MATHEMATICS OF COMPUTATION
Volume 87, Number 309, January 2018, Pages 381–423
http://dx.doi.org/10.1090/mcom/3215
Article electronically published on June 21, 2017

CERTIFICATION OF MODULAR GALOIS REPRESENTATIONS

NICOLAS MASCOT

Abstract. We show how the output of the algorithm to compute modular Galois representations previously described by the author [Rend. Circ. Mat. Palermo (2) 62 (2013), no. 3, 451–476] can be certified. We have used this process to compute certified tables of such Galois representations obtained thanks to an improved version of this algorithm, including representations modulo primes up to 31 and representations attached to a newform with nonrational (but of course algebraic) coefficients, which had never been done before. These computations take place in the Jacobian of modular curves of genus up to 26.

We begin with a short summary about Galois representations attached to modular forms and how we used these in [Mas13] to compute Fourier coefficients of modular forms in section 1. This computation becomes much easier if the polynomial in $\mathbb{Q}[x]$ defining the representation and computed by the algorithm along the way is reduced, and we show new ideas to do so efficiently in section 2. We then show in section 3 how the outputs of this computation can be formally certified. Finally, we comment on the use of this certification method on our own data in the last section 4.

1. Introduction

Let $f = q + \sum_{n=2}^{+\infty} a_n q^n \in S_k\big(\Gamma_1(N), \varepsilon\big)$ be a classical newform of weight $k \in \mathbb{N}_{\geqslant 2}$, level $N \in \mathbb{N}_{\geqslant 1}$ and nebentypus ε. Jean-Pierre Serre conjectured and Pierre Deligne proved in [Del71] that for every finite prime $\mathfrak{l}$ of the number field $K_f = \mathbb{Q}(a_n,\ n \geqslant 2)$ spanned by the coefficients a_n of the q-expansion of f at infinity, there exists a continuous Galois representation

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_{K_f,\mathfrak{l}})$$

which is unramified outside ℓN and such that the image of any Frobenius element at $p \nmid \ell N$ has characteristic polynomial $x^2 - a_p x + \varepsilon(p)p^{k-1} \in \mathbb{Z}_{K_f,\mathfrak{l}}[x]$, where $\mathbb{Z}_{K_f,\mathfrak{l}}$ denotes the $\mathfrak{l}$-adic completion of the ring of integers $\mathbb{Z}_{K_f}$ of K_f, and ℓ is the rational prime lying below $\mathfrak{l}$.

Received by the editor October 28, 2015 and, in revised form, December 9, 2015 and April 6, 2016.

2010 *Mathematics Subject Classification.* Primary 11Y70, 11S20, 11F80, 11F11, 11Y40, 20B40, 20J06.

This research was supported by the French ANR-12-BS01-0010-01 through the project PEACE, by the DGA maîtrise de l'information, by ERC Starting Grant ANTICS 278537, and by the EPSRC Programme Grant EP/K034383/1 "LMF: L-Functions and Modular Forms".

Let $\mathbb{F}_\mathfrak{l}$ be the residue field of $\mathfrak{l}$. By reducing the above $\mathfrak{l}$-adic Galois representation modulo $\mathfrak{l}$ and semisimplifying, we get a modulo $\mathfrak{l}$ Galois representation

$$\rho_{f,\mathfrak{l}}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\mathfrak{l}),$$

which is unramified outside ℓN and such that the image of any Frobenius element at $p \nmid \ell N$ has characteristic polynomial $x^2 - a_p x + \varepsilon(p)p^{k-1} \in \mathbb{F}_\mathfrak{l}[x]$. In particular, the trace of this image is a_p mod $\mathfrak{l}$.

In [Mas13], we described an algorithm based on ideas from the book [CE11] edited by Jean-Marc Couveignes and Bas Edixhoven to compute such modulo $\mathfrak{l}$ Galois representations, provided that the image of the Galois representation contains $\mathrm{SL}_2(\mathbb{F}_\mathfrak{l})$ and that $k < \ell$. This gives a way to quickly compute the coefficients a_p modulo $\mathfrak{l}$ for huge primes p. We have used this algorithm to compute representations attached to forms of level 1 for ℓ up to 31.

In what follows, we will assume that the inertial degree of $\mathfrak{l}$ is 1, so that $\mathbb{F}_\mathfrak{l} = \mathbb{F}_\ell$. Indeed, although there is no theoretical obstacle to allowing primes of higher degree, we will have to deal explicitly with objects such as polynomials whose roots are indexed by ${\mathbb{F}_\ell}^2 \setminus \{(0,0)\}$ and whose Galois group is $\mathrm{GL}_2(\mathbb{F}_\ell)$, and this already requires considerable work when $\mathbb{F}_\mathfrak{l} = \mathbb{F}_\ell$.

The condition that the image of the Galois representation contain $\mathrm{SL}_2(\mathbb{F}_\mathfrak{l})$ is then generically satisfied. Indeed, by [Rib85, Theorem 2.1] and [Swi72, Lemma 2], for any non-CM newform f (and in particular for any newform f of level 1), the image of the representation $\rho_{f,\mathfrak{l}}$ contains $\mathrm{SL}_2(\mathbb{F}_\ell)$ for almost every $\mathfrak{l}$ of degree 1. The finitely many $\mathfrak{l}$ of degree 1 for which $\mathrm{SL}_2(\mathbb{F}_\ell) \not\subset \mathrm{Im}\,\rho_{f,\mathfrak{l}}$ are called *exceptional primes* of degree 1 for f, and we exclude them. They were explicitly determined by Sir Peter Swinnerton-Dyer in [Swi72] for the known[1] newforms f of level 1 whose coefficients a_n are rational. In our case, this means we exclude $\mathfrak{l} = 23$ for $f = \Delta$ and $\mathfrak{l} = 31$ for $f = E_4\Delta$.

Our algorithm relies on the fact that if $k < \ell$, then the Galois representation $\rho_{f,\mathfrak{l}}$ is afforded with multiplicity 1 by a subspace $V_{f,\mathfrak{l}}$ of the ℓ-torsion of the Jacobian $J_1(\ell N)$ of the modular curve $X_1(\ell N)$ under the natural $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action; cf. [Gro90, Proposition 9.3.2] and [Mas13, Section 1].

The algorithm first computes the number field $L = \overline{\mathbb{Q}}^{\mathrm{Ker}\,\rho_{f,\mathfrak{l}}}$ cut out by the Galois representation, by evaluating a well-chosen function $\alpha \in \mathbb{Q}\big(J_1(\ell N)\big)$ in the nonzero points of $V_{f,\mathfrak{l}}$ and forming the polynomial

$$F(x) = \prod_{\substack{v \in V_{f,\mathfrak{l}} \\ v \neq 0}} \big(x - \alpha(v)\big) \in \mathbb{Q}[x]$$

of degree $\ell^2 - 1$ whose decomposition field is L. The algorithm then uses a method from T. and V. Dokchitser (cf [Dok10]) to compute the image of the Frobenius element at p given a rational prime $p \nmid \ell N$. This method involves the computation of a family of resolvents

$$\Gamma_C(x) = \prod_{\sigma \in C} \left(x - \sum_{\substack{v \in V_{f,\mathfrak{l}} \\ v \neq 0}} h\big(\alpha(v)\big)\, \alpha(\sigma \cdot v) \right) \in \mathbb{Q}[x]$$

[1] According to Maeda's conjecture (cf [FW02]), there are only 6 such forms, namely Δ, $E_4\Delta$, $E_6\Delta$, $E_8\Delta$, $E_{10}\Delta$ and $E_{14}\Delta$, of respective weights 12, 16, 18, 20, 22 and 26.

indexed by the conjugacy classes C of $\mathrm{GL}_2(\mathbb{F}_\ell)$, where $h(x) \in \mathbb{Z}[x]$ is some fixed polynomial. These resolvents, which we will refer to as the Dokchitsers' resolvents, can then be used to determine which class the Frobenius element at p lies in for almost all $p \in \mathbb{N}$.

Remark 1. Actually, in order to obtain certified results, we will see that we should certify the polynomial $F(x)$ in the sense of section 3 before computing the Dokchitsers' resolvents.

Unfortunately, the output of the algorithm, although correct beyond reasonable doubt (cf. [Mas13], end of section 1), is not certified since it relies on the identification of floating point numbers as rational numbers. The purpose of this article is to show how these computations can be formally certified subsequently. As a side effect, we also obtain much tidier outputs.

A word on notation. Throughout this article, we will be dealing with two versions of most of the objects in play, namely the actual value of this object, and the version computed by the algorithm described above. For instance, the function $\alpha \in \mathbb{Q}\big(J_1(\ell N)\big)$ being fixed, the polynomial

$$F(x) = \prod_{\substack{v \in V_{f,\mathfrak{l}} \\ v \neq 0}} \big(x - \alpha(v)\big) \in \mathbb{Q}[x]$$

is a well-defined object attached to α, f and $\mathfrak{l}$, but what the algorithm outputs is an approximate version of this polynomial over $\mathbb{C}$, whose coefficients are then nonrigorously identified as rational numbers. Following the reviewer's comments on an older version of this article, we will denote the "true" value of $F(x)$ with an aureole, $\mathring{F}(x)$, so as to stress its "heavenly unattainable nature" (as the reviewer put it), and we will reserve the notation $F(x)$ to the polynomial "guessed" by the algorithm, and similarly for the other objects at play. We will follow this convention from now on, and we hope that doing so will reduce the confusion between the two versions of each object, and make our certification process clearer.

2. Reducing the polynomials

Unfortunately, the coefficients of the polynomial $F(x)$ produced by the algorithm described in [Mas13] tend to have larger and larger height as ℓ grows. More precisely, in practice this polynomial is of the form

$$F(x) = x^{\deg F} + \frac{1}{d} \sum_{i < \deg F} c_i x^i,$$

where d is an (unfortunately large) positive integer and the c_i are integers whose gcd with d is several orders of magnitude smaller than d; in other words, apart from the leading one, these coefficients roughly all have the same denominator, with a few "accidental" simplifications here and there. The following table, which shows the genus $g = \frac{(\ell-5)(\ell-7)}{24}$ of the modular curves $X_1(\ell)$ and the rough number $h \approx \log_{10} d$ of decimal digits in the denominator d of the polynomials $F(x)$ associated to newforms of level $N = 1$ that we computed using the algorithm described

in [Mas13], seems to indicate the heuristic $h \approx g^{2.5}$:

ℓ	g	h
11	1	0
13	2	5
17	5	50
19	7	150
23	12	500
29	22	1800
31	26	2500

While this is rather harmless for $\ell \leqslant 17$, it makes the Dokchitsers' method intractable as soon as $\ell \geqslant 29$. It is thus necessary to reduce this polynomial, that is to say, to compute another polynomial whose splitting field is isomorphic to the splitting field of $F(x)$ but whose coefficients are much nicer. An algorithm to perform this task based on LLL lattice reduction is described in [Coh93, Section 4.4.2] and implemented in [Pari/GP] under the name `polred`. Its complexity is polynomial in the degree and the height of the coefficients, provided that the factorisation of the discriminant of the corresponding field is known, which is the case for us. However, the polynomial $F(x)$ has degree $\ell^2 - 1$ and tends to have really large coefficients, and this makes `polred` choke on it, even for small values of ℓ. Indeed, the fact that `polred` is based on LLL reduction means that its execution time is especially sensitive to the degree of the polynomial.

On the other hand, it would be amenable to apply the `polred` algorithm to the polynomial

$$\mathring{F}^{\mathrm{proj}}(x) = \prod_{W \in \mathbb{P}(V_{f,\mathfrak{l}})} \left(x - \sum_{\substack{w \in W \\ w \neq 0}} \alpha(w) \right) \in \mathbb{Q}[x]$$

whose splitting field is[2] the number field $\mathring{L}^{\mathrm{proj}}$ cut out by the *projective* Galois representation

$$\mathring{\rho}^{\mathrm{proj}}_{f,\mathfrak{l}} \colon \ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\mathring{\rho}_{f,\mathfrak{l}}} \mathrm{GL}_2(\mathbb{F}_\ell) \longrightarrow\!\!\!\!\!\rightarrow \mathrm{PGL}_2(\mathbb{F}_\ell)$$

since the degree of this polynomial is only $\ell + 1$. Unfortunately, this projective version of the representation does not contain enough information to recover[3] the values of $a_p \bmod \mathfrak{l}$.

However, we noted in [Mas13, Section 3.7.2] that if $S \subset \mathbb{F}_\ell^*$ denotes the largest subgroup of $\mathbb{F}_\ell^*$ such that $S \not\ni -1$, then the knowledge of the quotient representation

$$\mathring{\rho}^{S}_{f,\mathfrak{l}} \colon \ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\mathring{\rho}_{f,\mathfrak{l}}} \mathrm{GL}_2(\mathbb{F}_\ell) \longrightarrow\!\!\!\!\!\rightarrow \mathrm{GL}_2(\mathbb{F}_\ell)/S \ ,$$

[2]To be precise, it is clear that the splitting field of $\mathring{F}^{\mathrm{proj}}(x)$ is contained in the number field $\mathring{L}^{\mathrm{proj}}$ cut out by the projective representation. Very often, this containment is an equality and so $\mathring{F}^{\mathrm{proj}}(x)$ is irreducible, but it may sometimes happen that this containment is proper, in which case $\mathring{F}^{\mathrm{proj}}(x)$ becomes reducible over $\mathbb{Q}$. We can work around this pathological behaviour by replacing the summation over W in the definition of $\mathring{F}^{\mathrm{proj}}(x)$ by another symmetric combination (e.g. a product), or by applying a Tschirnhausen transform. For notational convenience, we will henceforth assume that no such problem is encountered; should this not be the case, the necessary modifications are completely straightforward.

[3]One could at most recover these values with a sign ambiguity, as in [CE11].

combined with the fact that the image in $\mathrm{GL}_2(\mathbb{F}_\ell)$ of a Frobenius element at p has determinant $p^{k-1}\varepsilon(p) \bmod \mathfrak{l}$, is enough to recover $\mathring{\rho}_{f,\mathfrak{l}}$ and hence the values of $a_p \bmod \mathfrak{l}$. It is therefore enough for our purpose to compute this quotient representation, first by forming the polynomial

$$\mathring{F}^S(x) = \prod_{\substack{Sv \in V_{f,\mathfrak{l}}/S \\ v \neq 0}} \left(x - \sum_{s \in S} \alpha(sv) \right) \in \mathbb{Q}[x],$$

whose splitting field is the number field $\mathring{L}^S$ cut out by $\mathring{\rho}^S_{f,\mathfrak{l}}$, and then by applying the Dokchitsers' method on it in order to compute the images of the Frobenius elements by $\mathring{\rho}^S_{f,\mathfrak{l}}$; cf. [Mas13, Section 3.7.2].

Note that since we assumed that f and $\mathfrak{l}$ are such that $\mathring{\rho}_{f,\mathfrak{l}}$ is not exceptional,[4] the quotient representation $\mathring{\rho}^S_{f,\mathfrak{l}}$ is surjective. Indeed, since f is a form of level $N = 1$ and of even weight, the determinant of $\rho_{f,\mathfrak{l}}$ is an odd power of the mod ℓ cyclotomic character. In particular, the polynomial $\mathring{F}^S(x)$ is irreducible over $\mathbb{Q}$.

Also note that the complex roots of $\mathring{F}(x)$ are approximately known as an output of the algorithm [Mas13], and so is their indexation by $V_{f,\mathfrak{l}} - \{0\}$. We thus have an indexation of the roots of $F(x)$ by $V_{f,\mathfrak{l}} - \{0\}$, and so we can compute an approximation $F^S(x) \in \mathbb{Q}[x]$ of $\mathring{F}^S(x)$ by grouping the roots, expanding over $\mathbb{C}$, and guessing the coefficients by continued fractions just as for $F(x)$.

In practice, the coefficients of $F^S(x)$ have roughly the same denominator as the ones of $F(x)$, so we are not improving anything on this side, but of course the degree of $F^S(x)$ can be much smaller, so we may try to `polred` it. Let $\ell - 1 = 2^r s$ with $s \in \mathbb{N}$ odd. Since we have $|S| = s$, the degree of F^S is $2^r(\ell+1)$, so `polred`ing is amenable in the cases $\ell = 19$ or 23, but the cases $\ell = 29$ or 31 remain impractical.

For these remaining cases, Bill Allombert suggested to the author that one can still reduce $F^S(x)$ in several steps, as we now explain. Since $\mathbb{F}_\ell^*$ is cyclic, we have a filtration

$$\mathbb{F}_\ell^* = S_0 \underset{2}{\supset} S_1 \underset{2}{\supset} \cdots \underset{2}{\supset} S_r = S$$

with $[S_i : S_{i+1}] = 2$ for all i, namely

$$S_i = \{x^{2^i}, x \in \mathbb{F}_\ell^*\}.$$

For each $i \leqslant r$, let us define

$$\mathring{F}_i(x) = \prod_{\substack{S_i v \in V_{f,\mathfrak{l}}/S_i \\ v \neq 0}} \left(x - \sum_{s \in S_i} \alpha(sv) \right) \in \mathbb{Q}[x],$$

let $F_i(x) \in \mathbb{Q}[x]$ be guesses for $\mathring{F}_i(x)$ obtained as for $F^S(x)$ above, let

$$\mathring{K}_i = \mathbb{Q}[x]/\mathring{F}_i(x), \qquad K_i = \mathbb{Q}[x]/F_i(x),$$

and let $\mathring{L}_i$ (resp. L_i) be the normal closure of $\mathring{K}_i$ (resp. K_i), so that $\mathring{L}_i$ is the number field cut out by the quotient representation

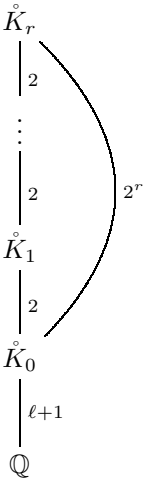
$$\mathring{\rho}^{S_i}_{f,\mathfrak{l}} \colon \ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\mathring{\rho}_{f,\mathfrak{l}}} \mathrm{GL}_2(\mathbb{F}_\ell) \twoheadrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)/S_i \ .$$

[4] In the sense that its image contains $\mathrm{SL}_2(\mathbb{F}_\ell)$.

In particular, we have $\mathring{\rho}_{f,\mathfrak{l}}^{S_0} = \mathring{\rho}_{f,\mathfrak{l}}^{\mathrm{proj}}$, $\mathring{L}_0 = \mathring{L}^{\mathrm{proj}}$, and we are looking for a nice model of K_r.

Note that again because f is of level $N = 1$, and is not exceptional mod $\mathfrak{l}$, the polynomials $\mathring{F}_i(x)$ are irreducible over $\mathbb{Q}$, and so $\mathring{K}_i$ is indeed a field. We assume that the $F_i(x)$ are also irreducible.

By construction, the degree of $\mathring{K}_i$ over $\mathbb{Q}$ is $\#\big((V_{f,\mathfrak{l}} - \{0\})/S_i\big) = 2^i(\ell+1)$, so the fields $\mathring{K}_i$ fit in an extension tower



and we are going to `polred` the polynomials $F_i(x)$ along this tower recursively from the bottom up.

First, we apply directly the `polred` algorithm to $F_0(x) = F^{\mathrm{proj}}(x)$. Since the degree of this polynomial is only $\ell + 1$, this is amenable, as mentioned above, and yields a monic reduced polynomial in $\mathbb{Z}[x]$.

Then, assuming we have managed to reduce $F_i(x)$, we have a nice model for $K_i = \mathbb{Q}[x]/F_i(x)$, and so we can factor $F_{i+1}(x)$ over K_i. Since the extension $K_{i+1} = \mathbb{Q}[x]/F_{i+1}(x)$ should be quadratic over K_i, there must be at least one factor of degree 2. Let $G_{i+1}(x)$ be one of those, and let $\Delta_i \in K_i$ be its discriminant, so that we have

$$K_{i+1} \simeq K_i[x]/G_{i+1}(x) \simeq K_i\big(\sqrt{\Delta_i}\big).$$

In order to complete the recursion, all we have to do is to strip Δ_i from the largest square factor we can find, say $\Delta_i = A_i^2\delta_i$ with $A_i, \delta_i \in K_i$ and δ_i as small as possible. Indeed we then have $K_{i+1} = K_i\big(\sqrt{\delta_i}\big)$, and actually even $K_{i+1} = \mathbb{Q}\big(\sqrt{\delta_i}\big)$ unless we are very unlucky,[5] so that if we denote by $\chi_i(x) \in \mathbb{Q}[x]$ the minimal polynomial of δ_i, then we have

$$K_{i+1} \simeq \mathbb{Q}[x]/\chi_i(x^2),$$

so that $\chi_i(x^2)$ is a reduced version of $F_{i+1}(x)$. If its degree and coefficients are not too big, we can even apply the `polred` algorithm to this polynomial in order to further reduce it, which is what we do in practice.

[5]In practice, the case $K_{i+1} \supsetneq \mathbb{Q}\big(\sqrt{\delta_i}\big)$ has never happened to us. Should it happen, it can be corrected by multiplying δ_i by the square of an (hopefully small) element in K_i.

In order to write $\Delta_i = A_i^2\delta_i$, we would like to factor Δ_i in K_i, but even if K_i is principal, this is not amenable whatsoever because Δ_i is huge. We can, however, consider the ideal generated by Δ_i in K_i, and remove its ℓN-part. The fractional ideal $\mathfrak{B}_i$ we obtain must then be a perfect square, since K_{i+1} is unramified outside ℓN (since L is), and the very efficient `idealsqrt` script from [BS14] can explicitly factor it into $\mathfrak{B}_i = \mathfrak{A}_i^2$. If A_i denotes an element in $\mathfrak{A}_i$ close to being a generator of $\mathfrak{A}_i$ (an actual generator, if amenable, would be even better), then $\delta_i := \Delta_i/A_i^2$ is small.

We have thus managed to reduce our polynomials $F_i(x)$. In what follows, we will use the notation $F_i(x)$ to refer to the reduced versions, which are monic and lie in $\mathbb{Z}[x]$. They were each obtained from the nonreduced version by an explicit change of variable, and we can apply the same changes of variables to the "true" polynomials $\mathring{F}_i(x)$, thus yielding new polynomials that we will denote by $\mathring{F}_i(x)$ from now on.

3. Certification of the computations

The output of the algorithm relies on the identification as rational numbers of the coefficients of the polynomials $F_i(x)$ given in approximate form as floating-point numbers, by using continued fractions. In order to certify these results, it is thus necessary to make sure the we have correctly identified not only that the number fields cut out by the representation (i.e., that $K_i = \mathring{K}_i$), but also the Galois action on the roots of the $F_i(x)$, otherwise we would be doing nonsense with the Dokchitsers' resolvents $\Gamma_C(x)$.

