_3(\mathbb{F}_9)$ is the image of $\overline{M}$ by the inverse of this isomorphism.

We thus apply the Dokchitsers' method to the case where $f(x)$ is the polynomial of degree 28 displayed in the previous section. This polynomial has Galois group $\mathrm{PSU}_3(\mathbb{F}_9)$, and its roots are indexed by the lines of $\mathbb{F}_9^3$ that are isotropic with respect to a certain hermitian form H. We can determine H from the fact that it is preserved by the action of Frob_{11}, and after a change of basis of $\mathbb{F}_9^3$ we can assume that H is the standard Hermitian form.

The group $\mathrm{PSU}_3(\mathbb{F}_9)$ has order 6048, which is small enough that [Magma] can effortlessly decompose it explicitly into conjugacy classes, which is all we need to compute the resolvents $\Gamma_C(x)$.

Thanks to these resolvents, we can now determine the image of Frob_p by $\rho_{u,3}$ for almost all p. Let us start by the primes between 5 and 67, for which the value of the Hecke eigenvalue $a_p \in \mathbb{Z}[i]$ is given in [GT94].

p	$\rho_{u,3}(\mathrm{Frob}_p)$	a_p from [GT94]
5	3 possibilities	$-4i-1$
7	$+\begin{bmatrix} 0 & i+1 & i-1 \\ 0 & i+1 & -i+1 \\ 1 & 0 & 0 \end{bmatrix}$	$4i+1$
11	$-\begin{bmatrix} 0 & i+1 & i-1 \\ 0 & i+1 & -i+1 \\ 1 & 0 & 0 \end{bmatrix}$	$-10i-7$
13	$+\begin{bmatrix} 0 & i+1 & i+1 \\ 0 & i-1 & -i+1 \\ 1 & 0 & 0 \end{bmatrix}$	$4i-1$
17	$-\begin{bmatrix} 1 & 0 & 0 \\ 0 & i-1 & i-1 \\ 0 & i+1 & -i-1 \end{bmatrix}$	7
19	$+\begin{bmatrix} 0 & i+1 & i-1 \\ 0 & i+1 & -i+1 \\ 1 & 0 & 0 \end{bmatrix}$	$-14i+1$
23	$-\begin{bmatrix} 0 & i+1 & i-1 \\ 0 & i+1 & -i+1 \\ 1 & 0 & 0 \end{bmatrix}$	$-4i+17$
29	$-\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$	$-12i-9$
31	3 possibilities	1
37	2 possibilities	$28i-25$
41	$-\begin{bmatrix} 1 & 0 & 0 \\ 0 & i-1 & i-1 \\ 0 & i+1 & -i-1 \end{bmatrix}$	-5
43	$+\begin{bmatrix} 1 & 0 & 0 \\ 0 & i-1 & i-1 \\ 0 & i+1 & -i-1 \end{bmatrix}$	$30i-7$
47	$-\begin{bmatrix} 0 & i+1 & -i-1 \\ 0 & -i+1 & -i+1 \\ 1 & 0 & 0 \end{bmatrix}$	$40i+17$
53	2 possibilities	$-20i+23$
59	$-\begin{bmatrix} 0 & 0 & -i \\ 0 & -i & 0 \\ 1 & 0 & 0 \end{bmatrix}$	$22i-39$
61	$+\begin{bmatrix} 0 & 0 & -i \\ 0 & -i & 0 \\ 1 & 0 & 0 \end{bmatrix}$	$20i+63$
67	$+\begin{bmatrix} 0 & i+1 & -i+1 \\ 0 & -i-1 & -i+1 \\ 1 & 0 & 0 \end{bmatrix}$	$-22i+65$

With our choice our h, the resolvents $\Gamma_C(x)$ do not remain coprime mod p for $p \in \{5, 31, 37, 53\}$, so for these p we cannot determine the image of Frob_p without re-computing the resolvents with another choice of $h(x)$. For the other p, we can compute the conjugacy class $C \subset \mathrm{PSU}_3(\mathbb{F}_9)$ containing Frob_p, and we display the image of Frob_p by $\rho_{u,3}$ as

$$\left(\frac{-3}{p}\right) M \in \mathrm{U}_3(\mathbb{F}_9),$$

where M is a fixed representative of its conjugacy class in $\mathrm{SU}_3(\mathbb{F}_9) \simeq \mathrm{PSU}_3(\mathbb{F}_9)$ that we have arbitrarily chosen because many of its coefficients were 0.

The fact that the trace agrees with the reduction mod 3 of the value of a_p given in [GT94] is convincing evidence that we have correctly computed $\rho_{u,3}$.

