Journal de Théorie des Nombres
de Bordeaux **13** (2001), 395–411

Newforms, inner twists, and the inverse Galois problem for projective linear groups

par Luis. V. Dieulefait

Résumé. Nous reformulons de manière plus explicite les résultats de Momose, Ribet et Papier sur les images des représentations galoisiennes attachées à des newforms sans multiplication complexe, en nous restreignant aux formes de poids 2 et de caractère trivial. Nous calculons deux tels exemples de newforms, possédant une unique tordue conjuguée à la forme, et nous démontrons que pour tout nombre premier $\ell > 3$, l'image est aussi grosse que possible. Nous utilisons ce résultat pour prouver que les groupes $\mathrm{PGL}(2, \mathbb{F}_{\ell^2})$ ($\ell \equiv 3, 5 \pmod 8$, $\ell > 3$) et $\mathrm{PGL}(2, \mathbb{F}_{\ell^5})$ ($\ell \not\equiv 0, \pm 1 \pmod{11}$, $\ell > 3$) sont groupes de Galois sur $\mathbb{Q}$.

Abstract. We reformulate more explicitly the results of Momose, Ribet and Papier concerning the images of the Galois representations attached to newforms without complex multiplication, restricted to the case of weight 2 and trivial nebentypus. We compute two examples of these newforms, with a single inner twist, and we prove that for every inert prime greater than 3 the image is as large as possible. As a consequence, we prove that the groups $\mathrm{PGL}(2, \mathbb{F}_{\ell^2})$ for every prime $\ell \equiv 3, 5 \pmod 8$, $\ell > 3$, and $\mathrm{PGL}(2, \mathbb{F}_{\ell^5})$ for every prime $\ell \not\equiv 0, \pm 1 \pmod{11}$, $\ell > 3$, are Galois groups over $\mathbb{Q}$.

1. Introduction

Let $f = \sum_{n=1}^{\infty} a_n q^n$ be a weight 2 newform on $\Gamma_0(N)$. In particular f is a normalized eigenform for the whole Hecke algebra. Let $\mathbb{Q}_f$ be the number field generated by its coefficients a_n and $\mathcal{O}$ its ring of integers. For every prime ℓ put: $\mathcal{O}_\ell = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ and $\mathbb{Q}_{f,\ell} = \mathbb{Q}_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$.
By Deligne's theorem (see [D71]), there exists a continuous Galois representation:

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathcal{O}_\ell) \subseteq \mathrm{GL}(2, \mathbb{Q}_{f,\ell})$$

Manuscrit reçu le 8 septembre 1999.
supported by TMR - Marie Curie Fellowship ERB4001GT974451.

unramified outside ℓN satisfying, for every prime $p \nmid \ell N$:

$$\text{trace } \rho_\ell(\text{Frob } p) = a_p, \qquad \det\ \rho_\ell(\text{Frob } p) = p.$$

Let $G = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $G_\ell = \rho_\ell(G)$, closed subgroup of $\text{GL}(2, \mathcal{O}_\ell)$. From the decompositions: $\mathbb{Q}_{f,\ell} = \prod_{\lambda|\ell} \mathbb{Q}_{f,\lambda}$ and $\mathcal{O}_\ell = \prod_{\lambda|\ell} \mathcal{O}_\lambda$ we obtain a decomposition of ρ_ℓ as direct sum of the representations:

$$\rho_\lambda : G \to \text{GL}(2, \mathcal{O}_\lambda) \subseteq \text{GL}(2, \mathbb{Q}_{f,\lambda}).$$

From now on, we will assume that the newform f does not have complex multiplication (CM); see [R80], page 48, or [S71b] for a definition.
Let λ be a prime in $\mathbb{Q}_f$. Consider the reduction $\overline{\rho}_\lambda$ of ρ_λ, obtained by composing ρ_λ with the reduction map: $\text{GL}(2, \mathcal{O}_\lambda) \to \text{GL}(2, \mathbb{F}_\lambda)$, where $\mathbb{F}_\lambda$ is the residue field of λ. Let $\ell = \ell(\lambda)$ be the rational prime such that $\lambda \mid \ell$ and let $\overline{G}_\lambda$ be the image of $\overline{\rho}_\lambda$. In order to determine the images of the representations $\overline{\rho}_\lambda$ we will need the following result of Ribet ([R85], theorem 2.1):