For this, a first possibility consists in proving bounds on the height of the rational numbers that the algorithm will have to identify (e.g., the coefficients of $\mathring{F}(x)$), and then to certify that the continued fraction identification process is correct, for instance by running the computation with high enough precision in $\mathbb{C}$ and controlling the round-off errors all along. Although it is indeed possible in theory to bound the height of these rational numbers by using Arakelov theory (cf. [CE11, Theorem 11.7.6]), this approach gives unrealistic titanic bounds and thus seems ominously tedious, especially as it requires controlling the round-off error in the linear algebra steps of K. Khuri-Makdisi's algorithms to compute in the modular Jacobian (cf. [Mas13, Section 3.3]). We have therefore not attempted to follow it.

Instead, we deemed it much better to first run the computations in order to obtain unproven results, and to prove these results afterwards. We explain in this section how to do so.

3.1. **Sanity checks.** Before attempting to prove the results, it is comforting to perform a few easy checks so as to ensure that they seem correct beyond reasonable doubt (cf. the end of section 1 in [Mas13]). Namely,

- Since we are working with a form of level $N = 1$, the number field $\mathring{L}$ cut out by the Galois representation $\mathring{\rho}_{f,\mathfrak{l}}$ is ramified only at ℓ. Therefore, we can check that the discriminant of the polynomial $F(x) \in \mathbb{Q}[x]$ is of the form
$$\pm\ell^n M^2$$
for some $M \in \mathbb{Q}^*$. Even better, we can compute the maximal order of the field $K = \mathbb{Q}[x]/F(x)$ whose Galois closure is L and check that its

discriminant is, up to sign, a power of ℓ. Since a number field ramifies at the same primes as its Galois closure, this proves that the decomposition field L of $F(x)$ is ramified only at ℓ, as expected. If the coefficients of $F(x)$ are too horrible for that, we can apply this check on $F_r(x)$ instead.

- Since Galois representations attached to modular forms are odd, the image of complex conjugation by these representations is an involutory matrix in $\mathrm{GL}_2(\mathbb{F}_\mathfrak{l})$ of determinant -1, hence similar to $\left[\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right]$ if $\ell \geqslant 2$. This means that the polynomial $F(x)$ of degree ℓ^2-1 computed by the algorithm should have exactly $\ell-1$ roots in $\mathbb{R}$, which can be checked numerically, and that the sign of its discriminant should be $(-1)^{\ell(\ell-1)/2}$, which can be checked exactly.
- The fact that the resolvents $\Gamma_C(x)$ computed by the Dokchitsers' method and used to identify the image of Frobenius elements seem to have integer (and not just complex) coefficients hints that $\mathrm{Gal}(L/\mathbb{Q})$ is indeed isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, so that the number field L is indeed a number field cut out by a Galois representation, and that the Galois action on $V_{f,\mathfrak{l}} \subset J_1(\ell)[\ell]$ is linear. Again, we can replace $F(x)$ with $F_r(x)$ and $\mathrm{GL}_2(\mathbb{F}_\ell)$ with $\mathrm{GL}_2(\mathbb{F}_\ell)/S_r$ to ease computation.
- The fact that the approximations $F_i(x)$ of the polynomials $\mathring{F}_i(x)$ computed by regrouping the roots of $F(x)$ along their S-orbits for the various subgroups $S \subseteq \mathbb{F}_\ell^*$ considered during the polynomial reduction process (cf. section 2) seem to have rational coefficients with common denominator dividing the one of $F(x)$ also hints that the coefficients of these polynomials have been correctly identified as rational numbers, that $\mathrm{Gal}(L/\mathbb{Q})$ is indeed isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, and that the Galois action on the roots of $F(x)$ is the expected one.
- Finally, we can check that the values $a_p \bmod \mathfrak{l}$ obtained by the algorithm for a few small primes p are correct, by comparing them with the ones computed by "classical" methods such as based on modular symbol-based ones.

We will now present a method to formally prove rigorously our computations, while keeping the amount of required extra computations to a minimum.

3.2. **A certification algorithm.** We keep the notation of section 2: we fix a prime $\ell \geqslant 5$, and we let $r \in \mathbb{N}$ be such that $\ell - 1 = 2^r m$ for some odd $m \in \mathbb{N}$, so that we have the filtration

$$\mathbb{F}_\ell^* = S_0 \underset{2}{\supset} S_1 \underset{2}{\supset} \cdots \underset{2}{\supset} S_r = S$$

with $\#S_r$ odd and $[S_i : S_{i+1}] = 2$ for all i. Let $V = {\mathbb{F}_\ell}^2 - \{0\}$, the vector plane minus the origin, on which $\mathrm{GL}_2(\mathbb{F}_\ell)$ acts transitively, and let $V_i = V/S_i$, so that we have a natural transitive action of $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ on V_i. We denote by $\pi_i \colon V_{i+1} \twoheadrightarrow V_i$ the natural projection, and we note for future reference that each element of $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ has a well-defined trace in $\mathbb{F}_\ell/S_i$, as well as a well-defined determinant in $\mathbb{F}_\ell^*/S_i^2$, where

$$S_i^2 = \{s^2, s \in S_i\} = \begin{cases} S_{i+1}, & \text{if } i < r, \\ S_i, & \text{if } i = r. \end{cases}$$

For each $0 \leqslant i \leqslant r$, we have constructed a monic, irreducible polynomial $F_i(x) \in \mathbb{Z}[x]$ of degree $2^i(\ell+1)$. Let K_i be the root field of $F_i(x)$, let L_i be its Galois closure. We have that K_{i+1} is a quadratic extension of K_i, generated by the square root of some explicitly known integral primitive element δ_i of K_i, as this is a by-product of the reduction process presented in section 2.

For each i, let $Z_i \subset \mathbb{C}$ denote the set of complex roots of $F_i(x)$. As noted in section 2, we have an indexation of Z_i by V_i, which we denote by $\theta_i \colon Z_i \xrightarrow{\sim} V_i$. Via these indexations, the Galois action on the Z_i should be "linear", but we do not know that yet.

Moreover, by construction of the $F_i(x)$, for each root $z \in Z_{i+1}$ there exists another root $z' \in Z_{i+1}$ such that $z+z'$ is extremely close to a root of $F_i(x)$. We can check numerically that each root of $F_i(x)$ is the sum of two roots of $F_{i+1}(x)$ in a unique way, whence 2-to-1 projections map $\varpi_i \colon Z_{i+1} \twoheadrightarrow Z_i$ such that

$$z \approx \sum_{\substack{z' \in Z_{i+1} \\ \varpi_i(z')=z}} z'$$

for all $z \in Z_i$.

We can check that these approximate identities are in fact exact, i.e.,

$$z = \sum_{\substack{z' \in Z_{i+1} \\ \varpi_i(z')=z}} z', \tag{T}$$

by computing rigorously[6] for each i the polynomial

$$\prod_{I \in \binom{Z_i}{2}} \left(x - \sum_{z \in I} z \right) \in \mathbb{Z}[x],$$

where $\binom{Z_i}{2}$ denotes the set of 2-element subsets of Z_i, and by checking that $F_i(x)$ divides this polynomial and that the complex roots match as expected. We can then also check numerically that the diagram

$$\begin{array}{ccc} Z_{i+1} & \xrightarrow[\theta_{i+1}]{\sim} & V_{i+1} \\ {\scriptstyle \varpi_i}\downarrow & & \downarrow{\scriptstyle \pi_i} \\ Z_i & \xrightarrow[\theta_i]{\sim} & V_i \end{array} \tag{Π}$$

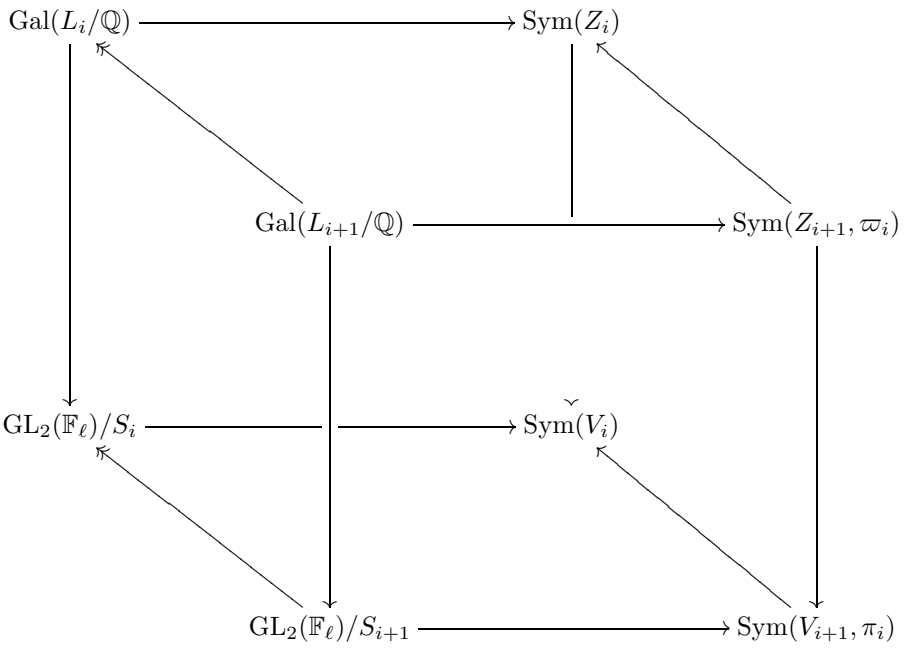
commutes for each i, as expected. This proves that the projections π_i are Galois-equivariant.

What we want to prove is that there exists a compatible[7] system of isomorphisms between $\mathrm{Gal}(L_i/\mathbb{Q})$ and $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ such that the Galois action on Z_i is equivalent

[6]Here and in what follows, by *rigorously* we mean by the use of exact methods such as resultants, as opposed to the expansion of the product over a nonexact field followed by the identification of the coefficients as elements of $\mathbb{Z}$ or $\mathbb{Q}$.

[7]Here and in what follows, by *compatible* we mean compatible with the natural projections from objects at level $i+1$ to objects at level i.

via our bijections θ_i to the natural action of $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ on V_i, so that the diagram



commutes for all i, where the vertical arrows are isomorphisms, $\mathrm{Sym}(V_{i+1}, \pi_i)$ denotes the group of permutations of V_{i+1} that admit the fibres of the projection π_i as a block system, and similarly for $\mathrm{Sym}(Z_{i+1}, \varpi_i)$.

Furthermore, we also want to prove that for all i, the Galois action on Z_i affords a quotient Galois representation $\rho_{f,\mathfrak{l}}^{S_i}$ which is equivalent to $\mathring{\rho}_{f,\mathfrak{l}}^{S_i}$. For brevity, we will then say that the polynomials $F_i(x)$ *correspond* to $\mathring{\rho}_{f,\mathfrak{l}}$.

We will present two methods to rigorously prove that our polynomials $F_i(x)$ correspond to a Galois representation ρ, the second one being more efficient but unfortunately much more complicated than the first one. We will then finally show how to prove that $\rho \sim \mathring{\rho}_{f,\mathfrak{l}}$.

Both methods require that we first check that $F_0(x)$ indeed corresponds to $\mathring{\rho}_{f,\mathfrak{l}}^{\mathrm{proj}}$, so we start by showing how this can be done.

3.3. **Certification of the projective representation.**

3.3.1. *Certification of the Galois group of $F_0(x)$.* We thus begin with the polynomial $F_0(x)$, which ought to correspond to the projective Galois representation $\mathring{\rho}_{f,\mathfrak{l}}^{\mathrm{proj}}$. The first thing to do is to make sure that this polynomial does define a projective Galois representation, by proving that there exists an indexation of Z_0 by $\mathbb{P}^1(\mathbb{F}_\ell)$ such that $\mathrm{Gal}(L_0/\mathbb{Q})$ is permutation isomorphic to a subgroup of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ acting on $\mathbb{P}^1(\mathbb{F}_\ell)$. Since by assumption f has level $N = 1$ and is not exceptional mod $\mathfrak{l}$, we actually expect $\mathrm{Gal}(L_0/\mathbb{Q})$ to be isomorphic to the whole of $\mathrm{PGL}_2(\mathbb{F}_\ell)$.

In principle, we could prove this by computing the polynomial

$$R_4(x) = \prod_{\substack{z_1,z_2,z_3,z_4 \in Z_0 \\ \text{pairwise distinct}}} \left(x - \sum_{n=1}^{4} \lambda_n z_n \right) \in \mathbb{Z}[x]$$

by rigorous methods (e.g., resultants), and by checking how it factors over $\mathbb{Q}$. Here, the λ_n are fixed integers chosen so that $R_4(x)$ is squarefree, so that $R_4(x)$ monitors the action of Galois on quadruplets of roots of $F_0(x)$. The point is that a permutation of $\mathbb{P}^1(\mathbb{F}_\ell)$ comes from $\mathrm{PGL}_2(\mathbb{F}_\ell)$ if and only if it preserves cross-ratios, and this should become apparent in the factorisation of $R_4(x)$.

However, the degree of $R_4(x)$ is approximately ℓ^4, which is quite large for $\ell = 31$, not to mention that since the parameters λ_n must necessarily be distinct, the coefficients of $R_4(x)$ will be huge. As a result, computing $R_4(x)$ would be too slow in practice.

We can instead compute the polynomial

$$R_{4,\mathrm{sym}}(x) = \prod_{I \in \binom{z_0}{4}} \left(x - \sum_{z \in I} z \right) \in \mathbb{Z}[x],$$

where the notation $\binom{X}{n}$ means the set of unordered subsets of cardinal n of the set X. This polynomial monitors the action of Galois on *unordered* quadruplets of roots of $F_0(x)$, and compared to $R_4(x)$, its degree is 24 times smaller, and its coefficients are much smaller, so that computing it is much more amenable. It turns out that the way $R_{4,\mathrm{sym}}(x)$ factors is enough to indicate that $\mathrm{Gal}(L_0/\mathbb{Q})$ is a subgroup of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ in most cases.

To make this claim more precise, let us fix some notation: we let k be a field[8] of characteristic different from 2, and let H be the so-called *anharmonic group*, that is to say, the group of permutations of $\mathbb{P}^1(k)$ generated by $\lambda \mapsto 1 - \lambda$ and $\lambda \mapsto 1/\lambda$. It is well known that $H \simeq \mathfrak{S}_3$ is the stabiliser of the set $\{\infty, 0, 1\}$ for the action of $\mathrm{PGL}_2(k)$ on $\mathbb{P}^1(k)$, and that if $(a, b, c, d) \in \mathbb{P}^1(k)^4$ is a quadruplet of pairwise distinct points, then the cross-ratios of all possible 24 permutations of this quadruplet form an orbit under H. Moreover, since the fibres of the map

$$\begin{array}{ccc} j \colon \mathbb{P}^1(k) \setminus \{\infty, 0, 1\} & \longrightarrow & k \\ \lambda & \longmapsto & 256 \frac{(1-\lambda+\lambda^2)^3}{\lambda^2(1-\lambda)^2} \end{array}$$

are precisely the H-orbits,[9] the composition of the cross-ratio with j yields a well-defined "unordered cross-ratio" map

$$\begin{array}{rccc} u \colon & \binom{\mathbb{P}^1(k)}{4} & \longrightarrow & k \\ & \{a, b, c, d\} & \longmapsto & j([a, b, c, d]), \end{array}$$

where $[\cdot, \cdot, \cdot, \cdot]$ denotes the usual cross-ratio. This map is constant if and only if the anharmonic group H acts transitively on $\mathbb{P}^1(\mathbb{F}_\ell) \setminus \{\infty, 0, 1\}$. Since a H-orbit has at most 6 elements, it is easy to see that for $k = \mathbb{F}_\ell$ with $\ell \in \mathbb{N}$ prime, u is constant if and only if $\ell \leqslant 5$.

Theorem 2. *If $\ell \neq 5$, then the permutations of $\mathbb{P}^1(\mathbb{F}_\ell)$ that preserve the unordered cross-ratio map u are precisely the ones that come from $\mathrm{PGL}_2(\mathbb{F}_\ell)$.*

[8] We have $k = \mathbb{F}_\ell$ in mind, but we would like to make general statements.

[9] This is because $j(\lambda)$ is the j-invariant of the Legendre curve $y^2 = x(x-1)(x-\lambda)$, so that the map j we define is the projection from the modular curve $X(2)$ (identified to the λ-line via Legendre curves) to $X(1)$ (identified to the j-line), and because H is the Galois group of the covering $X(2) \longrightarrow X(1)$ under these identifications. The author thanks S. Siksek for bringing this to his attention.

Proof. If $\ell \leqslant 3$, then every permutation of $\mathbb{P}^1(\mathbb{F}_\ell)$ comes from $\mathrm{PGL}_2(\mathbb{F}_\ell)$ and so there is nothing to prove. We may therefore assume that $\ell \geqslant 7$. But then $u\colon \binom{\mathbb{P}^1(k)}{4} \longrightarrow k$ is not a constant map, so its stabiliser in $\mathfrak{S}_{\ell+1}$ is a strict subgroup $S < \mathfrak{S}_{\ell+1}$ which clearly contains $\mathrm{PGL}_2(\mathbb{F}_\ell)$. But $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is a maximal subgroup of $\mathfrak{S}_{\ell+1}$ according to the following theorem, whence the result. □

Theorem 3. *Let $\ell \geqslant 5$ be a prime. The permutation group $\mathrm{PGL}_2(\mathbb{F}_\ell)$ of $\mathbb{P}^1(\mathbb{F}_\ell)$ is a maximal subgroup of the symmetric group $\mathfrak{S}_{\ell+1}$.*

Proof. Since $\ell \geqslant 5$, $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is a strict subgroup of $\mathfrak{S}_{\ell+1}$. Suppose that there is a group X such that $\mathrm{PGL}_2(\mathbb{F}_\ell) < X < \mathfrak{S}_{\ell+1}$. Then X is at least 3-transitive. By looking through the list of 2-transitive finite permutation groups given in section 7.7 of [DM96], it can be derived that the 3-transitive finite permutation groups are the following:

- the projective semilinear groups G with $\mathrm{PSL}_2(\mathbb{F}_q) \leqslant G \leqslant \mathrm{P\Gamma L}_2(\mathbb{F}_q)$, where q is a power of a prime p and $G \not\leqslant \mathrm{P\Sigma L}_2(\mathbb{F}_q)$ if $p \neq 2$, degree $q+1$,
- the affine groups $\mathrm{AGL}_n(\mathbb{F}_2) = \mathbb{F}_2^n \rtimes \mathrm{GL}_n(\mathbb{F}_2)$, degree 2^n,
- the group $\mathbb{F}_2^4 \rtimes \mathfrak{A}_7$, degree 16,
- the Mathieu groups M_{11}, M_{12}, M_{22}, $\mathrm{Aut}(M_{22})$, M_{23} and M_{24}, respective degrees 11 or 12, 12, 22, 22, 23, 24,
- the alternating groups $\mathfrak{A}_n$ ($n \geqslant 5$), degree n,
- and the symmetric groups $\mathfrak{S}_n$ ($n \geqslant 3$), degree n,

where $\mathrm{P\Gamma L}_2(k)$ (resp. $\mathrm{P\Sigma L}_2(k)$) denotes the permutation group of $\mathbb{P}^1(k)$ generated by $\mathrm{PGL}_2(k)$ (resp. $\mathrm{PSL}_2(k)$) and by the automorphisms of the ground field k.

As we want degree $\ell+1$ with ℓ prime, this only leaves $\mathrm{AGL}_n(\mathbb{F}_2)$, M_{11}, M_{12}, M_{24} and $\mathfrak{A}_{\ell+1}$ as candidates for X. However, these groups are all perfect, so they all act by even permutations and thus cannot contain $\mathrm{PGL}_2(\mathbb{F}_\ell)$. □

As far as we are concerned, the main consequence of this is that it is enough to see how $R_{4,\mathrm{sym}}(x)$ factors to prove that $\mathrm{Gal}(L_0/\mathbb{Q})$ is permutation isomorphic to a subgroup of $\mathrm{PGL}_2(\mathbb{F}_\ell)$, and this is a stark improvement compared to working with $R_4(x)$, whose degree is 24 times larger.

The computer algebra package [Magma] contains two functions named, respectively, `GaloisGroup` and `GaloisProof` whose aim is to compute Galois groups by the algorithm described in [FK14]. The former, when supplied with an irreducible polynomial $f(x) \in \mathbb{Z}[x]$ and a prime number $v \in \mathbb{N}$, tries to guess the Galois group of $f(x)$ as a permutation group acting on the v-adic roots of $f(x)$, albeit nonrigorously; in order to get a certification of this result, it is necessary to then apply the latter function.

In our case, if we pick a prime $p \in \mathbb{N}$ such that $F_0(x)$ is irreducible[10] mod p, then when we call `GaloisGroup` on $\big(F_0(x), p\big)$, it only takes a few seconds (even for $\ell = 31$) for [Magma] to return a guess for $\mathrm{Gal}(L_0/\mathbb{Q})$, thanks to the efficiency of [FK14], the fact that $F_0(x)$ is of degree only $\ell+1$ and has been `polred`ed, and to the nontrivial information provided by the cyclic action of the Frobenius at p on the p-adic roots of $F_0(x)$. However, as explained above, this is not rigorous, so we then call `GaloisProof`, which forces [Magma] to compute and factor $R_{4,\mathrm{sym}}(x)$ rigorously so as to verify the output of `GaloisGroup`. This takes of course much

[10]Such a prime should exist and should not be too hard to come by, as a nonnegligible proportion $\left(\frac{\varphi(\ell+1)}{2(\ell+1)}, \text{ to be precise}\right)$ of elements of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ act as $(\ell+1)$-cycles on $\mathbb{P}^1(\mathbb{F}_\ell)$.

longer (up to 4 days for $\ell = 31$), and in fact this is by far the most time-consuming part of the whole certification process of our polynomials, at least for large ℓ.

We then check explicitly that this Galois group is permutation-isomorphic to $\mathrm{PGL}_2(\mathbb{F}_\ell)$ acting on $\mathbb{P}^1(\mathbb{F}_\ell)$. We fix such an isomorphism,[11] and we will use it to identify $\mathrm{Gal}(L_0/\mathbb{Q})$ with $\mathrm{PGL}_2(\mathbb{F}_\ell)$ from now on. This yields a bijection θ_0 between the roots of $F_0(x)$ in $\overline{\mathbb{Q}_p}$ and $\mathbb{P}^1(\mathbb{F}_\ell)$ which makes the Galois action equivalent to the natural action of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ on $\mathbb{P}^1(\mathbb{F}_\ell)$.