Next, we do the same thing for the first twenty primes above 10^{1000}. Of course, the $\Gamma_C(x)$ remain coprime mod p for such large p, so we find unambiguously the conjugacy class of $\rho_{u,3}(\mathrm{Frob}_p)$. By looking at the trace, we deduce the value of a_p mod 3. The results are displayed in the table below.

Remark 6.1. It takes about 100 seconds for [Pari/GP] to certify the primality of such a large prime, but only 4 seconds to compute the conjugacy class of $\rho_{u,3}(\mathrm{Frob}_p)$, almost all of which are spent computing $\mathrm{Tr}_{\mathbb{F}_p}^{A_p}\left(a^p h(a)\right) \in \mathbb{F}_p$.

The resolvents $\Gamma_C(x)$ are available on the author's web page [Mas].

p	$\rho_{u,3}(\mathrm{Frob}_p)$	$a_p \bmod 3\mathbb{Z}[i]$
$10^{1000}+453$	$+\begin{bmatrix} 1 & 0 & 0 \\ 0 & i-1 & i-1 \\ 0 & i+1 & -i-1 \end{bmatrix}$	-1
$10^{1000}+1357$	$-\begin{bmatrix} 0 & 0 & i \\ 0 & i & 0 \\ 1 & 0 & 0 \end{bmatrix}$	$-i$
$10^{1000}+2713$	$-\begin{bmatrix} 0 & 0 & -i \\ 0 & -i & 0 \\ 1 & 0 & 0 \end{bmatrix}$	i
$10^{1000}+4351$	$-\begin{bmatrix} 0 & i+1 & -i-1 \\ 0 & -i+1 & -i+1 \\ 1 & 0 & 0 \end{bmatrix}$	$i-1$
$10^{1000}+5733$	$+\begin{bmatrix} 0 & i+1 & -i+1 \\ 0 & -i-1 & -i+1 \\ 1 & 0 & 0 \end{bmatrix}$	$-i-1$
$10^{1000}+7383$	$+\begin{bmatrix} 0 & 0 & -i \\ 0 & -i & 0 \\ 1 & 0 & 0 \end{bmatrix}$	$-i$
$10^{1000}+10401$	$+\begin{bmatrix} 1 & 0 & 0 \\ 0 & i & 0 \\ 0 & 0 & -i \end{bmatrix}$	1
$10^{1000}+11979$	$+\begin{bmatrix} 0 & i+1 & i+1 \\ 0 & i-1 & -i+1 \\ 1 & 0 & 0 \end{bmatrix}$	$i-1$
$10^{1000}+17557$	$-\begin{bmatrix} 1 & 0 & 0 \\ 0 & i-1 & i-1 \\ 0 & i+1 & -i-1 \end{bmatrix}$	1
$10^{1000}+21567$	$+\begin{bmatrix} 1 & 0 & 0 \\ 0 & i-1 & i-1 \\ 0 & i+1 & -i-1 \end{bmatrix}$	-1
$10^{1000}+22273$	$-\begin{bmatrix} 0 & i+1 & -i-1 \\ 0 & -i+1 & -i+1 \\ 1 & 0 & 0 \end{bmatrix}$	$i-1$
$10^{1000}+24493$	$-\begin{bmatrix} 0 & i+1 & -i-1 \\ 0 & -i+1 & -i+1 \\ 1 & 0 & 0 \end{bmatrix}$	$i-1$
$10^{1000}+25947$	$+\begin{bmatrix} 0 & i+1 & i-1 \\ 0 & i+1 & -i+1 \\ 1 & 0 & 0 \end{bmatrix}$	$i+1$
$10^{1000}+27057$	$+\begin{bmatrix} 0 & i+1 & -i+1 \\ 0 & -i-1 & -i+1 \\ 1 & 0 & 0 \end{bmatrix}$	$-i-1$
$10^{1000}+29737$	$-\begin{bmatrix} 0 & i+1 & -i+1 \\ 0 & -i-1 & -i+1 \\ 1 & 0 & 0 \end{bmatrix}$	$i+1$
$10^{1000}+41599$	$-\begin{bmatrix} 1 & 0 & 0 \\ 0 & i & 0 \\ 0 & 0 & -i \end{bmatrix}$	-1
$10^{1000}+43789$	$-\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$	0
$10^{1000}+46227$	$+\begin{bmatrix} 0 & i+1 & -i-1 \\ 0 & -i+1 & -i+1 \\ 1 & 0 & 0 \end{bmatrix}$	$-i+1$
$10^{1000}+46339$	$-\begin{bmatrix} 0 & 0 & i \\ 0 & i & 0 \\ 1 & 0 & 0 \end{bmatrix}$	$-i$
$10^{1000}+52423$	$-\begin{bmatrix} 0 & i+1 & i-1 \\ 0 & i+1 & -i+1 \\ 1 & 0 & 0 \end{bmatrix}$	$-i-1$

References

[BHPvV] Barth, Wolf P.; Hulek, Klaus; Peters, Chris A. M.; Van de Ven, Antonius, **Compact complex surfaces**. Second edition. Ergebnisse der Mathematik und ihrer Grenzgebiete, Volume 4. Springer-Verlag, Berlin, 2004. ISBN: 3-540-00832-2.