Theorem 1.1. *Let H be an open subgroup of G. Then for almost every λ we have:*
a) *The representation $\overline{\rho}_\lambda|_H$ is an irreducible 2-dimensional representation of H over $\mathbb{F}_\lambda$.*
b) *The order of the group $\overline{H}_\lambda = \overline{\rho}_\lambda(H)$ is divisible by ℓ.*

For every automorphism γ of the field $\mathbb{Q}_f$ consider the newform:

$$\gamma f = \sum_{n=1}^{\infty} \gamma(a_n) q^n.$$

Suppose that there exists a Dirichlet character χ such that:

$$\gamma(a_p) = \chi(p) a_p$$

for almost every p. This character must be unique (because we are assuming that f does not have CM) and we will call it χ_γ. In general, for a cusp form $f \in S_2(\Gamma_0(N), \varepsilon)$ it holds: $\varepsilon \chi_\gamma^2 = \gamma(\varepsilon)$. In our particular case ($\varepsilon = 1$) this implies that χ_γ is a quadratic character. When such a character exists we say that γf is an **inner twist** of f .
Let Γ be the set of those γ giving an inner twist. We recall some properties of Γ :

- For every $\gamma \in \Gamma$ the conductor of χ_γ is divisible only by the primes dividing N.
- Γ is an abelian elementary 2-group.
- Let $F_f = \mathbb{Q}_f^\Gamma$, the fixed field of Γ. Then F_f is the field generated by $\{a_p^2\}$, with $p \nmid N$ ranging over a density one set of primes.

- Whenever N is square-free, no $f \in S_2(\Gamma_0(N))$ has CM or inner twists, so that $\Gamma = \{1\}$.

For all but the first of these properties, see [R80], page 49. The first property follows from the equality $\gamma(\rho_\ell) = \rho_\ell \otimes \chi_\gamma$ that will be proved later. Using the fact that the Galois representation $\gamma(\rho_\ell)$ is unramified outside ℓN it follows that χ_γ can only ramify at primes dividing N.
Every character χ_γ may be thought of as a character on the Galois group G, so its kernel H_γ is an open subgroup of G. Let H be the intersection of the H_γ, $\gamma \in \Gamma$, and let K be its fixed field (cf. [R85], page 190).
Let $H_\ell = \rho_\ell(H)$ and let

$$A_\ell = \{x \in \mathrm{GL}(2, R_\ell) \quad / \ \det(x) \in \mathbb{Z}_\ell^*\},$$

where R is the ring of integers of F_f and $R_\ell = R \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$.
The following theorem of Momose ([M81]; [R85], theorem 3.1) determines the image of these modular ℓ-adic Galois representations:

Theorem 1.2. *For almost every prime ℓ we have $H_\ell = A_\ell$.*

What is known for every prime ℓ is that ρ_ℓ restricted to H gives a map:

$$\rho_\ell : H \to (D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)^*,$$

where D is a quaternion division algebra over F_f (this quaternion algebra is related to a central simple algebra over F_f defined by a certain 2-cocycle on Γ with values in $\mathbb{Q}_f^*$). This implies that, first of all, we should restrict ourselves to those primes such that:

$$D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong M(2, F_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell). \tag{0}$$

For these primes, H_ℓ is an open subgroup of A_ℓ (condition (0) holds for almost every ℓ, the exceptions are the primes dividing the discriminant of D).
Then the theorem is proved after applying a result of [R75] (cf. [R75], corollary 2.2 and theorem 3.1, and [R85], page 192) stating that $H_\ell = A_\ell$ if the following hold:

(1) The determinant map $H_\ell \to \mathbb{Z}_\ell^*$ is surjective.
(2) $\ell \geq 5$.
(3) H_ℓ contains an element x_ℓ such that: (trace $x_\ell)^2$ generates R_ℓ as a $\mathbb{Z}_\ell$-algebra.
(4) For each $\lambda \mid \ell$, the group $\overline{\rho}_\lambda(H)$ is an irreducible subgroup of $\mathrm{GL}(2, \mathbb{F}_\lambda)$ whose order is divisible by ℓ.