3.3.2. *Correctness of the projective representation.* Now that we have made sure that the Galois action on the roots of $F_0(x)$ does define a projective representation

$$\rho^{\mathrm{proj}} \colon G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(L_0/\mathbb{Q}) = \mathrm{PGL}_2(\mathbb{F}_\ell)\ ,$$

we want to prove that this representation is isomorphic to $\mathring{\rho}^{\mathrm{proj}}_{f,\mathfrak{l}}$ as expected. For this, we use the following result from [Bos07, Section 2]:

Theorem 4. *Let $\pi \colon G_{\mathbb{Q}} \longrightarrow \mathrm{PGL}_2(\mathbb{F}_\ell)$ be an irreducible projective* mod ℓ *Galois representation, where $\ell \geqslant 3$. Let $H < \mathrm{PGL}_2(\mathbb{F}_\ell)$ be the stabiliser of a point of $\mathbb{P}^1(\mathbb{F}_\ell)$, and let $K = \overline{\mathbb{Q}}^{\pi^{-1}(H)}$ be the corresponding number field. If K has exactly two real places, and if there exists an integer $k \geqslant 3$ such that*

$$\operatorname{disc} K = \pm \ell^{k+\ell-2},$$

then there exists a newform $f \in S_k(1)$ and a prime $\mathfrak{l}$ of $\overline{\mathbb{Q}}$ above ℓ such that

$$\pi \sim \mathring{\rho}^{\mathrm{proj}}_{f,\mathfrak{l}}.$$

Sketch of proof. By assumption, the image of complex conjugation by π is a non-trivial matrix which is diagonalisable over $\mathbb{F}_\ell$, and so π is absolutely irreducible. The idea is then that π can be lifted to a linear representation

$$\rho \colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}_\ell})$$

which, just like π, is absolutely irreducible, odd, and ramifies only at ℓ. Serre's modularity conjecture (cf. [KW09]) then applies and shows that ρ is modular, say $\rho \sim \mathring{\rho}_{f,\mathfrak{l}}$ for some newform $f \in S_{k_\rho}(N_\rho, \varepsilon_\rho)$ and some prime $\mathfrak{l}$ of $\overline{\mathbb{Q}}$ above ℓ. Then, since ρ ramifies only at ℓ, its Artin conductor is a power of ℓ, so ρ comes from a form f of level $N_\rho = 1$. Finally, if the lift ρ is chosen so that the weight k_ρ of f is minimal, then [MT03, Theorem 3] gives a formula for the ℓ-adic valuation of the discriminant of the Galois number field cut out by ρ, which by J. Bosman's work boils down to

$$\operatorname{disc} K = \pm \ell^{k_\rho+\ell-2}.$$

□

Thus, in order to prove that $\rho^{\mathrm{proj}} \sim \mathring{\rho}^{\mathrm{proj}}_{f,\mathfrak{l}}$, all we have to do is count the real roots of $F_0(x)$, which can be done by using Sturm's method (cf. [Lan02, Chapter XI, Theorem 2.7]), and check that the discriminant of the root field $K^{\mathrm{proj}} = \mathbb{Q}[x]/F_0(x)$ is $\pm\ell^{k+\ell-2}$, which is a piece of cake for [Pari/GP]. If k is such that $\dim S_k(1) = 1$, e.g., $k \leqslant 22$, then this is enough to conclude that $\rho^{\mathrm{proj}} \sim \mathring{\rho}^{\mathrm{proj}}_{f,\mathfrak{l}}$, as the coefficients of f are then rational so that the choice of the prime $\mathfrak{l}$ lying above ℓ does not matter.

[11] Note that as every automorphism of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is inner, our isomorphism must be the "right" one.

In the case $\dim S_k(1) > 1$, we can check that the newforms in $S_k(1)$ are all conjugate under Galois as predicted by Maeda's conjecture, and so we only have to make sure that $\rho^{\mathrm{proj}} \sim \mathring{\rho}^{\mathrm{proj}}_{f,\mathfrak{l}}$ for the right prime $\mathfrak{l}$ above ℓ. For instance, in the case $\ell = 31, k = 24$, we have that $S_{24}(1)$ has dimension 2 and is spanned by the two conjugates of a newform $f_{24} = \sum_{n\geqslant 1} \tau_{24}(n)q^n$ whose eigenvalues lie in a quadratic field; since 31 splits in this field, say $31 = \mathfrak{l}_1\mathfrak{l}_2$, we know that ρ^{proj} is equivalent either to $\mathring{\rho}^{\mathrm{proj}}_{f_{24},\mathfrak{l}_1}$ or to $\mathring{\rho}^{\mathrm{proj}}_{f_{24},\mathfrak{l}_2}$. In order to tell which, we pick a small prime $p \in \mathbb{N}$ such that $F_0(x)$ is squarefree mod p (in particular $p \neq \ell$), and such that $\tau_{24}(p) \equiv 0 \bmod \mathfrak{l}_1$ but $\tau_{24}(p) \not\equiv 0 \bmod \mathfrak{l}_2$ (the opposite would do too). Since an element of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is of order 2 if and only if it has trace 0, looking at the factorisation of F_0 mod p allows us to tell $\mathfrak{l}_1$ and $\mathfrak{l}_2$ apart: if $F_0(x)$ mod p splits into linear and quadratic factors but does not split completely, then it is associated to $\mathring{\rho}^{\mathrm{proj}}_{f_{24},\mathfrak{l}_1}$, otherwise it is associated to $\mathring{\rho}^{\mathrm{proj}}_{f_{24},\mathfrak{l}_2}$.

3.4. **Two approaches to the certification of the Galois groups of the $F_i(x)$.** In principle, we could simply ask again [Magma] to determine the Galois group of the $F_i(x)$, as we did above for $F_0(x)$. However, the permutation groups $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ are not characterised as nicely as $\mathrm{PGL}_2(\mathbb{F}_\ell)$, which can be defined as the group of permutations of $\mathbb{P}^1(\mathbb{F}_\ell)$ that preserve cross-ratios. As a result, Magma would have to rely on much more involved group-algorithmic methods, which would make the computation much slower.[12] We are going to present methods which require much less computation, and which also yield proofs that are more human-readable.

We are actually going to present two methods to exhibit a permutation isomorphism between the Galois group of $F_r(x)$ and $\mathrm{GL}_2(\mathbb{F}_\ell)/S_r$ acting naturally on $V_r = V/S_r$. The first one, which we present in section 3.5, is the more natural one, and is entirely due to the reviewer of an older version of this article; the author wishes to thank him profusely for this. Unfortunately, it leads to computations which, albeit not as slow as a blunt [Magma] attack, still require quite a bit of computation time. The method that we will present in the next section 3.6 requires much less computation time; unfortunately, it is also much more complicated to explain.

3.5. **The geometric approach.** The method presented in this section could be used with pretty much any representation $\mathring{\rho}\colon \mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$ whose quotients $\mathring{\rho}^{S_i}$ are surjective, where $\mathbb{K}$ can be any field[13] in which we can perform computations such as polynomial factorisation.

In this section, we thus suppose that we have a collection of irreducible polynomials $F_i(x) \in \mathbb{K}[x]$, $0 \leqslant i \leqslant r$, which ought to correspond to such a Galois representation $\mathring{\rho}$. We also suppose that the $F_i(x)$ split completely in some extension[14] Ω of $\mathbb{K}$, and that we have conjectured a compatible system of bijections $(\theta_i)_{0\leqslant i\leqslant r}$ between the roots of $F_i(x)$ in Ω and the V_i such that we expect the Galois action on the roots of $F_i(x)$ to be permutation isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ acting

[12] In fact, the `GaloisGroup` function can still make the right guess pretty quickly, but this guess must then be proved by calling the `GaloisProof` function, and this is far too slow because of the degree of the polynomials $F_i(x)$ for $i > 0$. For instance, for Δ mod 19, it takes [Magma] four days to laboriously manage to certify that the Galois group of $F_1(x)$ is permutation isomorphic to $\mathrm{GL}_2(\mathbb{F}_{19})/\mathbb{F}_{19}^{*2}$. By comparison, the method presented in section 3.6 below merely takes a few minutes.

[13] We have a number field in mind.

[14] We have $\Omega = \mathbb{C}$ or some finite extension of $\mathbb{Q}_p$ in mind.

naturally on V_i, and such that the relations (Π) and (T) defined on page 389 hold between the roots of $F_i(x)$ and those of $F_{i+1}(x)$ for all $i < r$. For each i, we identify via θ_i the set of roots of $F_i(x)$ with V_i, and the Galois group of $F_i(x)$ with a permutation group of V_i; the projections $\pi_i \colon V_{i+1} \twoheadrightarrow V_i$ are then Galois-equivariant. Finally, we also assume that we have managed to prove that the Galois group of $F_0(x)$ is indeed permutation isomorphic to $\mathrm{PGL}_2(\mathbb{F}_\ell)$ via θ_0 by a method similar to the one described in section 3.3.1 above. We may thus identify the Galois group of $F_0(x)$ with $\mathrm{PGL}_2(\mathbb{F}_\ell)$.

Our goal is to prove that the Galois group of $F_r(x)$ is contained in $\mathrm{GL}_2(\mathbb{F}_\ell)/S_r$. The key idea of the method presented in this section is to prove that its action on V_r is "linear". However, as the addition of vectors does not descend to a well-defined operation on V_r, this is not completely straightforward.

To begin with, the relation (T) tells us that the Galois group of $F_r(x)$ is a subgroup of the wreath product $\mathrm{Sym}(\mathbb{F}_\ell^*/S_r) \wr \mathrm{PGL}_2(\mathbb{F}_\ell)$. We first want to prove that it is actually a subgroup of $(\mathbb{F}_\ell^*/S_r) \wr \mathrm{PGL}_2(\mathbb{F}_\ell)$, in other words that the action of Galois commutes with scalar multiplication.

Clearly, it is enough to prove that Galois commutes with the scalar multiplication by a generator ε of $\mathbb{F}_\ell^*/S_r$. To do so, we compute by interpolation a polynomial $\widetilde{E}(x) \in \Omega[x]$ which, for all $v \in V_r$, maps the root of $F_r(x)$ indexed by v to the root indexed by $\varepsilon \cdot v$. We then try to identify the coefficients of this polynomial as approximations of elements of $\mathbb{K}$, whence a polynomial $E(x) \in \mathbb{K}[x]$. If $E(x)$ indeed approximately maps the root indexed by v to the one indexed by $\varepsilon \cdot v$ for all $v \in V_r$ and if $F_r(x)$ divides $F_r \circ E(x)$, this proves that the Galois action commutes with scalar multiplication on V_r.

We expect this approach to succeed since multiplication by ε indeed defines an automorphism not only of the splitting field but also of the root field $\mathbb{K}[x]/\mathring{F}_r(x)$ of $\mathring{F}_r(x)$. Moreover, interpolating over the roots of $F_r(x)$ amounts to solving a linear system whose determinant is the discriminant of $F_r(x)$, so that the coefficients of $E(x)$ should not be too difficult to identify if the ones of $F_r(x)$ are nice. In practice, with our `polred`ed polynomial $F_r(x) \in \mathbb{Z}[x]$, it indeed takes just a few seconds to compute $E(x) \in \mathbb{Q}[x]$ and to check that $F_r \circ E(x) \equiv 0 \bmod F_r(x)$.

We may thus assume henceforth that the Galois group of $F_r(x)$ is contained in $P = (\mathbb{F}_\ell^*/S_r) \wr \mathrm{PGL}_2(\mathbb{F}_\ell)$. Let us consider, for all triples $(L_1, L_2, M) \in \mathbb{P}^1(\mathbb{F}_\ell)^3$ of pairwise distinct vector lines in $\mathbb{F}_\ell^2$, the map

$$t_{L_1,L_2,M} \colon L_1 \longrightarrow L_2$$

that sends a point $x \in L_1$ to the intersection of L_2 and of the line through x that is parallel to M (cf. Figure 1).

Clearly, for all $S \leqslant \mathbb{F}_\ell^*$, this map descends to a map

$$t^S_{L_1,L_2,M} \colon L_1/S \longrightarrow L_2/S.$$

If we now let X denote the set of triples $(v_1, v_2, M) \in V_r \times V_r \times \mathbb{P}^1(\mathbb{F}_\ell)$ such that the line L_1 spanned by v_1, the line L_2 spanned by v_2, and the line M are pairwise distinct, we can define another map

$$\Lambda \colon X \longrightarrow \mathbb{F}_\ell^*/S_r$$

by sending (v_1, v_2, M) to the unique scalar $\lambda \in \mathbb{F}_\ell^*/S_r$ such that $v_2 = \lambda \cdot t^S_{L_1,L_2,M}(v_1)$.

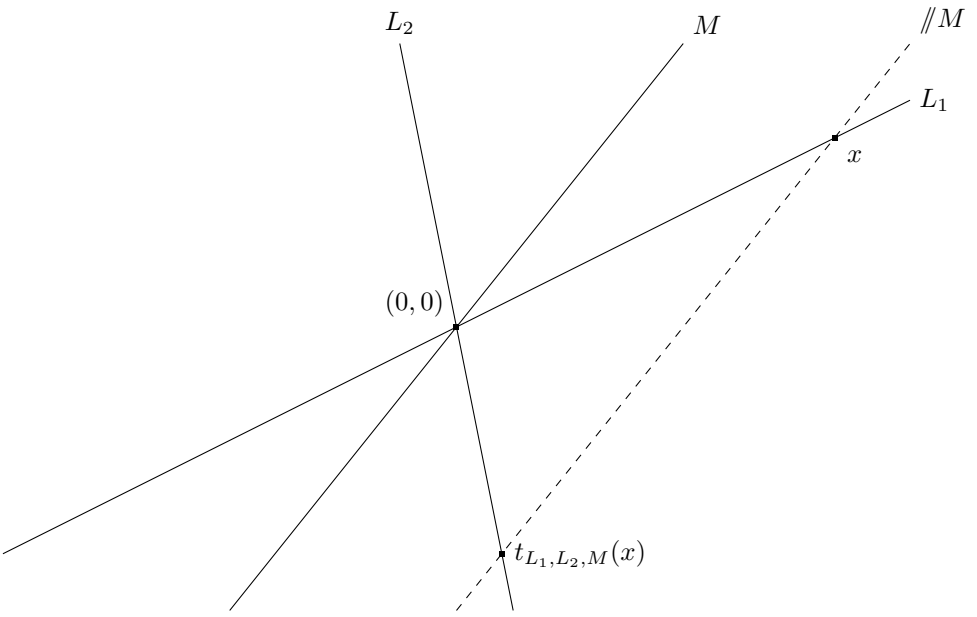


FIGURE 1

The group $\mathrm{GL}_2(\mathbb{F}_\ell)/S_r$ acts diagonally on X, and it is clear that Λ is invariant under this action. Conversely, we have the following:

Lemma 5. *Let $\sigma \in P$. If $\Lambda(\sigma\cdot v_1, \sigma\cdot v_2, \sigma\cdot M) = \Lambda(v_1, v_2, M)$ for all $(v_1, v_2, M) \in X$, then $\sigma \in \mathrm{GL}_2(\mathbb{F}_\ell)/S_r$.*

Proof. Let $\sigma \in P$ be such an element, and let $g \in \mathrm{GL}_2(\mathbb{F}_\ell)/S_r$ have the same image in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ as σ. Then $\sigma' = g^{-1}\sigma$ lies in $(\mathbb{F}_\ell^*/S_r)^{\mathbb{P}^1(\mathbb{F}_\ell)}$ and leaves Λ invariant, and so in fact lies in the diagonal $\mathbb{F}_\ell^*/S_r$. It follows that $\sigma \in \mathrm{GL}_2(\mathbb{F}_\ell)/S_r$. □

As a result, all we need to do is check that Λ is invariant under Galois. This leads us to the resolvent

$$R(x) = \prod_{(\alpha_1,\alpha_2,\alpha_3)\in Z} \left(x - \sum_{i=1}^{3} \lambda_i \alpha_i \right) \in \mathbb{K}[x],$$

where the $\lambda_i \in \mathbb{Z}$ are parameters chosen so that $R(x)$ is squarefree, and Z is the set of triples $(\alpha_1, \alpha_2, \alpha_3)$ with α_3 a root $F_0(x)$, α_1,α_2 roots of $F_r(x)$, and α_1, α_2 and α_3 corresponding to three distinct roots of $F_0(x)$ under the correspondence (T). If we can compute $R(x)$ rigorously and prove that it factors along the fibres of Λ, then we have proved that the Galois group of $F_r(x)$ is contained in $\mathrm{GL}_2(\mathbb{F}_\ell)/S_r$.

Unfortunately, just like the resolvent $R_4(x)$ from section 3.3.1, the resolvent $R(x)$ would take a lot of time to compute in our case. Indeed, its degree is $2^{2r}(\ell^3-\ell)$, and for us this is too much: we have $\ell \leqslant 31$ in mind, but even if we restricted ourselves to the primes $\ell \equiv -1 \bmod 4$ so that $r = 1$ so as to get an asymptotic $\deg R(x) = O(\ell^3)$, which is better than the degrees $\deg R_4(x) = O(\ell^4)$ of the resolvents considered in section 3.3.1, we would still have

$$\deg R(x) \gg \deg R_{4,\mathrm{sym}}(x),$$

due to the factor 24 in $\deg R_{4,\mathrm{sym}}(x) = \binom{\ell+1}{4} \sim \ell^4/24$. In fact, it can easily be checked that $\deg R(x) > \deg R_{4,\mathrm{sym}}(x)$ for all $\ell < 103$, which incidentally illustrates again how useful switching from $R_4(x)$ to $R_{4,\mathrm{sym}}(x)$ was in section 3.3.1.

As certifying the Galois group of $F_0(x)$ thanks to the resolvent $R_{4,\mathrm{sym}}(x)$ already took up to 4 days for $\ell = 31$, this is a real problem. For this reason, we introduce another method to certify the Galois group of the $F_i(x)$ in the next section. This other method is much more complicated, but the computation time it requires is almost negligible compared to the time needed to certify the Galois group of $F_0(x)$, at least when $r \leqslant 2$.

3.6. **The group cohomology approach.** Just like the method presented in the previous section, the method that we are now going to introduce could be applied to a more general framework than the case of modular Galois representations attached to forms of level 1. It is not as general as the previous one though, in that it requires working with representations $\mathring{\rho}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$ whose image contains $\mathrm{SL}_2(\mathbb{F}_\ell)$ and whose determinant is still an odd power of the mod ℓ cyclotomic character. For instance, it could be used to certify Galois representation computations attached to newforms of any level, but of trivial nebentypus.

Therefore, in this section we merely suppose that we want to prove that the polynomials $F_i(x) \in \mathbb{Z}[x]$ correspond to such a Galois representation $\mathring{\rho}$. In particular, this implies that $\mathring{\rho}^{S_i}$ surjects to $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ for all i. We also suppose that we have a relation of the form (T) between the roots of $F_i(x)$ and $F_{i+1}(x)$, that is to say, that for all $i < r$, any root of $F_i(x)$ is the sum of precisely two roots of $F_{i+1}(x)$. However, even though we want to prove the existence of a compatible system of indexations of the sets Z_i of roots of $F_i(x)$ by V_i making the Galois action permutation isomorphic to the natural action of $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$, this time we do **not** suppose that we already have a candidate for such a system of indexations. Indeed, we are going to work with p-adic roots, whereas our algorithm [Mas13] returns a candidate indexation of the *complex* roots of the $F_i(x)$. We therefore let Z_i denote the set of roots of $F_i(x)$ in some large enough extension of $\mathbb{Q}_p$, where $p \in \mathbb{N}$ is some fixed prime. We reserve the letter p for this prime from now on.

Remark 6. It could be argued that since Magma's function `GaloisGroup` is so efficient, we could easily find a candidate for such a system of indexation of the Z_i by the V_i if we wanted to. However, we would still have to prove that this indexation is correct, and the method which we are going to present will involve constructing a certified system of indexations from scratch anyway.

In the last steps of the method presented in this section, it will be necessary to assume that p is such that $F_r(x)$ (and hence all the $F_i(x)$) is irreducible mod p, and it will be convenient to further assume that p is rather large, say roughly the size of a machine word. Just as in the projective case, there are plenty of elements of $\mathrm{GL}_2(\mathbb{F}_\ell)/S_r$ which act as transitive cycles on V_r, so such a prime should not be too difficult to come by. We thus henceforth assume that p is such a prime, and that we gave this p as a parameter to [Magma] when we certified that the Galois group of $F_0(x)$ may be identified to $\mathrm{PGL}_2(\mathbb{F}_\ell)$ as a permutation group of Z_0.

Finally, as before we let K_i denote the root field $K_i = \mathbb{Q}[x]/F_i(x)$ of $F_i(x)$, and L_i denote its Galois closure, and we suppose that for each $i < R$ we know a primitive integral element $\delta_i \in K_i$ such that $K_{i+1} = K_i(\sqrt{\delta_i})$.

The idea of the method which we are going to present is to first see the Galois group of $F_i(x)$ as a group extension of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ of a certain kind, then to use explicit group cohomology arguments so as to establish a finite list of possibilities for this group, and next to rely on ramification arguments to eliminate all possibilities but one.[15] This process will rely on an induction on i, and will allow us to prove that $\mathrm{Gal}(L_i/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ as an *abstract* group. We will then prove, again by induction on i, that this isomorphism can be turned into an isomorphism of *permutation* groups, in other words that Galois acts on Z_i in the expected way. Finally, we will use the Frobenius at p to determine explicitly a system of indexation of the Z_i by the V_i corresponding to this isomorphism.

3.6.1. *Certification of the Galois group of $F_i(x)$ as an abstract group.* Let

$$\mathbb{Q} = \kappa_0 \underset{2}{\subsetneq} \kappa_1 \underset{2}{\subsetneq} \cdots \underset{2}{\subsetneq} \kappa_r \underset{\text{odd}}{\subseteq} \mathbb{Q}(\mu_\ell)$$

be the subfields of the cyclotomic extension $\mathbb{Q}(\mu_\ell)$ such that for all $0 \leqslant i \leqslant r$, $\mathrm{Gal}(\kappa_i/\mathbb{Q}) \simeq \mathbb{Z}/2^i\mathbb{Z}$. Thus for instance $\kappa_1 = \mathbb{Q}(\sqrt{\ell^*})$, where $\ell^* = \left(\frac{-1}{\ell}\right)\ell$.

Consider the following assertions:

(A1) If $C \subseteq L_r$ is a Galois subfield of L_r such that $\mathrm{Gal}(C/\mathbb{Q}) \simeq \mathbb{Z}/2^k\mathbb{Z}$ for some integer $k \leqslant r+1$, then C ramifies only at ℓ.