[BO74] Bloch, Spencer; Ogus, Arthur, **Gersten's conjecture and the homology of schemes**. Ann. Sci. École Norm. Sup. (4) 7 (1974), 181–201.

[CE11] **Computational aspects of modular forms and Galois representations**. Edited by Jean-Marc Couveignes and Bas Edixhoven, with contributions by Johan Bosman, Jean-Marc Couveignes, Bas Edixhoven, Robin de Jong, and Franz Merkl. Ann. of Math. Stud., 176, Princeton Univ. Press, Princeton, NJ, 2011.

[Dok13] Dokchitser, Tim and Vladimir, **Identifying Frobenius elements in Galois groups**. Algebra & Number Theory, Volume 7, Number 6 (2013), 1325–1352.

[GT94] van Geemen, Bert; Top, Jaap, **A non-selfdual automorphic representation of GL_3 and a Galois representation**. Invent. Math. 117 (1994), no. 3, 391–401.

[HLTT16] Harris, Michael; Lan, Kai-Wen; Taylor, Richard; Thorne, Jack **On the rigid cohomology of certain Shimura varieties**. Res. Math. Sci. 3 (2016), Paper No. 37, 308 pp.

[IKM18] Ito, Tetsushi; Koshikawa, Teruhisa; Mieda, Yoichi, **Galois representations associated with a non-selfdual automorphic representation of GL(3)**. arXiv preprint 1811.11544.

[Jan90] Jannsen, Uwe, **Mixed motives and algebraic K-theory**. Lecture Notes in Mathematics, 1400. Springer-Verlag, Berlin, 1990. xiv+246 pp. ISBN: 3-540-52260-3.

[Jin17] Jin, Jinbi, **Explicit computation of the first étale cohomology on curves**. arXiv preprint 1707.08825, to appear in the Journal de Théorie des Nombres de Bordeaux.

[LMFDB] The LMFDB Collaboration, **The L-functions and Modular Forms Database**. `http://www.lmfdb.org`.

[Magma] Bosma, Wieb; Cannon, John; Playoust, Catherine, **The Magma algebra system. I. The user language** J. Symbolic Comput., 24 (1997), 235–265.

[Mas] Mascot, Nicolas, Personal web page. `https://staff.aub.edu.lb/~nm116/`.

[Mas18a] Mascot, Nicolas, **Certification of modular Galois representations**. Mathematics of Computation 87 (2018), 381–423.

[Mas18b] Mascot, Nicolas, **Companion forms and explicit computation of PGL_2 number fields with very little ramification**. Journal of Algebra, Volume 509, 1 September 2018, 476–506.

[Mas18c] Mascot, Nicolas, **Hensel-lifting torsion points on Jacobians and Galois representations**. arXiv preprint 1808.03939.

[MilEC] Milne, James S., **Lectures on Etale cohomology**, version 2.21. `https://www.jmilne.org/math/`.

[MO15] Madore, David A.; Orgogozo, Fabrice, **Calculabilité de la cohomologie étale modulo ℓ**. Algebra Number Theory 9 (2015), no. 7, 1647–1739.

[BLR90] Bosch, Siegfried; Lütkebohmert, Werner; Raynaud, Michel, **Néron models**. Ergebnisse der Mathematik und ihrer Grenzgebiete (3). Springer-Verlag, Berlin, 1990. x+325 pp. ISBN: 3-540-50587-3.

[Pari/GP] The PARI Group, PARI/GP development version `2.12.0`, Bordeaux, 2018. `http://pari.math.u-bordeaux.fr/`.

[PTvL15] Poonen, Bjorn; Testa, Damiano; van Luijk, Ronald, **Computing Néron-Severi groups and cycle class groups**. Compos. Math. 151 (2015), no. 4, 713–734.

[Sch15] Scholze, Peter, **On torsion in the cohomology of locally symmetric varieties**. Ann. of Math. (2) 182 (2015), no. 3, 945–1066.

[SGA4$\frac{1}{2}$] Deligne, Pierre, **Cohomologie étale**. Séminaire de géométrie algébrique du Bois-Marie (SGA $4\frac{1}{2}$). Lecture Notes in Mathematics, 569. Springer-Verlag, Berlin, 1977. iv+312 pp. ISBN: 3-540-08066-X; 0-387-08066-X.