To see that these conditions hold for almost every prime, theorem 1.1 is applied (to deal with condition (4)) together with the following facts:
- There exists an integer v such that v is relatively prime to N, Frob $v \in H$ and a_v^2 generates F_f over $\mathbb{Q}$ (condition (3)).

• The determinant of ρ_ℓ coincides on H with the ℓ-adic cyclotomic character χ_ℓ (condition (1)).

We are interested in the image of G, $G_\ell = \rho_\ell(G)$. ρ_ℓ is a continuous homomorphism

$$G \to \mathrm{GL}(2, \mathcal{O}_\ell)$$

whose restriction to H takes values in $A_\ell \subseteq \mathrm{GL}(2, R_\ell)$, if ℓ satisfies condition (0).

For $\gamma \in \Gamma$ let us consider $\gamma\rho_\ell$ and $\rho_\ell \otimes \chi_\gamma$. These two representations are isomorphic (semisimple with the same character). Thus there is a matrix $X \in \mathrm{GL}(2, \mathbb{Q}_{f,\ell})$ such that:

$$X(\gamma\rho_\ell)X^{-1} = \rho_\ell \otimes \chi_\gamma.$$

χ_γ being trivial on H and γ on $H_\ell \subseteq A_\ell$, X commutes with H_ℓ. Then X is a scalar matrix and we obtain the equality:

$$\gamma(\rho_\ell(g)) = \rho_\ell(g)\chi_\gamma(g), \qquad \text{for all } g \in G \text{ and } \gamma \in \Gamma.$$

For $g \in G$ let $\alpha(g) \in \mathbb{Q}_f^*$ be an element such that: $\gamma(\alpha(g)) = \chi_\gamma(g)\alpha(g)$ for all $\gamma \in \Gamma$, whose existence is guaranteed by Hilbert's Satz 90, and $\alpha(g)$ does not depend on ℓ. Moreover, it only depends on the image $\overline{g}$ of g in G/H. Therefore, we have only a finite number of $\alpha(g)$, and they belong to $\mathcal{O}_\ell^*$ for almost every ℓ.

The matrices $\rho_\ell(g)\alpha(g)^{-1}$ are Γ-invariants (because $\gamma \in \Gamma$ acts on both ρ_ℓ and α by multiplication by χ_γ), so they are in $\mathrm{GL}(2, R_\ell)$. In the equality:

$$\rho_\ell(g) = \begin{pmatrix} \alpha(g) & 0 \\ 0 & 1/\alpha(g) \end{pmatrix} \left\{ \begin{pmatrix} 1 & 0 \\ 0 & \alpha^2(g) \end{pmatrix} (\alpha(g)^{-1}\rho_\ell(g)) \right\} \tag{1.1}$$

let us call B_ℓ the subgroup generated by the products in curly brackets, when g ranges over G. It is contained in A_ℓ because it is in $\mathrm{GL}(2, R_\ell)$ and has determinant χ_ℓ. Note that $\alpha^2(g) \in R_\ell$ because it is Γ-invariant:

$$\gamma(\alpha^2(g)) = (\gamma(\alpha(g)))^2 = (\chi_\gamma(g))^2\alpha^2(g) = \alpha^2(g).$$

For an element $g \in H$ we can take $\alpha(g) = 1$, so that $H_\ell \subseteq B_\ell$.

An application of theorem 1.2 proves the following theorem of E. Papier ([R85], theorem 4.1):

Theorem 1.3. *For almost every prime ℓ, the image G_ℓ of ρ_ℓ is the subgroup of $\mathrm{GL}(2, \mathcal{O}_\ell)$ generated by the group A_ℓ and the finite set of matrices:*

$$\begin{pmatrix} \alpha(g) & 0 \\ 0 & 1/\alpha(g) \end{pmatrix}, \qquad \textit{with } g \in G/H.$$

Now, let us introduce a variant of this theorem that will allow us to compute the exceptional primes in some examples.