(A2) For each $i < r$, let $\Delta_i(x) \in \mathbb{Z}[x]$ be the monic minimal polynomial of δ_i over $\mathbb{Q}$, and let

$$Q_i(x) = \frac{\mathrm{Res}_y\left(\Delta_i(y), \Delta_i(xy)\right)}{(x-1)^{2^i(\ell+1)}} \in \mathbb{Z}[x].$$

Then, for each irreducible factor $R(x)$ of $Q_i(x)$ over $\mathbb{Q}$, there exists an integer $j \leqslant i$ such that the field $\mathbb{Q}[x]/R(x)$ does not contain κ_{j+1}, whereas the algebra $\mathbb{Q}[x]/R(x^2)$ does contain κ_{j+1} (as a subalgebra with unit).

(A3) For each $i < r$, there exists a prime $v \in \mathbb{N}$ such that $F_i(x)$ is squarefree and totally split mod v, but $F_{i+1}(x)$ is not.

We do not know yet whether these assertions hold, but, we expect them to:

(1) Since the abelianisation of $\mathrm{GL}_2(\mathbb{F}_\ell)$ is given by the determinant, if, as expected, the polynomials $F_i(x)$ have Galois group $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ and correspond to a Galois representation whose determinant is a power of the mod ℓ cyclotomic character, then the maximal Abelian subextension of L_r will be contained in the cyclotomic extension $\mathbb{Q}(\mu_\ell)$; we therefore expect (A1) to hold.

Conversely, we note that if (A1) holds, then any 2-cyclic subextension field L_r is contained in $\mathbb{Q}(\mu_{\ell^\infty})$, hence in $\mathbb{Q}(\mu_\ell)$. Since $\mathrm{PGL}_2(\mathbb{F}_\ell)$ has a quotient $\mathrm{PGL}_2(\mathbb{F}_\ell)/\mathrm{PSL}_2(\mathbb{F}_\ell)$ of order 2, the fields $L_i \supset L_0$ all have at least one quadratic subfield, which must then be $\kappa_1 = \mathbb{Q}(\sqrt{\ell^*})$, and in particular be unique. We will use this fact repeatedly to prove Theorem 7 below.

(2) We expect (A2) to hold, but it will make much more sense to explain why after the proof of Lemma 9 below, so we postpone the explanation

[15] This is where we need the hypothesis that $\det \mathring{\rho}$ is a power of the mod ℓ cyclotomic character for our approach to have a chance to work.

to Remark 10. For now, we just note that for any polynomial $P(x) = \prod_{i=1}^{n}(x-\alpha_i)$ such that $P(0) \neq 0$,

$$\mathrm{Res}_y\big(P(y), P(xy)\big) = (-1)^n P(0) \prod_{i,j} \left(x - \frac{\alpha_i}{\alpha_j}\right),$$

so that

$$\frac{\mathrm{Res}_y\big(P(y), P(xy)\big)}{(x-1)^n} = (-1)^n P(0) \prod_{i \neq j} \left(x - \frac{\alpha_i}{\alpha_j}\right).$$

Therefore, $Q_i(x)$ is indeed a polynomial.

(3) Finally, we also expect (A3) to hold: for each i, it suffices to consider a prime at which the Frobenius element is $\left[\begin{smallmatrix} \varepsilon & 0 \\ 0 & \varepsilon \end{smallmatrix}\right]$ for some $\varepsilon \in S_i - S_{i+1}$. We can thus even predict that at such a prime, while $F_i(x)$ splits in linear factors, $F_{i+1}(x)$ will split in quadratic factors.

Conversely, in this subsection and the next one, we are going to prove the following result, which thus yields an efficient method to formally prove our computations:

Theorem 7. *Assume that the assertions* (A1), (A2) *and* (A3) *hold. In addition, if ℓ is such that $r \geqslant 3$, also assume that $\kappa_{i+1} \subset L_i$ for all $2 \leqslant i < r$. Then, for all $i \leqslant r$,*

(i) $\mathrm{Gal}(L_i/\mathbb{Q})$ *is isomorphic to* $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$*, not only abstractly, but also as an extension of* $\mathrm{PGL}_2(\mathbb{F}_\ell)$*, and*

(ii) *there exists such an isomorphism which makes the Galois action on the roots of $F_i(x)$ equivalent to the natural action of* $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ *on V_i.*

Remark 8. It is unfortunate that we have to make the extra assumption that $\kappa_{i+1} \subset L_i$ for all $2 \leqslant i < r$ when $r \geqslant 3$, especially as the author does not know of any computationally cheap way to check this assumption rigorously. Indeed, if as expected the polynomials $F_i(x)$ correspond to a Galois representation $\mathring{\rho}$, then under the isomorphism $\mathrm{Gal}(L_i/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)/S_i$, κ_{i+1} corresponds to the kernel of the determinant, whereas the bigger compositum of K_i with itself (cf. Remark 10 below) corresponds to $\left\{\left[\begin{smallmatrix} s & 0 \\ 0 & s' \end{smallmatrix}\right] \bmod S_i \mid s, s' \in S_i\right\}$ and so does not contain κ_{i+1}, so that unfortunately one has to deal with the 3-fold compositum of K_i to show that $\kappa_{i+1} \subset L_i$. The method presented in the previous section does not suffer from this shortcoming; on the other hand, the values of ℓ for which we have data to use Theorem 7 on, namely $\ell \leqslant 31$, are all such that $r \leqslant 2$, except for $\ell = 17$ for which even the method presented in section 2 does not suffice to reduce the polynomials $F_i(x)$ anyway.

Before we start proving Theorem 7, let us indicate how the assertions (A1), (A2) and (A3) can be checked in practice.

(1) Let N be the product of the odd primes different from ℓ that ramify in L_r, and let C be a 2-cyclic subextension of L_r of degree 2^k, $k \leqslant r+1$. Then $C \subseteq \mathbb{Q}(\mu_{2^{r+3}\ell N})$, and so $\mathrm{Gal}\big(\mathbb{Q}(\mu_{2^{r+3}\ell N})/C\big)$ is the kernel of some surjective morphism

$$\varphi\colon \mathrm{Gal}\big(\mathbb{Q}(\mu_{2^{r+3}\ell N})/\mathbb{Q}\big) \simeq (\mathbb{Z}/2^{r+3}\ell N\mathbb{Z})^* \longrightarrow \mathbb{Z}/2^k\mathbb{Z}.$$

By Chinese remainders, we can write $\varphi = \varphi_\ell + \psi$, where

$$\varphi_\ell\colon (\mathbb{Z}/\ell\mathbb{Z})^* \longrightarrow \mathbb{Z}/2^k\mathbb{Z} \quad \text{and} \quad \psi\colon (\mathbb{Z}/2^{r+3}N\mathbb{Z})^* \longrightarrow \mathbb{Z}/2^k\mathbb{Z}.$$

We then look for odd primes $v \in \mathbb{N}$ such that $v \equiv 1 \bmod \ell$ and $F_r(x)$ is squarefree and splits completely mod v. For such v, we have $\varphi_\ell(v) = 0$ and $\varphi(v) = 0$, so that $\psi(v) = 0$ too. Therefore, if we can find a collection of such v which spans $(\mathbb{Z}/2^{r+3}N\mathbb{Z})^* \otimes \mathbb{Z}/2^{r+1}\mathbb{Z}$, then this proves that ψ is necessarily trivial, and thus that (A1) holds.

In practice, finding primes v which split $F_r(x)$ completely should not be too difficult since we expect $\mathrm{Gal}(L_r/\mathbb{Q})$ to be isomorphic to the $\mathrm{GL}_2(\mathbb{F}_\ell)/S_r$. Then, the fact that a collection of primes v spans $(\mathbb{Z}/2^{r+3}N\mathbb{Z})^* \otimes \mathbb{Z}/2^{r+1}\mathbb{Z}$ can be checked by expressing the latter group explicitly as a product of cyclic groups, by determining the image of the primes v in these groups thanks to a discrete logarithm computation, and finally by computing a Smith normal form. This should all be painless, as N will typically involve few prime factors, and these primes will not be very large. Note that even in the case where r is large, the $(\mathbb{Z}/2^{r+3}\mathbb{Z})^*$-part can be treated easily, since for any integer $a \geqslant 3$, a subgroup of $(\mathbb{Z}/2^a\mathbb{Z})^*$ which surjects onto $(\mathbb{Z}/8\mathbb{Z})^*$ is necessarily the whole of $(\mathbb{Z}/2^a\mathbb{Z})^*$.

We expect this approach to succeed, because if, as expected, $\mathrm{Gal}(L_r/\mathbb{Q})$ is isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)/S_r$ and the determinant of the associated Galois representation is a power of the mod ℓ cyclotomic character, then L_r will have a unique maximal 2-cyclic subextension C, which has no nontrivial Abelian subextensions since

$$\mathrm{Gal}(L_r/C) = \{A \in \mathrm{GL}_2(\mathbb{F}_\ell)/S_r \mid \det A = 1\} \simeq \mathrm{SL}_2(\mathbb{F}_\ell)$$

has trivial abelianisation.

Note that in the particular case of a Galois representation of level 1, there is much less work to do: it suffices to check that the discriminant of K_r is, up to a sign, a power of ℓ.

Also note that if (A1) does hold, then L_r cannot actually have any subextension C such that $\mathrm{Gal}(C/\mathbb{Q}) \simeq \mathbb{Z}/2^{r+1}\mathbb{Z}$, by definition of r.

(2) We explain in Remark 10 below why we expect $Q_i(x)$ to factor into $2^i - 1$ irreducible factors of degree $2^i(\ell+1)$ and one large irreducible factor, and why (A2) should be satisfied for $j = 0$ for the small factors and $j = 1$ for the large factor. To check that $\kappa_{j+1} \not\subset \mathbb{Q}[x]/R(x)$, it suffices to find a prime $v \in \mathbb{N}$ such that the splitting behaviour of $R(x)$ mod v is inconsistent with the splitting behaviour of v in κ_{j+1}, for instance such that v is not a square mod ℓ and such that $R(x)$ mod v is squarefree and splits into factors whose degrees are not all divisible by 2^{j+1}. To prove that $\kappa_{j+1} \subset \mathbb{Q}[x]/R(x^2)$, we check that $R(x^2)$ splits into 2^{j+1} factors over κ_{j+1}, which means that the $\mathbb{Q}$-algebra $\kappa_{j+1} \otimes_{\mathbb{Q}} \big(\mathbb{Q}[x]/R(x^2)\big)$ has 2^{j+1} factors and thus that the minimal polynomial of a primitive element of κ_{j+1} splits completely[16] in $\mathbb{Q}[x]/R(x^2)$.

Although this is the most computation time-demanding part of the certification process, it is quite fast when $r = 1$ (for $\ell = 31$ it merely takes a few minutes on the author's laptop), which occurs for half of the values of

[16] In principle one may directly factor over $\mathbb{Q}[x]/R(x^2)$ the minimal polynomial of a primitive element of κ_{j+1}, but this would involve performing arithmetic in $\mathbb{Q}[x]/R(x^2)$ and in particular to compute an integral basis thereof, which is much slower than working over κ_{j+1}.

ℓ, and for $r = 2$ it remains quite tractable. This is a major improvement compared to the geometric method presented in section 3.5.

(3) For (A3), we simply loop over primes $v \in \mathbb{N}$ and factor the polynomials $F_i(x) \bmod v$ until all the couples $(i, i+1)$ have been dealt with. As explained above, such primes v should not be too hard to come by.

We assume henceforth that (A1), (A2) and (A3) hold, and proceed to the proof of part (i) of Theorem 7. Our proof consists in examining $\mathrm{Gal}(L_i/\mathbb{Q})$ inductively for $i = 1, \ldots, r$. For clarity, we have divided the induction loop into six steps.

Step 1 (The Galois closures are not so large). Since $K_{i+1} = K_i(\sqrt{\delta_i})$, we know that $L_{i+1} = L_i\big(\sqrt{\delta_i^\sigma}, \sigma \in \mathrm{Gal}(L_i/\mathbb{Q})\big)$.

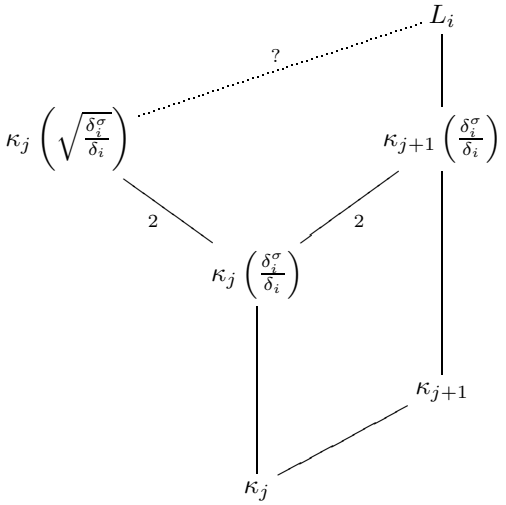
Lemma 9. *Actually, $L_{i+1} = L_i(\sqrt{\delta_i})$ is a nontrivial quadratic extension of L_i.*

Proof. According to (A3), for each i, there exists a rational prime that is totally split in L_i but not in L_{i+1}, which proves that the extension L_{i+1}/L_i is not trivial. Showing that it is quadratic amounts to proving that $\frac{\delta_i^\sigma}{\delta_i}$ is a square in L_i for all $\sigma \in \mathrm{Gal}(L_i/\mathbb{Q})$. To see this, pick a $\sigma \in G_\mathbb{Q}$ such that $\delta_i^\sigma \neq \delta_i$, so that $\mathbb{Q}\big(\frac{\delta_i^\sigma}{\delta_i}\big)$ is isomorphic to $\mathbb{Q}[x]/R(x)$ for some irreducible factor $R(x)$ of $Q_i(x)$ over $\mathbb{Q}$. The polynomial $R(x^2)$ may be reducible, but in any case $\mathbb{Q}\left(\sqrt{\frac{\delta_i^\sigma}{\delta_i}}\right)$ is a factor of the algebra $\mathbb{Q}[x]/R(x^2)$.

We claim that $\kappa_{i+1} \subset L_i$ for all $i < r$. Indeed,

- for $i = 0$ it follows from the fact that $\mathrm{Gal}(L_0/\mathbb{Q}) = \mathrm{PGL}_2(\mathbb{F}_\ell)$ has a quotient of order 2 so that L_0 has a quadratic subfield, which can only be $\kappa_1 = \mathbb{Q}(\sqrt{\ell^*})$ according to (A1),
- for $i = 1$ (which we only need to consider when $r \geqslant 2$), it follows again from (A1) and the fact that we know after one induction loop (cf. Proposition 14) that $\mathrm{Gal}(L_1/\mathbb{Q})$ is isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)/S_1$ and thus has a quotient isomorphic to $\mathbb{Z}/4\mathbb{Z}$ since $r \geqslant 2$,
- and finally, for $i \geqslant 2$, this is the extra hypothesis of Theorem 7 (which we thus only need when $r \geqslant 3$).

Therefore, for $j \leqslant i$ we may then consider the extension diagram



The two extensions marked with a 2 in this diagram are at most quadratic. We may assume that the extension $\kappa_j\left(\sqrt{\frac{\delta_i^\sigma}{\delta_i}}\right)/\kappa_j\left(\frac{\delta_i^\sigma}{\delta_i}\right)$ is not trivial, since the proof that $\sqrt{\frac{\delta_i^\sigma}{\delta_i}} \in L_i$ is over if it is. According to (A2), we may pick j such that $\kappa_{j+1} \subset \mathbb{Q}\left(\sqrt{\frac{\delta_i^\sigma}{\delta_i}}\right)$. But then we must have

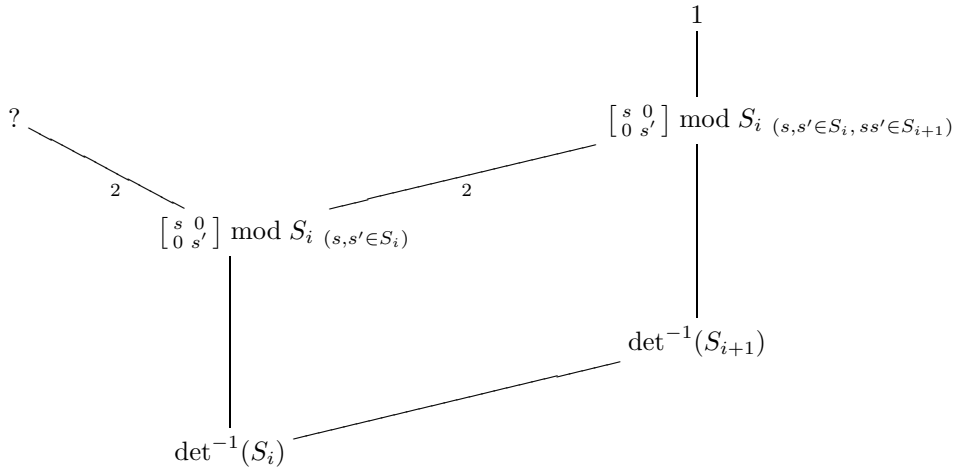
$$\kappa_j\left(\sqrt{\frac{\delta_i^\sigma}{\delta_i}}\right) = \kappa_{j+1}\left(\frac{\delta_i^\sigma}{\delta_i}\right),$$

so that $\sqrt{\frac{\delta_i^\sigma}{\delta_i}} \in L_i$ as claimed. □

As a consequence, $L_{i+1} = L_i(\sqrt{\delta_i})$ and $\mathrm{Gal}(L_{i+1}/\mathbb{Q})$ is an extension of $\mathrm{Gal}(L_i/\mathbb{Q})$ by C_2. This extension is necessarily central, since $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z})$ is trivial.

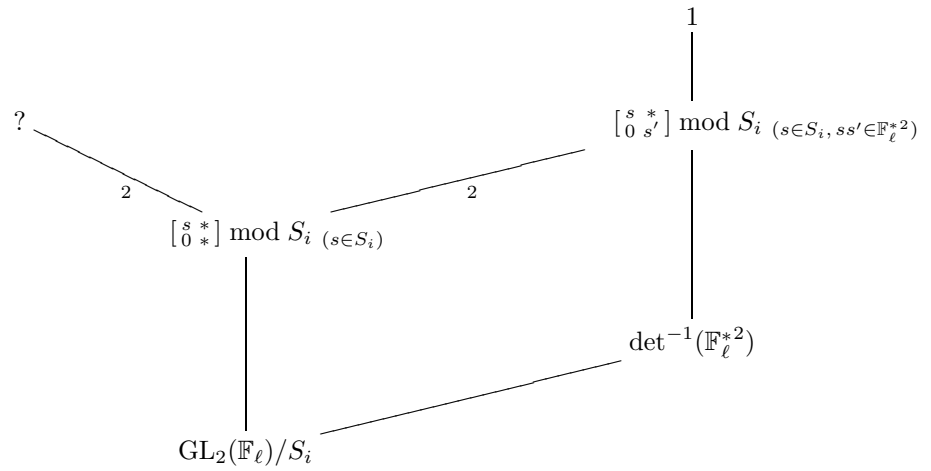
Remark 10. If $F_i(x)$ corresponds to $\mathring{\rho}^{S_i}$ as expected, and if it holds that $K_i = \mathbb{Q}(\delta_i)$ and that $\mathbb{Q}\left(\frac{\delta_i^\sigma}{\delta_i}\right) = \mathbb{Q}(\delta_i, \delta_i^\sigma)$ (which is extremely likely), then we get an indexation of the conjugates of δ_i by V_i, and under the identification of $\mathrm{Gal}(L_i/\mathbb{Q})$ with $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ provided by ρ^{S_i}, the field $\mathbb{Q}\left(\frac{\delta_i^\sigma}{\delta_i}\right)$ corresponds by Galois theory to a conjugate of the subgroup $\{\left[\begin{smallmatrix} s & * \\ 0 & * \end{smallmatrix}\right] \bmod S_i,\ s \in S_i\}$ or $\{\left[\begin{smallmatrix} s & 0 \\ 0 & s' \end{smallmatrix}\right] \bmod S_i,\ s, s' \in S_i\}$ of $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$, depending on whether the vectors indexing δ_i and δ_i^σ are collinear or not. Therefore, we expect $Q_i(x)$ to split over $\mathbb{Q}$ into $2^i - 1$ irreducible factors of degree $2^i(\ell+1)$, corresponding to the nontrivial scalar elements in $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$, plus one large irreducible factor corresponding to nonscalar elements.

Moreover, in the case when the vectors indexing δ_i and δ_i^σ are not collinear, for $j = i$ the Galois subgroup diagram corresponding to the subfield diagram in the above proof would be



But the group $\{\left[\begin{smallmatrix} s & 0 \\ 0 & s' \end{smallmatrix}\right] \bmod S_i,\ s, s' \in S_i\}$ is isomorphic to S_i, hence is cyclic, so the two quadratic extensions of $\mathbb{Q}\left(\frac{\delta_i^\sigma}{\delta_i}\right)$ marked with a 2 in the above diagrams should coincide. We therefore expect (A2) to hold for the large factor $R(x)$ of $Q_i(x)$ with $j = i$.

Similarly, when the vectors indexing δ_i and δ_i^σ are collinear, we get for $j = 0$ the subgroup diagram



and since $\{\left[\begin{smallmatrix} s & * \\ 0 & * \end{smallmatrix}\right] \bmod S_i,\ s \in S_i\} \simeq \mathbb{F}_\ell \rtimes \mathbb{F}_\ell^*$ has only one subgroup of index 2, we expect (A2) to hold for the small factors of $Q_i(x)$ with $j = 0$.

Step 2 (Central 2-cyclic extensions of $\mathrm{PGL}_2(\mathbb{F}_\ell)$). In what follows, for $n \in \mathbb{N}$ we denote by C_n the cyclic group of order n. In order to go on with the proof, we will need to know the classification of the central extensions of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ by C_{2^i}, $i \in \mathbb{N}$.

It is well known (cf. for instance [NSW08, Theorem 1.2.4]) that given a group G and a G-module M, the extensions of G by M such that the conjugation action of lifts of elements of G on M corresponds to the G-module structure on M are classified by the cohomology group $H^2(G, M)$. The class of the cocycle $\beta\colon G \times G \longrightarrow M$ corresponds to the set $M \times G$ endowed with the group law

$$(m, g) \cdot (m', g') = \big(m + g \cdot m' + \beta(g, g'), gg'\big).$$

In particular, the following result is immediate:

Lemma 11. *Consider a (necessarily central) extension*

$$1 \longrightarrow C_2 \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1$$

of a group G by C_2. Let $\beta\colon G \times G \longrightarrow C_2$ be a cocycle representing the corresponding cohomology class, and let $g \in G$ be an element of G of order 2. Then the lifts of g in $\widetilde{G}$ have order 2 if $\beta(g, g)$ is trivial, but have order 4 otherwise.

Furthermore (cf. [Kar87, Theorem 2.1.19]), if the G-action on M is trivial, then there is a split exact sequence of Abelian groups

$$(\star)\quad 0 \longrightarrow \mathrm{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}, M) \overset{\phi}{\hookrightarrow} H^2(G, M) \underset{}{\overset{\psi}{\rightleftarrows}} \mathrm{Hom}\left(\widehat{M}, H^2(G, \mathbb{C}^*)\right) \longrightarrow 0,$$

where $\mathrm{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}, M)$ classifies the Abelian extensions of the abelianised G^{ab} of G by M, $\widehat{M} = \mathrm{Hom}(M, \mathbb{C}^*)$ is the group of complex-valued characters on M, $H^2(G, \mathbb{C}^*)$ (with trivial G-action on $\mathbb{C}^*$) is the so-called *Schur multiplier* of G, and ψ maps

the class of the cocycle $\beta \in H^2(G, M)$ to the *transgression map* (not to be confused with a trace)

$$\begin{array}{rccc} \mathrm{Tra}_\beta\colon & \widehat{M} & \longrightarrow & H^2(G, \mathbb{C}^*) \\ & \chi & \longmapsto & \chi \circ \beta \end{array}$$

associated to the class of β. Moreover, the Schur multiplier $H^2(G, \mathbb{C}^*)$ is trivial if G is cyclic (cf. [Kar87, Proposition 2.1.1.(ii)]), and for each central extension $\widetilde{G}$ of G by M, the subgroup $M \cap D\widetilde{G}$ of $\widetilde{G}$ is isomorphic to the image of Tra_β, where $\beta \in H^2(G, M)$ is the cohomology class corresponding to $\widetilde{G}$, and $D\widetilde{G}$ denotes the commutator subgroup of $\widetilde{G}$ (cf. [Kar87, Proposition 2.1.7]).

Applying this to the group $G = \mathrm{PGL}_2(\mathbb{F}_\ell)$ and the trivial G-module $M = C_{2^i}$ yields the following result (cf. [Que95]):

Theorem 12. *Let $i \geqslant 1$ be an integer.*

(i) *$H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), C_{2^i}\big) \simeq C_2 \times C_2$, so that there are four central extensions of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ by C_{2^i}.*

(ii) *These extensions are:*

- *the trivial extension $C_{2^i} \times \mathrm{PGL}_2(\mathbb{F}_\ell)$, corresponding to the trivial cohomology class $\beta_0 \in H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), C_{2^i}\big)$,*
- *the group $2^i_{\det}\mathrm{PGL}_2(\mathbb{F}_\ell)$, whose class $\beta_{\det} \in H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), C_{2^i}\big)$ is the inflation of the nontrivial element of*

$$H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell)^{\mathrm{ab}}, C_{2^i}\big) \simeq C_2$$

  (in other words, $\beta_{\det}(g, g')$ is nonzero if and only if neither g nor g' lie in $\mathrm{PSL}_2(\mathbb{F}_\ell)$),
- *the group $2^i_-\mathrm{PGL}_2(\mathbb{F}_\ell)$, with class $\beta_- \in H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), C_{2^i}\big)$, defined for $i = 1$ as*

$$2_-\mathrm{PGL}_2(\mathbb{F}_\ell) = \mathrm{SL}_2(\mathbb{F}_\ell) \sqcup \begin{bmatrix} \sqrt{\varepsilon} & 0 \\ 0 & 1/\sqrt{\varepsilon} \end{bmatrix} \mathrm{SL}_2(\mathbb{F}_\ell) \subset \mathrm{SL}_2(\mathbb{F}_{\ell^2}),$$

  where ε denotes a generator of $\mathbb{F}_\ell^*$, and that for $i \geqslant 2$ corresponds to the image of the cohomology class of $2_-\mathrm{PGL}_2(\mathbb{F}_\ell)$ by the map

$$H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), C_2\big) \longrightarrow H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), C_{2^i}\big)$$

  induced by the embedding of C_2 into C_{2^i},
- *and the group $2^i_+\mathrm{PGL}_2(\mathbb{F}_\ell)$, whose associated cohomology class β_+ is the sum in $H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), C_{2^i}\big)$ of $\beta_{\det}$ and of β_-.*

(iii) *Identify C_2 with $\mathbb{Z}/2\mathbb{Z}$, let $g \in \mathrm{PGL}_2(\mathbb{F}_\ell)$ be an element of order 2, and let β_0, $\beta_{\det}$, β_- and β_+ be normalised cocycles (that is to say, $\beta(1, h) = \beta(h, 1) = 0$ for all $h \in \mathrm{PGL}_2(\mathbb{F}_\ell)$) representing the cohomology classes of these four extensions. If $i = 1$, then their value at (g, g) does not depend on the choice of these cocycles, and are:*

- $\beta_0(g, g) = 0$ $\forall g$,
- $\beta_{\det}(g, g) = \begin{cases} 0, & g \in \mathrm{PSL}_2(\mathbb{F}_\ell), \\ 1, & g \notin \mathrm{PSL}_2(\mathbb{F}_\ell), \end{cases}$
- $\beta_-(g, g) = 1$ $\forall g$ *of order* 2,
- $\beta_+(g, g) = \begin{cases} 1, & g \in \mathrm{PSL}_2(\mathbb{F}_\ell), \\ 0, & g \notin \mathrm{PSL}_2(\mathbb{F}_\ell). \end{cases}$

(iv) *For $i \geqslant 2$, the abelianisations of these extensions are:*
- $\big(C_{2^i} \times \mathrm{PGL}_2(\mathbb{F}_\ell)\big)^{\mathrm{ab}} \simeq C_{2^i} \times C_2$,
- $\big(2^i_{\det}\mathrm{PGL}_2(\mathbb{F}_\ell)\big)^{\mathrm{ab}} \simeq C_{2^{i+1}}$,
- $\big(2^i_{-}\mathrm{PGL}_2(\mathbb{F}_\ell)\big)^{\mathrm{ab}} \simeq C_{2^{i-1}} \times C_2$,
- $\big(2^i_{+}\mathrm{PGL}_2(\mathbb{F}_\ell)\big)^{\mathrm{ab}} \simeq C_{2^i}$.

Proof. We shall only give the idea of the proof here, and refer the reader to [Que95, Proposition 2.4 and Lemma 3.2].

(i) On the one hand, the abelianised of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is $\mathrm{PGL}_2(\mathbb{F}_\ell)/\mathrm{PSL}_2(\mathbb{F}_\ell) \simeq C_2$, so that

$$\mathrm{Ext}^1_{\mathbb{Z}}(\mathrm{PGL}_2(\mathbb{F}_\ell)^{\mathrm{ab}}, C_{2^i}) \simeq \mathrm{Ext}^1_{\mathbb{Z}}(C_2, C_{2^i}) \simeq C_2.$$

On the other hand, the Schur multiplier $H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), \mathbb{C}^*\big)$ is isomorphic to C_2 (cf. [Que95, Proposition 2.3]). The result then follows from the split exact sequence $(\star)$.

(ii) Consider again the exact sequence $(\star)$. Then $\beta_{\det}$ lies in the image of ϕ since it is inflated from $\mathrm{PGL}_2(\mathbb{F}_\ell)^{\mathrm{ab}}$. On the other hand, for $i = 1$, β_- does not lie in $\mathrm{Im}\,\phi$, for if it did, then the associated transgression map would be trivial, so that the commutator subgroup of $2_-\mathrm{PGL}_2(\mathbb{F}_\ell)$ would meet the kernel $\pm\left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right]$ of the extension trivially, which is clearly not the case since $\left[\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right]$ is a commutator in $\mathrm{SL}_2(\mathbb{F}_\ell) \subset 2_-\mathrm{PGL}_2(\mathbb{F}_\ell)$. For $i \geqslant 2$, the commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & C_2 & \longrightarrow & 2_-\mathrm{PGL}_2(\mathbb{F}_\ell) & \longrightarrow & \mathrm{PGL}_2(\mathbb{F}_\ell) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & C_{2^i} & \longrightarrow & 2^i_-\mathrm{PGL}_2(\mathbb{F}_\ell) & \longrightarrow & \mathrm{PGL}_2(\mathbb{F}_\ell) & \longrightarrow & 1
\end{array}$$

shows that C_{2^i} still intersects the commutator subgroup of $2^i_-\mathrm{PGL}_2(\mathbb{F}_\ell)$ nontrivially, so that β_- does not lie in $\mathrm{Im}\,\phi$ either. The extensions $2^i_{\det}\mathrm{PGL}_2(\mathbb{F}_\ell)$ and $2^i_-\mathrm{PGL}_2(\mathbb{F}_\ell)$ thus represent different nontrivial cohomology classes in $H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), C_{2^i}\big) \simeq C_2 \times C_2$, hence the result.

(iii) It is a general fact (cf. [Que95, Lemma 3.1] that the image at (g, g) of a normalised cocycle representing an extension of a group G by C_2 only depends on the cohomology class of this cocycle in $H^2(G, C_2)$.
- The case of the trivial extension is obvious since the trivial cohomology class is represented by the trivial cocycle.
- The case of $\beta_{\det}$ follows from its very definition.
- Since it is a subgroup of $\mathrm{SL}_2(\mathbb{F}_{\ell^2})$, the group $2_-\mathrm{PGL}_2(\mathbb{F}_\ell)$ has only one element of order 2, namely the central element $\left[\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right]$. In particular, no element $g \in \mathrm{PGL}_2(\mathbb{F}_\ell)$ of order 2 remains of order 2 when lifted to $2_-\mathrm{PGL}_2(\mathbb{F}_\ell)$, and the result follows from Lemma 11.
- The case of β_+ follows since we may take $\beta_+ = \beta_{\det} + \beta_-$.

(iv) Again, the case of the trivial extension is clear. In the other cases, the result follows from the fact that the intersection of C_{2^i} with the commutator subgroup of the extension is isomorphic to the image of the transgression map

$$\mathrm{Tra}_\beta \colon \widehat{C_{2^i}} \longrightarrow H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), \mathbb{C}^*\big) \simeq C_2,$$

which is trivial in the case of $\beta_{\det}$ and nontrivial in the case of β_- and β_+. □

We shall now use this classification to prove by elimination that $\mathrm{Gal}(L_i/\mathbb{Q})$ is isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ for all i.

Remark 13. The group $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ must be one of the cases presented in Theorem 12, but at this point it is not clear at all which one. We will eventually determine this, cf. Remark 15 below.

Step 3 (The case of L_1/L_0). We first deal with the first extension L_1/L_0 in the quadratic tower $L_r/\cdots/L_0$. The Galois group $\mathrm{Gal}(L_1/\mathbb{Q})$ is a (necessarily central) extension of $\mathrm{Gal}(L_0/\mathbb{Q}) \simeq \mathrm{PGL}_2(\mathbb{F}_\ell)$ by C_2.

Proposition 14. $\mathrm{Gal}(L_1/\mathbb{Q})$ *is isomorphic to* $\mathrm{GL}_2(\mathbb{F}_\ell)/S_1$ *as an extension of* $\mathrm{PGL}_2(\mathbb{F}_\ell)$.

Proof. Let β be a normalised cocycle representing the cohomology class corresponding to the extension $\mathrm{Gal}(L_1/\mathbb{Q})$ of $\mathrm{PGL}_2(\mathbb{F}_\ell)$. According to Theorem 12(ii), $\mathrm{Gal}(L_1/\mathbb{Q})$ is isomorphic either to $C_2 \times \mathrm{PGL}_2(\mathbb{F}_\ell)$, ${}_{2_{\det}}\mathrm{PGL}_2(\mathbb{F}_\ell)$, ${}_{2_-}\mathrm{PGL}_2(\mathbb{F}_\ell)$ or ${}_{2_+}\mathrm{PGL}_2(\mathbb{F}_\ell)$, and β is correspondingly cohomologous to β_0, $\beta_{\det}$, β_- or β_+.

If $\mathrm{Gal}(L_1/\mathbb{Q})$ were the trivial extension $C_2 \times \mathrm{PGL}_2(\mathbb{F}_\ell)$, then L_1 would have a subextension L_1^{ab} with Galois group isomorphic to

$$\big(C_2 \times \mathrm{PGL}_2(\mathbb{F}_\ell)\big)^{\mathrm{ab}} \simeq C_2 \times C_2,$$

and hence three distinct quadratic subfields, which contradicts (A1).

Now let $\tau_1 \in \mathrm{Gal}(L_1/\mathbb{Q})$ be the complex conjugation relative to some embedding of L_1 into $\mathbb{C}$. It induces an element $\tau_0 \in \mathrm{Gal}(L_0/\mathbb{Q})$, which is not the identity since its image by $\rho_{f,\mathfrak{l}}^{\mathrm{proj}}$ is conjugate to $g = \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right] \in \mathrm{PGL}_2(\mathbb{F}_\ell)$. In particular, τ_1 is not trivial either, so it has order 2. Therefore τ_0 has a lift to $\mathrm{Gal}(L_1/\mathbb{Q})$ of order 2, so that $\beta(\tau_0, \tau_0)$ is trivial by Lemma 11. Theorem 12(iii) then only leaves one possibility: if $\ell \equiv 1 \bmod 4$, then $g \in \mathrm{PSL}_2(\mathbb{F}_\ell)$, so that β cannot be cohomologous to β_- nor to β_+ and so $\mathrm{Gal}(L_1/\mathbb{Q})$ must be isomorphic to ${}_{2_{\det}}\mathrm{PGL}_2(\mathbb{F}_\ell)$, whereas if $\ell \equiv -1 \bmod 4$, then $g \notin \mathrm{PSL}_2(\mathbb{F}_\ell)$, so that β cannot be cohomologous to β_- nor to $\beta_{\det}$ and so $\mathrm{Gal}(L_1/\mathbb{Q})$ must be isomorphic to ${}_{2_+}\mathrm{PGL}_2(\mathbb{F}_\ell)$.

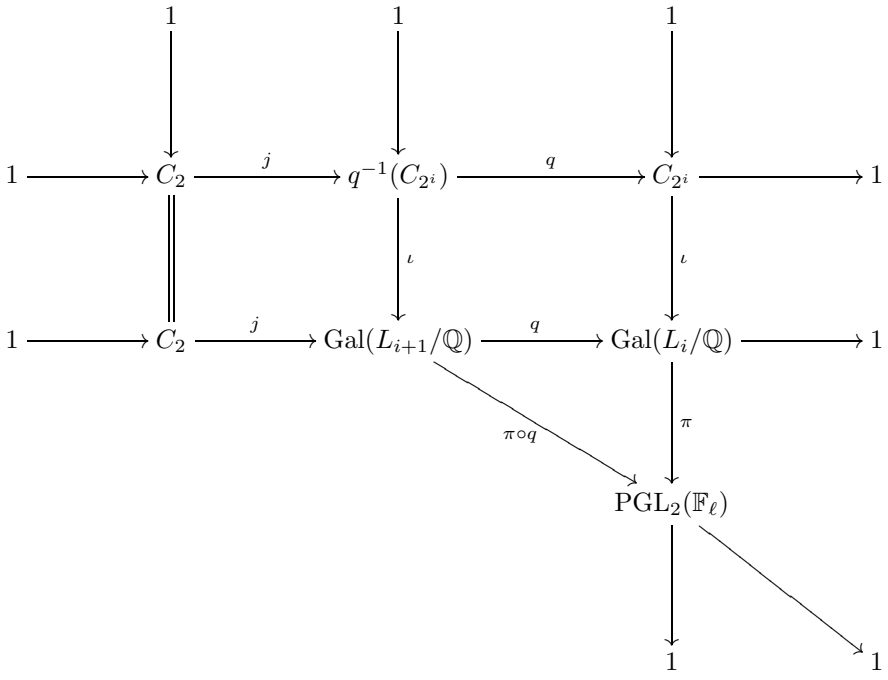
Moreover, $\mathring{L}_1$ is a quadratic extension of $\mathring{L}_0$ and has only one quadratic subfield since its Galois group is isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)/S_1$, so that the same reasoning applies and shows that $\mathrm{Gal}(\mathring{L}_1/\mathbb{Q})$ is isomorphic to ${}_{2_{\det}}\mathrm{PGL}_2(\mathbb{F}_\ell)$ if $\ell \equiv 1 \bmod 4$ and to ${}_{2_+}\mathrm{PGL}_2(\mathbb{F}_\ell)$ if $\ell \equiv 1 \bmod 4$. Either way, we have

$$\mathrm{Gal}(L_1/\mathbb{Q}) \simeq \mathrm{Gal}(\mathring{L}_1/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)/S_1.$$

□

Step 4 ($\mathrm{Gal}(L_i/\mathbb{Q})$ is an extension of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ by C_{2^i}). If $\ell \equiv -1 \bmod 4$, then $r = 1$, so that the proof that $\mathrm{Gal}(L_r/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)/S_r$ is over. We therefore assume that $\ell \equiv 1 \bmod 4$ henceforth until we finish proving part (i) of Theorem 7. We shall first prove by induction on i that $\mathrm{Gal}(L_i/\mathbb{Q})$ is an extension of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ by $\mathbb{F}_\ell^*/S_i \simeq C_{2^i}$, then that this extension is central, and finally that it is isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$. Note that we have just proved above that it is so for $i = 1$.

We first prove that $\mathrm{Gal}(L_i/\mathbb{Q})$ is an extension of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ by C_{2^i}. Let $1 \leqslant i < r$. By the induction hypothesis, we have the commutative diagram



whose middle row and right column are exact. A diagram chase then reveals that the top row and the diagonal short sequence

$$1 \longrightarrow q^{-1}(C_{2^i}) \xrightarrow{\ \iota\ } \mathrm{Gal}(L_{i+1}/\mathbb{Q}) \xrightarrow{\ \pi\circ q\ } \mathrm{PGL}_2(\mathbb{F}_\ell) \longrightarrow 1$$

are exact, so that $\mathrm{Gal}(L_{i+1}/\mathbb{Q})$ is an extension of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ by $q^{-1}(C_{2^i})$, which itself is an extension of C_{2^i} by C_2, which is necessarily central since $\mathrm{Aut}(C_2)$ is trivial.

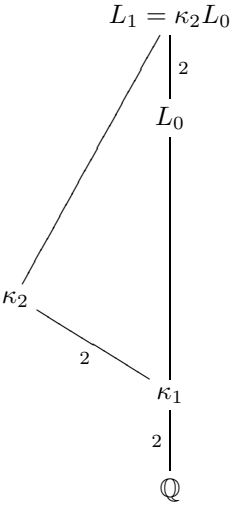
We have $H^2(C_{2^i}, \mathbb{C}^*) = \{0\}$ because C_{2^i} is cyclic, so the extensions of C_{2^i} by C_2 are all Abelian by the exact sequence $(\star)$, so that $q^{-1}(C_{2^i}) = \mathrm{Gal}(L_{i+1}/L_0)$ is isomorphic either to $C_{2^{i+1}}$ or to $C_{2^i} \times C_2$. We shall now prove that the latter is impossible.

Since $\ell \equiv 1 \bmod 4$, the group $S_1^2 = \mathbb{F}_\ell^{*4}$ is a strict subgroup of $S_1 = \mathbb{F}_\ell^{*2}$. The determinant induces a surjective morphism

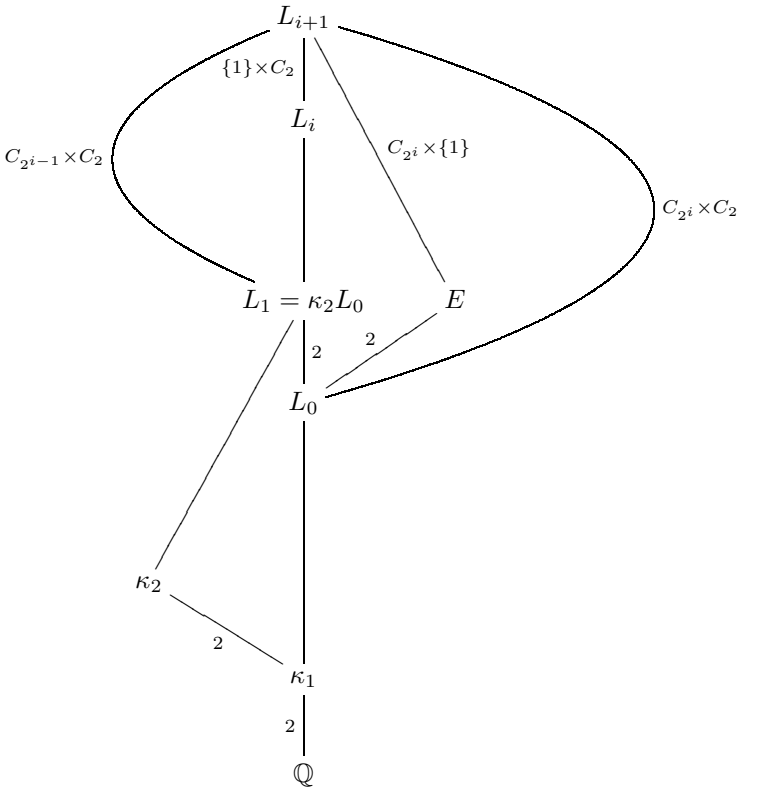
$$\mathrm{Gal}(L_1/\mathbb{Q}) \xrightarrow{\ \sim\ } \mathrm{GL}_2(\mathbb{F}_\ell)/S_1 \xrightarrow{\ \det\ } \mathbb{F}_\ell^*/S_1^2 = \mathbb{F}_\ell^*/{\mathbb{F}_\ell}^{*4} \simeq C_4,$$

so that L_1 has a C_4-subfield, which can only be the field $\kappa_2 \subset \mathbb{Q}(\mu_\ell)$ according to (A1).

Moreover, κ_2 cannot be contained in L_0 because $\mathrm{PGL}_2(\mathbb{F}_\ell)^{\mathrm{ab}} \simeq C_2$, and since κ_2 is a quadratic extension of $\kappa_1 = \mathbb{Q}(\sqrt{\ell^*}) \subset L_0$ and L_1 is a quadratic extension of L_0, we have $L_1 = \kappa_2 L_0$:



Now if $\mathrm{Gal}(L_{i+1}/L_0)$ were isomorphic to $C_{2^i} \times C_2$, then, letting E be the subfield of L_{i+1} fixed by $C_{2^i} \times \{1\}$, we would have the extension tower



where $C_{2^{i-1}}$ denotes the subgroup of C_{2^i} of index 2. The extensions E/L_0 and L_1/L_0 are both quadratic subextensions of L_{i+1}/L_0, but they are distinct since they correspond, respectively, to the distinct subgroups $C_{2^i} \times \{1\}$ and $C_{2^{i-1}} \times C_2$ of $\mathrm{Gal}(L_{i+1}/L_0) = C_{2^i} \times C_2$. On the other hand, the field E is contained in L_{i+1} and thus has only one quadratic subfield according to (A1), so that the same reasoning as in Step 3 above shows that $\mathrm{Gal}(E/\mathbb{Q})$ is isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)/S_1$. But then E has a C_4-subfield, which can only be κ_2, and so $E \supseteq \kappa_2 L_0 = L_1$, hence $E = L_1$ since they are both quadratic extensions of L_0, a contradiction.