The key observation is that we can replace the condition $H_\ell = A_\ell$ by the weaker equality $B_\ell = A_\ell$, because for every prime verifying this last

condition theorem 1.3 applies. To check which primes verify this equality, we will use the conditions (0) to (4) of theorem 1.2, this time applied to B_ℓ.
Condition (0) is needed a priori to ensure that $H_\ell \subseteq A_\ell$ and (see the proof of theorem 1.3) it also implies $B_\ell \subseteq A_\ell$. In [Q98] J. Quer gives a formula for the quaternion algebra D (see also [C92]) and condition (0) holds for all primes ℓ such that:

(i) $$\ell \nmid \operatorname{disc}(D).$$

Besides, as pointed out in the proof of theorem 1.3, the prime ℓ must verify:

(ii) $$\alpha(g) \in \mathcal{O}_\ell^*, \text{ for every } g \in G/H.$$

For ease of notation, let us write: $[x, y]$ for the diagonal matrix: $\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$.
As a consequence of (1.1), condition (1) for B_ℓ is satisfied by every prime ℓ because the matrices $[\alpha(g), 1/\alpha(g)]$ have determinant 1 and so all we need is the determinant map of G_ℓ to be surjective; this is equivalent to the surjectivity of the cyclotomic character $\chi_\ell : G \to \mathbb{Z}_\ell^*$.
Again, we look for the element specified by condition (3) in H_ℓ, this is more than enough because $H_\ell \subseteq B_\ell$. Then if v is such that $v \nmid N$, Frob $v \in H$ and a_v^2 generates F_f over $\mathbb{Q}$, ℓ must verify:

(iii) $$\ell \nmid v \text{ and } a_v^2 \text{ generates } R_\ell \text{ as a } \mathbb{Z}_\ell - \text{algebra}.$$

Condition (4) is the hard one. In spite of theorem 1.1 the determination of the finite exceptional set of primes is not trivial, even for G itself (see the next section). Taking B_ℓ instead of H_ℓ we can at least reduce the problem to verifying the condition on G_ℓ, avoiding the restriction $\ell > (G : H)$ (see the proof of theorem 2.1 of [Ri85]), not to mention the gain in condition (1).
Let us call $\overline{B}_{\lambda'}$ the reduction mod λ' of the λ'-component of B_ℓ, where $\lambda' \mid \ell$ is a prime in R , and let $\lambda_1, ..., \lambda_i$ be the primes dividing λ' in $\mathcal{O}$. Assume that for the prime ℓ theorem 1.1 applied to G holds. Then from the irreducibility of all the $\overline{\rho}_{\lambda_j}(G)$ and formula (1.1) it follows that $\overline{B}_{\lambda'}$ is an irreducible subgroup of $\mathrm{GL}(2, \mathbb{F}_{\lambda'})$. In the same way we see that if the groups $\overline{\rho}_{\lambda_j}(G)$ have orders multiple of ℓ the same holds for $\overline{B}_{\lambda'}$ because in (1.1) the matrices $[\alpha(g), \alpha^{-1}(g)]$, after reducing their coefficients modulo any prime dividing ℓ, have orders relatively prime to ℓ.
Thus, we have proved:

Theorem 1.4. *Let $\ell \geq 5$ be a prime such that for every place λ of $\mathbb{Q}_f$ lying above ℓ, the following holds: $\overline{G}_\lambda$ is an irreducible subgroup of* $\mathrm{GL}(2, \mathbb{F}_\lambda)$ *whose order is a multiple of ℓ. If, furthermore, ℓ satisfies conditions* (i), (ii) *and* (iii) *(see the previous discussion), then:*

G_ℓ is the subgroup of $\mathrm{GL}(2, \mathcal{O}_\ell)$ *generated by the group* A_ℓ *and the finite set of matrices:*

$$\begin{pmatrix} \alpha(g) & 0 \\ 0 & 1/\alpha(g) \end{pmatrix}, \qquad \textit{with } g \in G/H.$$

Remark. This result applies to almost every prime.