This shows that $\mathrm{Gal}(L_{i+1}/L_0)$ cannot be isomorphic to $C_{2^i} \times C_2$, so it must be isomorphic to $C_{2^{i+1}}$. It follows that $\mathrm{Gal}(L_{i+1}/\mathbb{Q})$ is an extension of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ by $\mathrm{Gal}(L_{i+1}/L_0) \simeq C_{2^{i+1}}$, and the induction is complete.

Step 5 ($\mathrm{Gal}(L_i/\mathbb{Q})$ is a *central* extension of $\mathrm{PGL}_2(\mathbb{F}_\ell)$). We shall now prove by induction on i that the extension

$$1 \longrightarrow C_{2^i} \longrightarrow \mathrm{Gal}(L_i/\mathbb{Q}) \longrightarrow \mathrm{PGL}_2(\mathbb{F}_\ell) \longrightarrow 1$$

is central. Note that it is so for $i = 1$ since $\mathrm{Aut}(C_2)$ is trivial.

Let $i \geqslant 2$, and assume on the contrary that this extension is not central. Since $\mathrm{Aut}(C_{2^i}) \simeq C_2 \times C_{2^{i-2}}$ is Abelian, the morphism $\mathrm{PGL}_2(\mathbb{F}_\ell) \longrightarrow \mathrm{Aut}(C_{2^i})$ expressing the conjugation action of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ on C_{2^i} factors through

$$\mathrm{PGL}_2(\mathbb{F}_\ell)^{\mathrm{ab}} = \mathrm{PGL}_2(\mathbb{F}_\ell)/\mathrm{PSL}_2(\mathbb{F}_\ell) \simeq C_2,$$

so that $\mathrm{PSL}_2(\mathbb{F}_\ell)$ acts trivially whereas there exists an involution ϕ of C_{2^i} such that $gxg^{-1} = \phi(x)$ for all $g \in \mathrm{PGL}_2(\mathbb{F}_\ell) - \mathrm{PSL}_2(\mathbb{F}_\ell)$ and $x \in C_{2^i}$. If we identify C_{2^i} with $\mathbb{Z}/2^i\mathbb{Z}$, then by induction hypothesis this involution induces the identity on $\mathbb{Z}/2^{i-1}\mathbb{Z}$, so it must be $x \mapsto (1 + 2^{i-1})x$.

There is thus only one possible nontrivial conjugation action of $\mathrm{PGL}_2(\mathbb{F}_\ell)$. In order to compute $H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), C_{2^i}\big)$ for this nontrivial action, we use the inflation-restriction exact sequence (cf. [Ser79, Proposition VII.6.5])

$$(\dagger) \qquad 0 \longrightarrow H^2(C_2, C_{2^i}) \xrightarrow{\mathrm{Inf}} H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), C_{2^i}\big) \xrightarrow{\mathrm{Res}} H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell), C_{2^i}\big).$$

This is legitimate since, as $\mathrm{PSL}_2(\mathbb{F}_\ell)$ acts trivially, we have

$$H^1\big(\mathrm{PSL}_2(\mathbb{F}_\ell), C_{2^i}\big) = \mathrm{Hom}\big(\mathrm{PSL}_2(\mathbb{F}_\ell), C_{2^i}\big) = 0$$

since $\mathrm{PSL}_2(\mathbb{F}_\ell)$ is simple.

On the one hand, since $C_2 = \{1, \varepsilon\}$ is cyclic, the groups $H^q(C_2, M)$ are the cohomology groups of the complex

$$0 \longrightarrow M \xrightarrow{\varepsilon - 1} M \xrightarrow{\varepsilon + 1} M \xrightarrow{\varepsilon - 1} M \xrightarrow{\varepsilon + 1} \cdots$$

for any C_2-module M (cf. [Lan02, Chapter XX, Exercise 16]). In particular,

$$H^2(C_2, C_{2^i}) = \frac{\ker(\varepsilon - 1)}{\mathrm{Im}(\varepsilon + 1)} = \frac{(\mathbb{Z}/2^i\mathbb{Z})[2^{i-1}]}{(2 + 2^{i-1})(\mathbb{Z}/2^i\mathbb{Z})} \simeq \begin{cases} C_2, & i = 2, \\ 0, & i \geqslant 3. \end{cases}$$

On the other hand, as $\mathrm{PSL}_2(\mathbb{F}_\ell)$ acts trivially, the group $H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell), C_{2^i}\big)$ can be computed by using the split exact sequence $(\star)$. As $\mathrm{PSL}_2(\mathbb{F}_\ell)^{\mathrm{ab}} = \{1\}$ since $\mathrm{PSL}_2(\mathbb{F}_\ell)$ is simple, and as the Schur multiplier is

$$H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell), \mathbb{C}^*\big) \simeq C_2$$

(Steinberg, cf. [Kar87, Theorem 7.1.1.(ii)]), it follows that

$$H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell), C_{2^i}\big) \simeq C_2.$$

Let $2^i\mathrm{PSL}_2(\mathbb{F}_\ell)$ denote the nontrivial extension. One has

$$2\mathrm{PSL}_2(\mathbb{F}_\ell) \simeq \mathrm{SL}_2(\mathbb{F}_\ell),$$

and the nontrivial element of $H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell), C_{2^i}\big)$ is the image of the nontrivial element $\gamma_{\mathrm{SL}_2} \in H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell), C_2\big)$ corresponding to $\mathrm{SL}_2(\mathbb{F}_\ell)$ by the map

$$H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell), C_2\big) \longrightarrow H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell), C_{2^i}\big)$$

induced by the embedding of C_2 into C_{2^i}.

Consider the inflation-restriction exact sequence (†), and let

$$\beta \in H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), C_{2^i}\big)$$

be the cohomology class corresponding to the extension

$$1 \longrightarrow C_{2^i} \longrightarrow \mathrm{Gal}(L_i/\mathbb{Q}) \longrightarrow \mathrm{PGL}_2(\mathbb{F}_\ell) \longrightarrow 1.$$

If $\gamma = \mathrm{Res}\,\beta \in H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell), C_{2^i}\big)$ were trivial, then $\beta = \mathrm{Inf}\,\alpha$ would be the inflation of some $\alpha \in H^2\big(C_2, C_{2^i}\big)$, so that $\mathrm{Gal}(L_i/\mathbb{Q})$ would be isomorphic to the fibred product $G_\alpha \underset{C_2}{\times} \mathrm{PGL}_2(\mathbb{F}_\ell)$, where G_α is the group extension

$$1 \longrightarrow C_{2^i} \longrightarrow G_\alpha \longrightarrow C_2 \longrightarrow 1$$

corresponding to α. Actually, if $i \geqslant 3$, then $\beta = \mathrm{Inf}\,\alpha$ would be trivial since $H^2\big(C_2, C_{2^i}\big) = 0$, so that $\mathrm{Gal}(L_i/\mathbb{Q})$ would be isomorphic to the semidirect product

$$C_{2^i} \rtimes \mathrm{PGL}_2(\mathbb{F}_\ell),$$

whereas if $i = 2$, then $H^2\big(C_2, C_{2^i}\big) \simeq C_2$, so that $\mathrm{Gal}(L_2/\mathbb{Q})$ would be isomorphic either to $C_4 \rtimes \mathrm{PGL}_2(\mathbb{F}_\ell)$ or to $Q_8 \underset{C_2}{\times} \mathrm{PGL}_2(\mathbb{F}_\ell)$, where Q_8, the quaternionic group $\{\pm 1, \pm i, \pm j, \pm k\}$, is the extension

$$1 \longrightarrow C_4 \longrightarrow Q_8 \longrightarrow C_2 \longrightarrow 1$$

corresponding to the nontrivial element of $H^2(C_2, C_4)$. However, the abelianisations

$$\Big(C_{2^i} \rtimes \mathrm{PGL}_2(\mathbb{F}_\ell)\Big)^{\mathrm{ab}} \simeq C_{2^{i-1}} \times C_2$$

and

$$\big(Q_8 \underset{C_2}{\times} \mathrm{PGL}_2(\mathbb{F}_\ell)\big)^{\mathrm{ab}} \simeq C_2 \times C_2$$

contradict (A1).

It follows that $\gamma = \mathrm{Res}\,\beta \in H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell), C_{2^i}\big)$ cannot be trivial, so it must be $\gamma_{\mathrm{SL}_2} \in H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell), C_2\big)$ followed by the embedding of C_2 into C_{2^i}. Let $g = \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right] \in \mathrm{PGL}_2(\mathbb{F}_\ell)$. As $\ell \equiv 1 \bmod 4$, g lies in $\mathrm{PSL}_2(\mathbb{F}_\ell)$, and since the only element of order 2 of $\mathrm{SL}_2(\mathbb{F}_\ell)$ is $\left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$, g cannot be lifted to an element of order 2 of $\mathrm{SL}_2(\mathbb{F}_\ell)$, so that $\gamma_{\mathrm{SL}_2}(g, g) \neq 0$ by Lemma 11. On the other hand, since g is the image of the complex conjugation (with respect to some embedding of L_0 into $\mathbb{C}$) by the projective Galois representation ρ^{proj}, it must lift to an element of order 2 of $\mathrm{Gal}(L_i/\mathbb{Q})$, which is contradictory: in the extension $\mathrm{Gal}(L_i/\mathbb{Q})$, seen as the set $\mathbb{Z}/2^i\mathbb{Z} \times \mathrm{PGL}_2(\mathbb{F}_\ell)$ endowed with the group law

$$(x_1, g_1) \cdot (x_2, g_2) = \big(x_1 + g_1 \cdot x_2 + \beta(g_1, g_2), g_1 g_2\big),$$

we compute that

$$(x, g) \cdot (x, g) = \big(x + g \cdot x + \beta(g, g), g^2\big) = \big(\beta(g, g), 1\big)$$

as $g \in \mathrm{PSL}_2(\mathbb{F}_\ell)$ acts trivially, so $\beta(g,g)$ must be zero, but $\beta(g,g) = \gamma_{\mathrm{SL}_2}(g,g) \neq 0$ since $g \in \mathrm{PSL}_2(\mathbb{F}_\ell)$.

It is therefore impossible that the extension

$$1 \longrightarrow C_{2^i} \longrightarrow \mathrm{Gal}(L_i/\mathbb{Q}) \longrightarrow \mathrm{PGL}_2(\mathbb{F}_\ell) \longrightarrow 1$$

be not central, which completes the induction.

Step 6 ($\mathrm{Gal}(L_i/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)/S_i$). We may now again apply Theorem 12 to $\mathrm{Gal}(L_r/\mathbb{Q})$. Part (iv) of this theorem combined with (A1) means that $\mathrm{Gal}(L_r/\mathbb{Q})$ cannot be isomorphic to $C_{2^r} \times \mathrm{PGL}_2(\mathbb{F}_\ell)$ nor to $2^r_- \mathrm{PGL}_2(\mathbb{F}_\ell)$. It cannot be isomorphic to $2^r_{\det}\mathrm{PGL}_2(\mathbb{F}_\ell)$ either, otherwise L_r would have a $C_{2^{r+1}}$-subfield by part (iv) of Theorem 12, which would be contained in the cyclotomic extension $\mathbb{Q}(\mu_\ell)$ according to (A1), but this would contradict the definition of r. Therefore, $\mathrm{Gal}(L_r/\mathbb{Q})$ must be isomorphic to $2^r_+\mathrm{PGL}_2(\mathbb{F}_\ell)$.

Moreover, the same reasoning applies to $\mathring{L}_r$, whose Galois group is isomorphic $\mathrm{GL}_2(\mathbb{F}_\ell)/S_r$ since $\det \mathring{\rho}$ is by assumption an odd power of the mod ℓ cyclotomic character. Therefore, we have

$$\mathrm{Gal}(L_r/\mathbb{Q}) \simeq 2^r_+\mathrm{PGL}_2(\mathbb{F}_\ell) \simeq \mathrm{Gal}(\mathring{L}_r/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)/S_r,$$

and the proof of part (i) of Theorem 7 is now complete.

Remark 15. We can now go back down the quadratic tower $L_r/\cdots/L_0$ and see that $\mathrm{Gal}(L_i/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ for all i. Moreover, it is easy to see that the abelianisation of $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ is

$$\det\colon \mathrm{GL}_2(\mathbb{F}_\ell)/S_i \longrightarrow \mathbb{F}_\ell^*/S_i^2,$$

and since $S_i^2 = S_{i+1} \subsetneq S_i$ for $i < r$ whereas $S_r^2 = S_r$ as $-1 \notin S_r$, Theorem 12 part (iv) leads to the unified formula

$$\mathrm{Gal}(L_i/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)/S_i \simeq \begin{cases} \mathrm{PGL}_2(\mathbb{F}_\ell), & i = 0, \\ 2^i_{\det}\mathrm{PGL}_2(\mathbb{F}_\ell), & 0 < i < r, \\ 2^r_+\mathrm{PGL}_2(\mathbb{F}_\ell), & i = r, \end{cases}$$

which is valid for $\ell \equiv 1 \bmod 4$ as well as $\ell \equiv -1 \bmod 4$. This allows us to identify for each i the extension $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ amongst the ones listed in part (ii) of Theorem 12.

3.6.2. *Certification of the Galois action.* At this point, we have proved that $\mathrm{Gal}(L_i/\mathbb{Q})$ is abstractly isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ for each $0 \leqslant i \leqslant r$, but only for $i = 0$ do we know that it is permutation-isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ acting naturally on $V_i = V/S_i$. For each $i > 0$, we will now determine an isomorphism between $\mathrm{Gal}(L_i/\mathbb{Q})$ and $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ and a bijection $\theta_i\colon Z_i \xrightarrow{\sim} V_i$ which make the Galois action on Z_i permutation-isomorphic to the natural action of $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ on V_i in a compatible way as i varies. This data can then be used to compute the Dokchitsers' resolvents $\Gamma_C(x)$, and thus to compute trace of Frobenius elements, in a certified way.

Let us first fix an isomorphism φ_r from the $\mathrm{Gal}(L_r/\mathbb{Q})$ to $\mathrm{GL}_2(\mathbb{F}_\ell)/S_r$. Since the Galois groups $\mathrm{Gal}(L_i/\mathbb{Q})$ are isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ as extensions of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ in a compatible way, φ_r induces a system of isomorphisms

$$\big(\varphi_i\colon \mathrm{Gal}(L_i/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)/S_i\big)_{0 \leqslant i \leqslant r}$$

such that the following diagram commutes:

$$\begin{array}{ccccccccc}
\mathrm{Gal}(L_r/\mathbb{Q}) & \twoheadrightarrow \cdots \twoheadrightarrow & \mathrm{Gal}(L_{i+1}/\mathbb{Q}) & \twoheadrightarrow & \mathrm{Gal}(L_i/\mathbb{Q}) & \twoheadrightarrow \cdots \twoheadrightarrow & \mathrm{Gal}(L_0/\mathbb{Q}) \\
\downarrow{\scriptstyle \varphi_r}\wr & & \downarrow{\scriptstyle \varphi_{i+1}}\wr & & \downarrow{\scriptstyle \varphi_i}\wr & & \downarrow{\scriptstyle \varphi_0}\wr \\
\mathrm{GL}_2(\mathbb{F}_\ell)/S_r & \twoheadrightarrow \cdots \twoheadrightarrow & \mathrm{GL}_2(\mathbb{F}_\ell)/S_{i+1} & \twoheadrightarrow & \mathrm{GL}_2(\mathbb{F}_\ell)/S_i & \twoheadrightarrow \cdots \twoheadrightarrow & \mathrm{PGL}_2(\mathbb{F}_\ell)
\end{array}$$

We choose φ_r such that the induced isomorphism

$$\varphi_0 \colon \mathrm{Gal}(L_0/\mathbb{Q}) \simeq \mathrm{PGL}_2(\mathbb{F}_\ell)$$

agrees with the one we determined with the help of [Magma] in section 3.3.1, and we will use the isomorphisms φ_i to identify $\mathrm{Gal}(L_i/\mathbb{Q})$ with $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ from now on.

Since, by section 3.3.1, the action of $\mathrm{Gal}(L_0/\mathbb{Q})$ on Z_0 is equivalent to the natural action of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ on $\mathbb{P}^1(\mathbb{F}_\ell)$, we know that the stabiliser of a root of $F_0(x)$ is conjugate to a group of upper triangular matrices in $\mathrm{PGL}_2(\mathbb{F}_\ell)$. Therefore, the stabiliser of a root of $F_1(x)$ is a subgroup of index 2 of the subgroup of upper triangular matrices in $\mathrm{GL}_2(\mathbb{F}_\ell)/S_1$.

Lemma 16. *Let B be a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ of the form*

$$B = \left\{ \left[\begin{smallmatrix} s & x \\ 0 & s' \end{smallmatrix}\right] \;\middle|\; s \in S, s' \in S', x \in \mathbb{F}_\ell \right\},$$

where $S, S' \leqslant \mathbb{F}_\ell^*$ are subgroups of the multiplicative group of $\mathbb{F}_\ell$. If neither S nor S' is reduced to $\{1\}$, then B has exactly 3 subgroups of index 2, namely

$$\left\{ \left[\begin{smallmatrix} s & x \\ 0 & s' \end{smallmatrix}\right] \;\middle|\; s \in S^2 \right\},$$
$$\left\{ \left[\begin{smallmatrix} s & x \\ 0 & s' \end{smallmatrix}\right] \;\middle|\; s' \in S'^2 \right\},$$
$$\text{and } \left\{ \left[\begin{smallmatrix} s & x \\ 0 & s' \end{smallmatrix}\right] \;\middle|\; s \in S^2 \Leftrightarrow s' \in S'^2 \right\},$$

where we write S^2 for $\{s^2, s \in S\}$, and similarly for S'^2.

Proof. Since a subgroup of index 2 is always normal, such a subgroup is the kernel of a nontrivial morphism from B to C_2. As the latter group is Abelian, such a morphism factors through the abelianisation of B. Let $s \in S$, $s \neq 1$. The identity $ghg^{-1}h^{-1} = \left[\begin{smallmatrix} 1 & 1-s \\ 0 & 1 \end{smallmatrix}\right]$ where $g = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$, $h = \left[\begin{smallmatrix} s & 0 \\ 0 & 1 \end{smallmatrix}\right] \in B$ shows that $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ lies in the commutator subgroup of B, so that the abelinanisation of B is

$$\begin{array}{ccc} B & \longrightarrow & S \times S' \\ \left[\begin{smallmatrix} s & x \\ 0 & s' \end{smallmatrix}\right] & \longmapsto & (s, s'). \end{array}$$

Therefore, we have canonically

$$\mathrm{Hom}(B, C_2) \simeq \mathrm{Hom}(S \times S', C_2) \simeq \mathrm{Hom}(S, C_2) \times \mathrm{Hom}(S', C_2).$$

Since S and S' are cyclic because $\mathbb{F}_\ell^*$ is, the result follows. □

According to this lemma, the stabiliser of a root of $F_1(x)$ in $\mathrm{Gal}(L_1/\mathbb{Q})$ could be either

$$H_+ = \left\{ \left[\begin{smallmatrix} s & x \\ 0 & s' \end{smallmatrix}\right] \;\middle|\; s \in \mathbb{F}_\ell^{*2}, s' \in \mathbb{F}_\ell^*, x \in \mathbb{F}_\ell \right\} / S_1,$$
$$H_- = \left\{ \left[\begin{smallmatrix} s & x \\ 0 & s' \end{smallmatrix}\right] \;\middle|\; s \in \mathbb{F}_\ell^*, s' \in \mathbb{F}_\ell^{*2}, x \in \mathbb{F}_\ell \right\} / S_1,$$
$$\text{or } H_0 = \left\{ \left[\begin{smallmatrix} s & x \\ 0 & s' \end{smallmatrix}\right] \;\middle|\; s, s' \in \mathbb{F}_\ell^*, x \in \mathbb{F}_\ell, ss' \in \mathbb{F}_\ell^{*2} \right\} / S_1.$$

However, the nontrivial element $\left[\begin{smallmatrix}\varepsilon & 0\\ 0 & \varepsilon\end{smallmatrix}\right] \in \mathrm{GL}_2(\mathbb{F}_\ell)/S_1$, where $\varepsilon \in \mathbb{F}_\ell^*/{\mathbb{F}_\ell^*}^2$, is central and lies in H_0, so it lies in the intersection of the conjugates of H_0, so that the action of $\mathrm{GL}_2(\mathbb{F}_\ell)/S_1$ on its H_0-cosets is not faithful. Therefore, the stabiliser of a root of $F_1(x)$ must be conjugate either to H_+ or to H_-.

Consider now the compatible collection of involutory automorphisms

$$\begin{array}{rccc} \Psi_i\colon & \mathrm{GL}_2(\mathbb{F}_\ell)/S_i & \longrightarrow & \mathrm{GL}_2(\mathbb{F}_\ell)/S_i \\ & A & \longmapsto & \frac{1}{\det A}A. \end{array}$$

Since Ψ_0 is the identity on $\mathrm{PGL}_2(\mathbb{F}_\ell)$, we may replace the isomorphisms φ_i with $\Psi_i \circ \varphi_i$ without breaking the compatibility with the identification of $\mathrm{Gal}(L_0/\mathbb{Q})$ with $\mathrm{PGL}_2(\mathbb{F}_\ell)$ made in section 3.3.1, and since Ψ_1 swaps H_+ and H_-, we may assume without loss of generality that the stabiliser of a root of $F_1(x)$ is conjugate to H_+.

An induction on i then reveals that the stabiliser in $\mathrm{Gal}(L_i/\mathbb{Q})$ of a root of $F_i(x)$ is conjugate to

$$\left\{\left[\begin{smallmatrix} s & x \\ 0 & y\end{smallmatrix}\right] \;\middle|\; s \in S_i, y \in \mathbb{F}_\ell^*, x \in \mathbb{F}_\ell\right\}/S_i.$$

Indeed, at each step of the induction, Lemma 16 gives us 3 possibilities, but only one of them yields a faithful action of $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ on its cosets, for the same reason as above.

As a consequence, we now know that for each i there exists a bijection

$$\theta_i\colon Z_i \xrightarrow{\sim} V_i$$

which makes the Galois action on Z_i equivalent to the natural action of $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ on V_i, so we have proved part (ii) of Theorem 7. However, we must make the indexation θ_r of Z_r by V_r explicit, so as to be able to proceed with the computation of the Dokchitsers' resolvents $\Gamma_C(x)$. We do so as follows.

3.6.3. *Recovering the indexation of the p-adic roots.* Recall that we have fixed a large prime $p \in \mathbb{N}$ such that $F_r(x) \bmod p$ is irreducible. Consider the field $\overline{K}_r = \mathbb{F}_p[t]/F_r(t)$. The t^{p^j}, $0 \leqslant j < 2^r(\ell+1)$, are the roots of F_r in $\overline{K}_r$, and so by the hypothesis we have made on the relation between the roots of $F_i(x)$ and the ones of $F_{i+1}(x)$, all the polynomials $F_i(x)$ are squarefree and split completely over $\overline{K}_r$. Let $\overline{Z}_i$ be the set of the roots of $F_i(x)$ in $\overline{K}_r$, so that we have[17] 2-to-1 projection maps $\overline{\varpi}_i\colon \overline{Z}_{i+1} \twoheadrightarrow \overline{Z}_i$ such that for all $z \in \overline{Z}_{i+1}$, there exists a unique $z' \in \overline{Z}_{i+1}$ such that $z + z' = \overline{\varpi}_i(z) \in \overline{Z}_i$.

In section 3.3.1, [Magma] computed for us the Galois group $\mathrm{Gal}(L_0/\mathbb{Q})$ as a permutation group on the roots of $F_0(x)$ in some extension M of $\mathbb{F}_p$, which unfortunately is not isomorphic[18] to $\overline{K}_r$. Magma also gave us an indexation $(m_P)_{P\in\mathbb{P}^1(\mathbb{F}_\ell)}$ of these roots, and we would like to transfer this indexation to $\overline{Z}_0 \subset \overline{K}_r$ while keeping compatibility with the action of $\mathrm{Gal}(L_0/\mathbb{Q}) = \mathrm{PGL}_2(\mathbb{F}_\ell)$. We do so by

[17] Although we certainly have such projections maps in characteristic zero, it might happen that these maps are no longer well-defined in characteristic p. However, as p is large, this problem should not occur for us.

[18] Indeed, unlike $\overline{K}_r$, M is an extension of $\mathbb{F}_p$ of degree $\ell+1 = \deg F_0(x)$. To make things worse, curiously Magma does not construct M as $\mathbb{F}_p[t]/F_0(t)$ but as $\mathbb{F}_p[t]/G(t)$ instead, where $G(t)$ is a sparse polynomial of degree $\ell+1$ which it cooks up.

computing mod p the factors

$$R_{4,P}(x) = \prod_{\substack{P_1,P_2,P_3,P_4 \in \mathbb{P}^1(\mathbb{F}_\ell) \\ \text{pairwise distinct} \\ [P_1,P_2,P_3,P_4]=P}} \left(x - \sum_{i=1}^{4} \lambda_i m_{P_i} \right) \in \mathbb{F}_p[x]$$

of the resolvent $R_4(x)$ from section 3.3.1 for each $P \in \mathbb{P}^1(\mathbb{F}_\ell) - \{\infty, 0, 1\}$, where $[\cdot,\cdot,\cdot,\cdot]$ denotes the cross-ratio and the $(\lambda_i)_{1\leqslant i\leqslant 4}$ are fixed distinct integers chosen so that these polynomials are pairwise coprime mod p. Although we did mention that the resolvent $R_4(x)$ is horribly expensive to compute, computing these factors is much easier, for three reasons: they are merely factors and so their degree is much smaller, we compute them mod p so the size of their coefficients is no longer a problem, and now we know that $\mathrm{Gal}(L_0/\mathbb{Q}) = \mathrm{PGL}_2(\mathbb{F}_\ell)$, it is rigorous to compute them by expanding the product that defines them instead of using resultants.

Then, since the action of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ on $\mathbb{P}^1(\mathbb{F}_\ell)$ is 3-transitive, we may index 3 distinct arbitrarily chosen points z_∞, z_0 and z_1 of $\overline{Z}_0$, respectively, by ∞, 0 and 1, after which we index each remaining point $z \in \overline{Z}_0$ by the unique $P \in \mathbb{P}^1(\mathbb{F}_\ell)$ such that

$$R_P(\lambda_1 z_\infty + \lambda_2 z_0 + \lambda_3 z_1 + \lambda_4 z) = 0.$$

Next, by looking at how the Frobenius of $\overline{K}_r$ permutes $\overline{Z}_0$, we may deduce which element $\overline{\Phi} \in \mathrm{PGL}_2(\mathbb{F}_\ell)$ it corresponds to.

Now let $z = z^{(r)} \in \overline{Z}_r$ be a fixed root of $F_r(x)$ in $\overline{K}_r$. By finding which other point of $\overline{Z}_r$ must be added to it to get a root $z^{(r-1)}$ of $F_{r-1}(x)$ mod p, then which point of $\overline{Z}_{r-1}$ must be added to this new root to get a root $z^{(r-2)}$ of $F_{r-2}(x)$ mod p, and so on until we get to $z^{(0)} \in \overline{Z}_0$, we can determine which point P of $\mathbb{P}^1(\mathbb{F}_\ell)$ corresponds to z. We index this z by a vector v of V_r whose reduction to $\mathbb{P}^1(\mathbb{F}_\ell)$ is P.

Now that we have indexed one root of $F_r(x)$, we index the other ones as follows: Let Φ be an arbitrary lift of $\overline{\Phi} \in \mathrm{PGL}_2(\mathbb{F}_\ell)$ to $\mathrm{GL}_2(\mathbb{F}_\ell)/S_r$. We know that the Frobenius of $\overline{K}_r$ acts as $\lambda\Phi$ for some $\lambda \in \mathbb{F}_\ell^*/S_r$. If we knew the value of λ, we would be able to complete the indexation of $\overline{Z}_r$ by V_r, since z^{p^j} must be indexed by $(\lambda\Phi)^j v$ for all $j < 2^r(\ell+1)$. Each value of λ thus corresponds to a candidate indexation of $\overline{Z}_r$ by V_r. In order to find out which is the correct one, we use the Dokchitsers' resolvents $\Gamma_C(x)$, albeit in an unusual way: we lift the elements of $\overline{Z}_r$ to some moderate p-adic precision in $\mathbb{Q}_p[t]/F_r(t)$, and we compute one coefficient of one of the resolvents $\Gamma_C(x)$ for each of these candidate indexations. The point is that we expect the correct indexation to yield a nice value, and the other ones to yield rubbish. Curiously, the wrong indexations yield values which are still rational over[19] $\mathbb{Q}_p$; however, in practice they will contradict archimedian bounds which can be derived from the modulus of the complex roots of $F_r(x)$, and so we can rigorously tell the right indexation apart from the wrong ones.

Remark 17. Let $\Gamma_C(x) = \prod_{\sigma\in C} \left(x - \sum_{z\in Z_r} \sigma(z)h(z)\right)$ be the resolvent whose coefficient we compute, where $h(x) \in \mathbb{Z}[x]$ and C is a conjugacy class, and let $n = \#C$ be its degree. Clearly, the coefficients of x^n, of x^{n-1} and of x^0 do not depend on the indexation and therefore give no information. Moreover, in practice the height of the coefficient of x^{n-i} is a roughly increasing function of i, so a good choice is

[19]This fact can be proved by a painful computation which we do not reproduce here.

to compute the coefficient of x^{n-2}, which can be done quickly by expanding the product to order 2 at infinity.

Remark 18. If r is large, it may be better to determine the image of the Frobenius in $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ inductively on $i = 1, \ldots, r$, since this reduces the number of trials to perform from 2^r to $2r$. On the other hand, in practice r is small (recall that $2^r < \ell$), so one may parallelise and treat all of the 2^r cases at once if one has enough cores to spare.

Remark 19. If we have some information about the trace or the determinant of the image by ρ of the Frobenius at p, we can make a partial prediction on which indexation is the correct one. However, we have not proved yet that the Galois set Z_r affords $\mathring{\rho}^{S_r}$ and not another Galois representation, so to be rigorous we must try out all the possibilities.

Once we know the correct indexation of $\overline{Z}_r$, we may compute the Dokchitsers' resolvents $\Gamma_C(x)$ by lifting p-adically the roots into Z_r. Indeed, we can deduce a bound on the necessary p-adic precision from archimedian bounds as above. We thus get a completely proved output.

3.7. **Certification of the representation.** Either by the geometric approach (section 3.5) or by the group cohomology one (section 3.6), we have now certified that the Galois action on the set Z_r of roots of $F_r(x)$ affords a quotient Galois representation ρ^{S_r}, for which we are able to compute the image of the Frobenius element at v for almost every prime $v \in \mathbb{N}$ thanks to the Dokchitsers' resolvents $\Gamma_C(x)$. We are now going to explain how to certify that this representation ρ^{S_r} is equivalent to the expected representation $\mathring{\rho}^{S_r}$.

By assumption, ρ^{S_r} and $\mathring{\rho}^{S_r}$ induce the same projective representation, so there exists a Galois character

$$\psi\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbb{F}_\ell^*/S_r \simeq \mathbb{Z}/2^r\mathbb{Z}$$

such that $\rho^{S_r} = \mathring{\rho}^{S_r} \otimes \psi$. Let $(p_j)_{j\in J}$ be the primes at which K_r ramifies. Since we expect ρ^{S_r} to be equivalent to $\mathring{\rho}^{S_r}$, these should be the same primes as the (known) ones at which $\mathring{\rho}^{S_r}$ ramifies, and we assume that it is indeed the case. For each $j \in J$, let

$$a_j = \begin{cases} r+2 & \text{if } p_j = 2, \\ 1 & \text{else,} \end{cases}$$

so that $\mathbb{Z}_{p_j}^* \otimes \mathbb{Z}/2^r\mathbb{Z} \simeq (\mathbb{Z}/p_j^{a_j}\mathbb{Z})^* \otimes \mathbb{Z}/2^r\mathbb{Z}$ for all $j \in J$. Since ψ is unramified outside the p_j and assumes values in $\mathbb{Z}/2^r\mathbb{Z}$, it factors through $\mathrm{Gal}\left(\mathbb{Q}(\mu_N)/\mathbb{Q}\right)$, where $N = \prod_{j\in J} p_j^{a_j}$.

It then suffices to find primes $v \in \mathbb{N}$:

- which span $(\mathbb{Z}/N\mathbb{Z})^* \otimes \mathbb{Z}/2^r\mathbb{Z}$,
- for which the Dokchitser resolvents can[20] determine the trace in $\mathbb{F}_\ell/S_r$ of the image by ρ^{S_r} of the Frobenius at v,
- such that this trace is nonzero,
- and which are small enough so that we can determine the trace of the image by $\mathring{\rho}$ of the Frobenius at v (for instance, if $\mathring{\rho} = \mathring{\rho}_{f,\mathfrak{l}}$, we can compute the coefficients $a_v(f) \bmod \mathfrak{l}$ using methods based on modular symbols).

[20]There are at most finitely many exceptions.

If for each of these v the trace is the same for ρ^{S_r} and $\mathring{\rho}^{S_r}$, this proves that ψ is trivial, so that ρ^{S_r} is equivalent to $\mathring{\rho}^{S_r}$.

Remark 20. In particular, it then follows that the splitting field L_r of $F_r(x)$ is indeed the field $\mathring{L}_r$ cut out by $\mathring{\rho}^{S_r}$. Moreover, since the Galois representation $\mathring{\rho}$ can be recovered from its quotient $\mathring{\rho}^{S_r}$ and its determinant character $\det\mathring{\rho}$, the field $\mathring{L}$ cut out by $\mathring{\rho}$ is the compositum of L_r and of the field cut out by $\det\mathring{\rho}$, which is by assumption a subfield of the cyclotomic field $\mathbb{Q}(\mu_\ell)$. Using the [Pari/GP] functions `polsubcyclo` and `polcompositum` to compute explicitly this latter field and then its compositum with L_r, we can thus easily compute a nice monic polynomial in $\mathbb{Z}[x]$ whose splitting field is $\mathring{L}$. This is useful since, as explained in section 2, the polynomial $F(x) \in \mathbb{Q}[x]$ of degree $\ell^2 - 1$ computed by the algorithm described in [Mas13] is usually too big to be reduced directly.

4. Application

Let R be the set of couples $(f, \mathfrak{l})$, where $\mathfrak{l}$ a prime ideal of degree 1 of the Hecke field[21] of f lying above a prime number $\ell \leqslant 31$, and $f \in S_k(1)$ a newform of level $N = 1$ and weight $k < \ell$, and let $R' \subsetneq R$ be the subset formed by the couples $(f, \mathfrak{l})$ such that the Galois representation $\mathring{\rho}_{f,\mathfrak{l}}$ attached to f mod $\mathfrak{l}$ is not exceptional.[22]

For each $(f, \mathfrak{l})$ in R', we have used the algorithm described in [Mas13] to compute a polynomial $F(x) \in \mathbb{Q}[x]$ supposedly attached to $\mathring{\rho}_{f,\mathfrak{l}}$. For $\ell \neq 17$, we have then reduced each of these data by the method presented in section 2, thus getting a collection of polynomials $F_i(x) \in \mathbb{Z}[x]$, $0 \leqslant i \leqslant r = \mathrm{ord}_2(\ell - 1)$, and we have applied the group cohomology method described in sections 3.3.1 and 3.6 to certify that these data do define the correct Galois representations. We have finally computed the Dokchitsers' resolvents corresponding to these representations, and we have used them to determine the image in $\mathrm{GL}_2(\mathbb{F}_\mathfrak{l})$ (up to similarity of course) of the Frobenius at p by each of these representations for the first 40 primes $p \in \mathbb{N}$ above 10^{1000}, so as to illustrate the fact that huge values of p are not a problem for our algorithm. In particular, we have determined the value of $a_p(f)$ mod $\mathfrak{l}$ for such p. All of these certified data (the reduced polynomials $F_i(x)$ with their ordered roots, the Dokchitsers' resolvents, and the tables of images of Frobenius elements) may be found on the author's webpage `http://www2.warwick.ac.uk/fac/sci/maths/people/staff/mascot/galreps`.

Remark 21. In [Mas13], we noted that it took [SAGE] about 30 minutes of CPU time to compute one coefficient a_p mod $\mathfrak{l}$ for $p \approx 10^{1000}$ via our Galois representation data. As we reran the computations with the certified resolvents, we realised that [Pari/GP] can do the same thing in less than 1 minute. The reason for this is that [SAGE] takes the time to check rigorously that p is prime before starting computations mod p, whereas [Pari/GP] does not. Amusingly, this shows that it takes much more time to find a prime number p of this size than to compute a_p mod $\mathfrak{l}$ by the Galois representation method.

We have certified that the 40 values of p used in the tables below are indeed prime, because we are not sure what would happen if we ran our algorithm with a composite pseudoprime. As a result, the values of a_p mod $\mathfrak{l}$ displayed in these tables are completely rigorous.

[21] By *Hecke field* of a newform, we mean the number field generated by its Fourier coefficients.
[22] So we exclude precisely Δ mod 23 and $E_4\Delta$ mod 31.

In order to give an idea of the size of the objects that our algorithms manipulate, we present here two cases extracted from the aforementioned tables. Instead of representing a similarity class in $\mathrm{GL}_2(\mathbb{F}_\mathfrak{l})$ by a matrix as we did in [Mas13], we deemed it more elegant to give its *minimal* polynomial in factored form over $\mathbb{F}_\mathfrak{l}$. Since $\mathrm{GL}_2(\mathbb{F}_\ell)$ splits into similarity classes as follows, this is a faithful representation.

Type of class	Representative	Minimal polynomial	# of classes	# of elements in class
Scalar	$\begin{bmatrix}\lambda & 0\\ 0 & \lambda\end{bmatrix}$	$x-\lambda$	$\ell-1$	1
Split semisimple	$\begin{bmatrix}\lambda & 0\\ 0 & \mu\end{bmatrix}$	$(x-\lambda)(x-\mu)$	$\frac{(\ell-1)(\ell-2)}{2}$	$\ell(\ell+1)$
Nonsplit semisimple	$\begin{bmatrix}0 & -n\\ 1 & t\end{bmatrix}$	x^2-tx+n irreducible over $\mathbb{F}_\ell$	$\frac{\ell(\ell-1)}{2}$	$\ell(\ell-1)$
Nonsemisimple	$\begin{bmatrix}\lambda & 1\\ 0 & \lambda\end{bmatrix}$	$(x-\lambda)^2$	$\ell-1$	$(\ell+1)(\ell-1)$

Example 1. Δ mod 29.

It seems natural to start with an example with $f=\Delta=q-24q^2+252q^3+O(q^4)$, the most famous cuspform of all. While for $\ell=31$ we have $r=1$, for $\ell=29$ we have $r=2$, so the polynomials $F_r(x)$ are more impressive for $\ell=29$ than for $\ell=31$. Here is the one corresponding to Δ mod 29:

$$
\begin{aligned}
F_2(x) = {} & x^{120} - 39\,x^{119} + 52\,x^{118} + 18802\,x^{117} - 260738\,x^{116} - 2224996\,x^{115} + 78123651\,x^{114}\\
& -328828100\,x^{113} - 8263917952\,x^{112} + 105418992285\,x^{111} - 9281370047\,x^{110} - 8673650394390\,x^{109}\\
& +67175813321912\,x^{108} + 3240223696313\,x^{107} - 3625273840703346\,x^{106} + 28868328866222299\,x^{105}\\
& -55712181926653112\,x^{104} - 831213186859484809\,x^{103} + 6400389530587512440\,x^{102}\\
& +5664948473704761298\,x^{101} - 23659909902580975583 7\,x^{100} - 86140460526574607141\,x^{99}\\
& +1804936115739873551282 7\,x^{98} - 1430341717384733246541 41\,x^{97} + 3099082799270361144089 48\,x^{96}\\
& +4110452935977502930211262\,x^{95} - 4980858750768408684161327 2\,x^{94}\\
& +2557183907977612189801122 49\,x^{93} - 3709382324225155502380307 06\,x^{92}\\
& -4239746526064029063336974560\,x^{91} + 4005926013783907999032473568 2\,x^{90}\\
& -2051341000354086474907092949 25\,x^{89} + 6908109596653217246541294631 70\,x^{88}\\
& -1150913531696070804731460240641\,x^{87} - 2905017526953691499670077418670\,x^{86}\\
& +4732265910209746550635239063585 6\,x^{85} - 4257922924780796168430467063140 83\,x^{84}\\
& +2739838234183913689504417826249525\,x^{83} - 1237724766258906442878486581595807 5\,x^{82}\\
& +4129625130076324291129187492449223 6\,x^{81} - 8609625448199280857324012768184753 4\,x^{80}\\
& -1741619874386173300695119574549482 16\,x^{79} + 3004945442865208465399646864785306007\,x^{78}\\
& -1942660986678065957896284118296271486 5\,x^{77} + 1081994531218585445622743376957315359 51\,x^{76}\\
& -5405623544854151705681718567243472490 28\,x^{75} + 2003170329279473549264139360014033008269\,x^{74}\\
& -4906345350745852789161273456858421483526\,x^{73}\\
& +6852101959985515455407213317694533880854\,x^{72}\\
& +2174483545654277797854401043201795757099 8\,x^{71}\\
& -3545316019601041868142880457529855348373 56\,x^{70}\\
& +2415813767710375355007174048785369337370619\,x^{69}\\
& -1179547632063718744711284789015725643064181 8\,x^{68}\\
& +5194978621545820186585016864765103871808353 3\,x^{67}\\
& -2058377607076522512366184693317153079538687 72\,x^{66}\\
& +6327946758916645542625328754755852246248855 01\,x^{65}\\
& -1549984687081576409789267803107087061300626754\,x^{64}\\
& +3780171680443736629265587788531817043101358021\,x^{63}\\
& -2032042888653854240770004273667014042737914619\,x^{62}\\
& -7529658639894485403313414406726846601816563437 1\,x^{61}\\
& +4924387744016044290089137008387594131408340290 77\,x^{60}\\
& -1872146628576921265301617989405459118651511828249\,x^{59}\\
& +7889534315510055163849348514205854835317146183354\,x^{58}
\end{aligned}
$$

$$
\begin{aligned}
&-37623219532998612719188117562544690312647851443329\,x^{57}\\
&+13371514909908766622187862220933002388583298017376 2\,x^{56}\\
&-35852785325935764310101641319443971116899858765364 6\,x^{55}\\
&+11502148737204037521457045167773014585402597085660 07\,x^{54}\\
&-42510587481283366287699900604810207731887388256957 02\,x^{53}\\
&+10642612653109338583300281664637819808188791020684 468\,x^{52}\\
&-17402914533613728148979826342208602338942607463119 246\,x^{51}\\
&+48633429629872181118699939461795124668503022992755 678\,x^{50}\\
&-16540327679263199728237165139508767478265423036671 4124\,x^{49}\\
&+14501599710790902139868676674267958724712106129340 8986\,x^{48}\\
&+49239284928006057377356534046161052525931714750729 4865\,x^{47}\\
&-27151145829643838248811169361077500249746512841717 0394\,x^{46}\\
&-65266461924862033039102664344481796104633328213640 5757\,x^{45}\\
&-16367594587199289948998686451709338569385261309703 750822\,x^{44}\\
&+44978511235283376299343780035953332879799842232519 914312\,x^{43}\\
&+19646073668559858224023650929822622112934080573795 228422\,x^{42}\\
&+28535167429260816202303363626597519751307292203748 180524\,x^{41}\\
&-49809082280959521158336743012213915583277009997639 543769\,x^{40}\\
&-94036437367922006793254947997975513463623401157942 7914542\,x^{39}\\
&+25216730525207486986122223772272388727259047605679 19548740\,x^{38}\\
&+70192831323040112722387958496867853076211563771489 40945457\,x^{37}\\
&+12407898598890801572422838737227607844456571501912 25495864\,x^{36}\\
&-54774940542932812395031549315157134292675987516857 162936933\,x^{35}\\
&-16728016029174311224390252816926845697895793955883 3200506384\,x^{34}\\
&+66685231231069675353959106828906025058508433889848 745908446\,x^{33}\\
&+11442002000712957961417469223262933210266204113319 4625544527\,x^{32}\\
&+14653807785163258028902251432891201438440039385977 99565942015\,x^{31}\\
&-45460422337524930825532557987937440330713755046993 52571051582\,x^{30}\\
&-12691048529690820177670723551290387902258432599474 582511011324\,x^{29}\\
&+52196452151843717788522917961185494980372647656700 11997356903\,x^{28}\\
&+59536146913870227752311679132874695245690076312069901091973737\,x^{27}\\
&+42271202746576508837242051054858488179771161211530729060009727\,x^{26}\\
&-16759366112021956566153640396247158312042267616195108600404872 1\,x^{25}\\
&-28636893748754359971189998301655247575846248490927406446948100 2\,x^{24}\\
&+23038205577101754705567772123400529018618056865297282092204922 4\,x^{23}\\
&+92828330220987715772153465190143678309565177219621360937478868 5\,x^{22}\\
&+17558593222346473655929959240584553368851628520778494380827842 0\,x^{21}\\
&-17588500169543654633050559945074633670317645824723656473069945 34\,x^{20}\\
&-14653272871023978636833263890273302011183473598023353001725593 28\,x^{19}\\
&+17733212208363071657021436446346921686107410133656139603568770 87\,x^{18}\\
&+29046067338605307030415144221275346360665462483034444592232528 69\,x^{17}\\
&-52030866913033939454439906383524952261538701115725802583460613 1\,x^{16}\\
&-29069471323187892048085241085333683213561739056446489612848357 69\,x^{15}\\
&-39353499300442587988370141687508955052047689347324728974677088 1\,x^{14}\\
&+21132554400954322321340674918756251709196622760315153390038656 08\,x^{13}\\
&+34352145505306437785857661486107760659838299790267498447572736 1\,x^{12}\\
&-19807338164200893019850765803145042813784036763640938598567502 80\,x^{11}\\
&-84142393859950854694903727654503716155489387356277077554734793 6\,x^{10}\\
&+15116111647215977623112811007473940824760445351802593433209130 07\,x^{9}\\
&+18658940710336150406651606475617929758727382467666827740648522 96\,x^{8}\\
&+88739877898580408922689998155325973256493162168980853639739762 2\,x^{7}\\
&+32795959883806144526965956855687168048601683645260921122269906 3\,x^{6}\\
&+28080703152959633946611160071802685942462524995498505977135070 9\,x^{5}\\
&+23443426269762331380963759055706503695084406373053498685235536 7\,x^{4}\\
&+12841838385978869133026735502344154968220367184475484918671124 8\,x^{3}\\
&+47862235923713816575492173460515921299171434171423149409051143\,x^{2}\\
&+79415324443768446047852151728092952463433175087099282314451 27\,x\\
&-80413918056996577703540784842644222296230035710806692803983 5.
\end{aligned}
$$

The images of the Frobenius elements are given in Table 1.

Example 2. f_{24} mod 31.

For the second example, we pick

$$f = f_{24} = q + 24(22+\alpha)q^2 + 36(4731 - 32\alpha)q^3 + O(q^4),$$

the unique (up to Galois conjugacy) newform of level 1 and of weight 24, because it is the one of lowest weight whose Hecke field is strictly larger than $\mathbb{Q}$. More precisely, the Hecke field of f_{24} is the real quadratic field $\mathbb{Q}(\alpha)$, $\alpha = \frac{1+\sqrt{144169}}{2}$. Its ring of integers is $\mathbb{Z}[\alpha]$.

TABLE 1

p	$\mathring{\rho}_{\Delta,29}(\mathrm{Frob}_p)$	$\tau(p) \bmod 29$
$10^{1000}+453$	$x^2+8x+24$	21
$10^{1000}+1357$	$x^2+21x+1$	8
$10^{1000}+2713$	$x^2+18x+20$	11
$10^{1000}+4351$	x^2+3	0
$10^{1000}+5733$	$(x-20)(x-2)$	22
$10^{1000}+7383$	$(x-19)(x-10)$	0
$10^{1000}+10401$	$(x-7)(x-2)$	9
$10^{1000}+11979$	$x^2+22x+22$	7
$10^{1000}+17557$	x^2+27	0
$10^{1000}+21567$	$(x-23)(x-3)$	26
$10^{1000}+22273$	$x^2+15x+3$	14
$10^{1000}+24493$	$x^2+25x+16$	4
$10^{1000}+25947$	$(x-27)(x-15)$	13
$10^{1000}+27057$	$x^2+22x+23$	7
$10^{1000}+29737$	$(x-23)(x-10)$	4
$10^{1000}+41599$	$(x-13)(x-5)$	18
$10^{1000}+43789$	$(x-18)(x-15)$	4
$10^{1000}+46227$	x^2+7x+3	22
$10^{1000}+46339$	$(x-26)(x-8)$	5
$10^{1000}+52423$	$(x-17)(x-16)$	4
$10^{1000}+55831$	$x^2+21x+4$	8
$10^{1000}+57867$	$(x-13)(x-11)$	24
$10^{1000}+59743$	$x^2+24x+2$	5
$10^{1000}+61053$	$x^2+18x+21$	11
$10^{1000}+61353$	$(x-24)(x-1)$	25
$10^{1000}+63729$	$(x-20)(x-1)$	21
$10^{1000}+64047$	$x^2+14x+6$	15
$10^{1000}+64749$	$x^2+14x+28$	15
$10^{1000}+68139$	$(x-12)(x-2)$	14
$10^{1000}+68367$	$x^2+26x+26$	3
$10^{1000}+70897$	$x^2+12x+28$	17
$10^{1000}+72237$	$x^2+27x+13$	2
$10^{1000}+77611$	$(x-14)(x-13)$	27
$10^{1000}+78199$	$(x-17)(x-14)$	2
$10^{1000}+79237$	$x^2+28x+25$	1
$10^{1000}+79767$	$x^2+13x+16$	16
$10^{1000}+82767$	$(x-27)(x-13)$	11
$10^{1000}+93559$	$x^2+13x+17$	16
$10^{1000}+95107$	$(x-25)(x-24)$	20
$10^{1000}+100003$	$(x-26)(x-13)$	10

In this field, the prime 31 splits into $(31) = \mathfrak{l}_5\mathfrak{l}_{27}$, where $\mathfrak{l}_5 = (31, \alpha - 5)$ and $\mathfrak{l}_{27} = (31, \alpha - 27)$. Instead of presenting the results for the Galois representations attached to f_{24} modulo $\mathfrak{l}_5$ and $\mathfrak{l}_{27}$ separately, it is more interesting to present them together, since we can then compute the coefficients $\tau_{24}(p) \bmod 31\mathbb{Z}[\alpha]$ by putting together the information coming from both representations and using Chinese remainders. This is what we do in Table 2.

Since $\ell = 31$, we have $r = 1$. The polynomial $F_r(x)$ corresponding to $\mathring{\rho}_{f_{24},\mathfrak{l}_5}$ is

$$\begin{aligned}F_1(x) = {} & x^{64} - 26\,x^{63} + 138\,x^{62} + 2883\,x^{61} - 50530\,x^{60} + 284952\,x^{59} + 1532392\,x^{58} - 42378023\,x^{57} \\ & + 313778342\,x^{56} - 30967109\,x^{55} - 15952723659\,x^{54} + 120293225685\,x^{53} - 294956419293\,x^{52} \\ & - 2450725406897\,x^{51} + 28694976228508\,x^{50} - 82028806284207\,x^{49} - 33797566443141\,x^{48} \\ & + 30936396673955\,x^{47} - 25385922046683633\,x^{46} + 285017809626505879\,x^{45} - 101340567457478942\,x^{44} \\ & - 5967948306452799555\,x^{43} + 18835587705819950118\,x^{42} - 14494324520552133971 0\,x^{41} \\ & + 60221904404445873974 2\,x^{40} + 22005353302997137094 69\,x^{39} - 16686864181478594950667\,x^{38} \\ & + 10797734164264641586719 2\,x^{37} - 47566878686442941629547 2\,x^{36} - 22529803768179514499258 6\,x^{35} \\ & + 13039469950621100673089867\,x^{34} - 37880916977102172639162818\,x^{33} \\ & + 23877972000622578505000183\,x^{32} - 37971635540990647459559288 3\,x^{31} \\ & - 35856184174592466142268374 7\,x^{30} + 21467502653993360143238405812\,x^{29} \\ & - 62531950374059451763223031677\,x^{28} - 14136317210764018713625927351 5\,x^{27} \\ & + 92089347276908863334727927726 0\,x^{26} - 76451350193454752144064305027 7\,x^{25} \\ & - 22275648914129968481978329438 52\,x^{24} + 47180361481882162760685243170 4\,x^{23} \\ & - 64034747781891178821434987652 56\,x^{22} + 12894528790058663976593729405532 3\,x^{21} \\ & - 26713019746887982367506934308328 2\,x^{20} - 60994232253776377479863725235135 7\,x^{19} \\ & + 28438481497941568243792515467189 28\,x^{18} - 14490089743082498766812177554223 92\,x^{17} \\ & - 86099647320854447391157124287404 43\,x^{16} + 11462233793731819908607681612424601\,x^{15} \\ & + 16721010272893391334932201233417682\,x^{14} - 29850257116492845020236438390839168\,x^{13} \\ & - 85528053082348511322543845120538291\,x^{12} + 28850563578110986681888475386863211 3\,x^{11} \\ & - 35293229333983240796518647599225700\,x^{10} - 12772621584964785197370587591566569 14\,x^{9} \\ & + 18340100422891596262536420580518187 96\,x^{8} + 13543167579028053878174181790958073 50\,x^{7} \\ & - 41638819207764211288090038979479002 49\,x^{6} + 98863028382531094552083553390858203 5\,x^{5} \\ & + 20408263088550284793926403564698985 42\,x^{4} - 78107432052915753460850249679413742 9\,x^{3} \\ & + 70957684944341669097877480376508212 7\,x^{2} - 15434654759069556686415222308642611594\,x \\ & + 68841325980335831334816353906529157 2,\end{aligned}$$

and the one corresponding to $\mathring{\rho}_{f_{24},\mathfrak{l}_{27}}$ is

$$\begin{aligned}F_1(x) = {} & x^{64} - 13\,x^{63} - 12\,x^{62} + 1798\,x^{61} - 2480\,x^{60} - 301351\,x^{59} + 2427920\,x^{58} + 3549779\,x^{57} \\ & - 128622131\,x^{56} - 605195516\,x^{55} + 18083445605\,x^{54} - 76623104240\,x^{53} - 136111338385\,x^{52} \\ & + 163365709662\,x^{51} + 36207027735933\,x^{50} - 333393729013025\,x^{49} \\ & + 1353870749023624\,x^{48} - 4874235588482263\,x^{47} + 57952977575049072\,x^{46} - 607869739537694 24\,x^{45} \\ & + 3885848486411353707\,x^{44} - 19706433793139872315\,x^{43} + 12048857914602562752 1\,x^{42} \\ & - 8839097877426513939 57\,x^{41} + 57253168828601343277 65\,x^{40} - 30772173337138099500438\,x^{39} \\ & + 15994391720767305806265 1\,x^{38} - 90278014264463522173891 1\,x^{37} + 51912709232869653604025 18\,x^{36} \\ & - 27218300530032866515284399\,x^{35} + 13183404322335505697730 6359\,x^{34} \\ & - 63456613757810228519377 8876\,x^{33} + 31216819109323324955006 70500\,x^{32} \\ & - 14916061491879244185623832302\,x^{31} + 66502847707000774372555381722\,x^{30} \\ & - 28006314449115885464848327512\,x^{29} + 11517979201913291880892190697 05\,x^{28} \\ & - 46475620824195630172502710306 29\,x^{27} + 17964227685904653209413452332198\,x^{26} \\ & - 65006898495556449638155640530135\,x^{25} + 22052977154374152324261752177116 5\,x^{24} \\ & - 70803086554625174239934030468988 4\,x^{23} + 21830954379064095202715391690529 77\,x^{22} \\ & - 64660454401897533842717608066247 55\,x^{21} + 18519022770605982324844617113128582\,x^{20} \\ & - 50903095666736365236595239907177352\,x^{19} + 13571229972534541771998218357821 7245\,x^{18} \\ & - 34902441492708441431329887927023933 2\,x^{17} + 87928261768113859350605164634216001 1\,x^{16} \\ & - 21288876367859999775432471375399126 26\,x^{15} + 49595673919460189540797332521231198 70\,x^{14} \\ & - 10698310092805038208309504750205888318\,x^{13} + 21185126053660446928251211870565927064\,x^{12} \\ & - 37034974052822943124568751376502208132\,x^{11} + 57682303937811470679764738932557333147\,x^{10} \\ & - 77659172323156765855997312303575730246\,x^{9} + 91059874206416211006654087253008834453\,x^{8} \\ & - 92285656456264804316815032164880452414\,x^{7} + 79794573183910939847907389673931597531\,x^{6} \\ & - 60780767548452665962995019987085052653\,x^{5} + 37996038264233396745310228794005562702\,x^{4} \\ & - 20277402785975735994777964167007154402\,x^{3} + 75749664506292977050112507720053450 04\,x^{2} \\ & - 13516374297426007349513323696473811 73\,x + 19356992438321173093146854904846611 3.\end{aligned}$$

The images of the Frobenius elements are given in Table 2.

TABLE 2

p	$\mathring{\rho}_{f_{24},\mathfrak{l}_5}(\mathrm{Frob}_p)$	$\mathring{\rho}_{f_{24},\mathfrak{l}_{27}}(\mathrm{Frob}_p)$	$a(f_{24},p) \bmod 31\mathbb{Z}[\alpha]$
$10^{1000}+453$	$x^2+26x+21$	$(x-20)(x-15)$	$1+7\alpha$
$10^{1000}+1357$	$(x-18)(x-3)$	$(x-25)(x-22)$	$1+4\alpha$
$10^{1000}+2713$	$(x-24)(x-2)$	$(x-29)(x-7)$	$4+23\alpha$
$10^{1000}+4351$	$(x-17)(x-13)$	$(x-11)(x-6)$	$9+29\alpha$
$10^{1000}+5733$	$(x-19)(x-12)$	$(x-15)(x-9)$	$3+18\alpha$
$10^{1000}+7383$	$x^2+4x+14$	$(x-7)(x-2)$	$17+2\alpha$
$10^{1000}+10401$	$(x-22)(x-5)$	$x^2+24x+17$	$9+16\alpha$
$10^{1000}+11979$	$x^2+17x+7$	$x^2+19x+7$	$6+14\alpha$
$10^{1000}+17557$	$(x-26)(x-24)$	$(x-17)(x-13)$	$1+16\alpha$
$10^{1000}+21567$	$x^2+6x+29$	$x^2+2x+29$	$10+3\alpha$
$10^{1000}+22273$	$x^2+10x+19$	$(x-16)(x-7)$	$29+17\alpha$
$10^{1000}+24493$	$(x-22)(x-12)$	$(x-25)(x-18)$	$8+30\alpha$
$10^{1000}+25947$	$(x-15)(x-12)$	$(x-24)(x-23)$	$14+15\alpha$
$10^{1000}+27057$	$x^2+10x+30$	$(x-26)(x-25)$	$17+7\alpha$
$10^{1000}+29737$	$x^2+3x+24$	$x^2+13x+24$	$19+8\alpha$
$10^{1000}+41599$	$x^2+11x+8$	$x^2+27x+8$	$18+19\alpha$
$10^{1000}+43789$	$x^2+14x+3$	x^2+7x+3	$14+13\alpha$
$10^{1000}+46227$	$x^2+15x+12$	$x^2+4x+12$	$29+16\alpha$
$10^{1000}+46339$	$(x-24)(x-9)$	$x^2+5x+30$	$5+18\alpha$
$10^{1000}+52423$	$(x-10)(x-1)$	$x^2+16x+10$	$27+3\alpha$
$10^{1000}+55831$	$x^2+7x+25$	$(x-28)(x-2)$	$17+20\alpha$
$10^{1000}+57867$	$x^2+12x+6$	x^2+6x+6	$12+20\alpha$
$10^{1000}+59743$	$x^2+16x+12$	$(x-21)(x-5)$	$28+16\alpha$
$10^{1000}+61053$	$(x-18)(x-16)$	$x^2+15x+9$	$24+2\alpha$
$10^{1000}+61353$	$(x-26)(x-13)$	$x^2+30x+28$	$11+18\alpha$
$10^{1000}+63729$	$x^2+4x+23$	$(x-18)(x-3)$	$3+11\alpha$
$10^{1000}+64047$	$(x-19)(x-3)$	$(x-13)(x-2)$	$25+18\alpha$
$10^{1000}+64749$	$(x-13)(x-10)$	$(x-17)(x-4)$	$15+14\alpha$
$10^{1000}+68139$	$x^2+2x+26$	$(x-19)(x-3)$	$1+18\alpha$
$10^{1000}+68367$	$(x-22)(x-2)$	$x^2+21x+13$	$30+5\alpha$
$10^{1000}+70897$	$x^2+8x+25$	$(x-26)^2$	$15+14\alpha$
$10^{1000}+72237$	$(x-11)(x-2)$	$(x-12)(x-7)$	$6+20\alpha$
$10^{1000}+77611$	$x^2+5x+15$	$x^2+28x+15$	$27+6\alpha$
$10^{1000}+78199$	$(x-30)(x-28)$	$(x-25)(x-15)$	$17+2\alpha$
$10^{1000}+79237$	$x^2+10x+26$	$(x-27)(x-9)$	$19+19\alpha$
$10^{1000}+79767$	$(x-15)(x-6)$	$(x-7)(x-4)$	$12+8\alpha$
$10^{1000}+82767$	$(x-13)(x-3)$	$(x-24)(x-21)$	$8+14\alpha$
$10^{1000}+93559$	$(x-15)(x-10)$	$x^2+8x+26$	$17+14\alpha$
$10^{1000}+95107$	$(x-28)(x-20)$	$(x-18)(x-7)$	$18+6\alpha$
$10^{1000}+100003$	$x^2+21x+8$	$(x-10)(x-7)$	$7+13\alpha$

ACKNOWLEDGEMENTS

The computations presented here would not have been amenable without Bill Allombert, who suggested to the author the idea of step-by-step polynomial reduction, and Karim Belabas and Denis Simon, who provided their [BS14] script. The

author also thanks J. Klüners for useful discussions in July 2015 in Oberwolfach about the algorithmic computation of Galois groups, D. Holt for his help in permutation group theory, and the author's friend and colleague A. Page for the clever suggestions that he provided. Finally, the author thanks the anonymous reviewer of the previous version of this article for suggesting a much simpler method to certify some Galois groups (cf. section 3.5) and more generally for his insightful suggestions, which helped to make this article clearer.

The computations presented in this paper were partly carried out using the PlaFRIM experimental testbed, being developed under the Inria PlaFRIM development action with support from LABRI and IMB and other entities: Conseil Régional d'Aquitaine, FeDER, Université de Bordeaux and CNRS (see https://plafrim.bordeaux.inria.fr/), and partly on the Warwick Mathematics Institute computer cluster provided by the EPSRC grant. The computer algebra packages used were [SAGE], [Pari/GP] and [Magma].

References

[BS14] K. Belabas and D. Simon, *Ideal power detection over number fields*, in preparation, personal communication.

[Bos07] J. Bosman, *On the computation of Galois representations associated to level one modular forms*, Chapter 7 in [CE11].

[Coh93] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. MR1228206

[CE11] B. Edixhoven and J.-M. Couveignes (eds.), *Computational Aspects of Modular Forms and Galois Representations*: *How One Can Compute in Polynomial Time the Value of Ramanujan's Tau at a Prime*, Annals of Mathematics Studies, vol. 176, Princeton University Press, Princeton, NJ, 2011. MR2849700

[Del71] P. Deligne, *Formes modulaires et représentations l-adiques* (French), Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363, Lecture Notes in Math., vol. 175, Springer, Berlin, 1971, pp. Exp. No. 355, 139–172. MR3077124

[DvHZ14] M. Derickx, M. van Hoeij, and J. Zeng, *Computing Galois representations and equations for modular curves* $X_H(\ell)$, arXiv:1312.6819.

[DM96] J. D. Dixon and B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics, vol. 163, Springer-Verlag, New York, 1996. MR1409812

[Dok10] T. Dokchitser and V. Dokchitser, *Identifying Frobenius elements in Galois groups*, Algebra Number Theory **7** (2013), no. 6, 1325–1352, DOI 10.2140/ant.2013.7.1325. MR3107565

[FW02] D. W. Farmer and K. James, *The irreducibility of some level 1 Hecke polynomials*, Math. Comp. **71** (2002), no. 239, 1263–1270, DOI 10.1090/S0025-5718-01-01375-8. MR1898755

[FK14] C. Fieker and J. Klüners, *Computation of Galois groups of rational polynomials*, LMS J. Comput. Math. **17** (2014), no. 1, 141–158, DOI 10.1112/S1461157013000302. MR3230862

[Gro90] B. H. Gross, *A tameness criterion for Galois representations associated to modular forms (mod p)*, Duke Math. J. **61** (1990), no. 2, 445–517, DOI 10.1215/S0012-7094-90-06119-8. MR1074305

[Kar87] G. Karpilovsky, *The Schur Multiplier*, London Mathematical Society Monographs. New Series, vol. 2, The Clarendon Press, Oxford University Press, New York, 1987. MR1200015

[KW09] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture. I, II*, Invent. Math. **178** (2009), no. 3, 485–504, 505–586, DOI 10.1007/s00222-009-0205-7. MR2551763, MR2551764

[Lan02] S. Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR1878556

[Magma] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. MR1484478

[Mas13] N. Mascot, *Computing modular Galois representations*, Rend. Circ. Mat. Palermo (2) **62** (2013), no. 3, 451–476, DOI 10.1007/s12215-013-0136-4. MR3118315

[MT03] H. Moon and Y. Taguchi, *Refinement of Tate's discriminant bound and non-existence theorems for mod p Galois representations*, Doc. Math. Extra Vol. (2003), 641–654. MR2046611

[NSW08] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of Number Fields*, 2nd ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008. MR2392026

[Pari/GP] The PARI Group, PARI/GP development version `2.8.0`, Bordeaux, 2015, `http://pari.math.u-bordeaux.fr/`

[Que95] J. Quer, *Liftings of projective 2-dimensional Galois representations and embedding problems*, J. Algebra **171** (1995), no. 2, 541–566, DOI 10.1006/jabr.1995.1027. MR1315912

[Rib85] K. A. Ribet, *On l-adic representations attached to modular forms. II*, Glasgow Math. J. **27** (1985), 185–194, DOI 10.1017/S0017089500006170. MR819838

[SAGE] *SAGE mathematics software*, version `5.3`. `http://sagemath.org/`.

[Ser79] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979. MR554237

[Swi72] H. P. F. Swinnerton-Dyer, *On l-adic representations and congruences for coefficients of modular forms*, Modular Functions of One Variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972), Springer, Berlin, 1973, pp. 1–55. Lecture Notes in Math., Vol. 350. MR0406931

IMB, Université Bordeaux 1, UMR 5251, F-33400 Talence, France – and – CNRS, IMB, UMR 5251, F-33400 Talence, France – and – INRIA, project LFANT, F-33400 Talence, France

Current address: Mathematics Institute, University of Warwick, Coventry CV4 7AL, United Kingdom

E-mail address: `n.a.v.mascot@warwick.ac.uk`