Let λ be a prime in $\mathcal{O}$ dividing ℓ for a prime ℓ satisfying the hypothesis of theorem 1.4.
Let us call $P(\overline{\rho}_\lambda(G))$ the image of $\overline{\rho}_\lambda(G)$ in $\mathrm{PGL}(2, \mathbb{F}_\lambda)$. It is well known (cf. [RV95], lemma 2.2) that the inclusion $A_\ell \subseteq G_\ell$ implies:

$$P(\overline{\rho}_\lambda(G)) \supseteq \mathrm{PXL}(2, \mathbb{F}_{\lambda'}), \tag{1.2}$$

where $\lambda' = \lambda \cap R$, and PXL = PSL if $r = [\mathbb{F}_{\lambda'} : \mathbb{F}_\ell]$ is even and PXL = PGL if r is odd.
Now observe that as elements of $\mathrm{PGL}(2, \mathbb{F}_\lambda)$ the matrices $[\overline{\alpha(g)}, \overline{\alpha^{-1}(g)}]$ and $[\overline{\alpha^2(g)}, 1]$ can be identified, and this is useful because $\alpha^2(g) \in R_\ell$ implies $[\overline{\alpha^2(g)}, 1] \in \mathrm{PGL}(2, \mathbb{F}_{\lambda'})$. From this and formula (1.2) we see that if r is odd we already have:

$$P(\overline{\rho}_\lambda(G)) = \mathrm{PGL}(2, \mathbb{F}_{\lambda'}). \tag{1.3}$$

If r is even, we have to determine if all the matrices $[\overline{\alpha^2(g)}, 1]$ are in $\mathrm{PSL}(2, \mathbb{F}_{\lambda'})$, in which case we will have:

$$P(\overline{\rho}_\lambda(G)) = \mathrm{PSL}(2, \mathbb{F}_{\lambda'}), \tag{1.4}$$

or if any one of them is not in $\mathrm{PSL}(2, \mathbb{F}_{\lambda'})$, in which case we will again have (1.3).
The determinant of these matrices being $\overline{\alpha^2(g)}$, we easily distinguish between these two cases, and we obtain:

Proposition 1.5. *Let ℓ, λ, λ' and r be as in the previous discussion. Then*

$$P(\overline{\rho}_\lambda(G)) = \begin{cases} \mathrm{PSL}(2, \mathbb{F}_{\lambda'}), & \textit{if } r \textit{ is even } \textbf{and } \overline{\alpha^2(g)} \in \mathbb{F}_{\lambda'}^2 \\ & \qquad\qquad \textit{for every } g \in G/H. \\ \mathrm{PGL}(2, \mathbb{F}_{\lambda'}), & \textit{if any of these conditions fails.} \end{cases}$$

2. Exceptional Primes for theorem 1.1

We will review the proof of theorem 1.1 given in [R85], finding conditions as explicit as possible for the determination of the exceptional primes.

2.1. Reducible Representations. Let us suppose that for a prime $\lambda \in \mathcal{O}$ dividing ℓ, $\overline{\rho}_\lambda(G)$ is a reducible subgroup of $\mathrm{GL}(2,\mathbb{F}_\lambda)$. Then

$$\overline{\rho}_\lambda \cong \begin{pmatrix} \phi_1 & * \\ 0 & \phi_2 \end{pmatrix},$$

with $\phi_i = \epsilon_i \overline{\chi}_\ell^{m_i}$, for $i = 1, 2$, ϵ_1, ϵ_2 Dirichlet characters unramified outside N with image in $\mathbb{F}_\lambda$ and $\overline{\chi}_\ell$ the cyclotomic character mod ℓ.
By Deligne's theorem, for every prime $p \nmid \ell N$ we have:

$$a_p = \text{trace } \rho_\lambda(\text{Frob } p) \overset{\text{mod } \lambda}{\equiv} \phi_1(\text{Frob } p) + \phi_2(\text{Frob } p) = \epsilon_1(p)\, p^{m_1} + \epsilon_2(p)\, p^{m_2},$$

$$p = \det\ \rho_\lambda(\text{Frob } p) \overset{\text{mod } \lambda}{\equiv} \phi_1(\text{Frob } p)\ \phi_2(\text{Frob } p) = \epsilon_1(p)\ \epsilon_2(p)\ p^{m_1+m_2}.$$

From the last formula we see that $m_1 + m_2 \equiv 1 \pmod{\ell - 1}$ and $\epsilon_1(p)\epsilon_2(p) = 1$ for every $p \nmid N$, so that we can choose $0 \leq m_1 < m_2 < \ell - 1$. Generalizing results of [S73] to the case of general level, Faltings and Jordan proved in [FJ95] the following result, which we will state for general weight, i.e., when the representation comes from a newform $f \in S_k(N)$:

Theorem 2.1. *Suppose that the representation $\overline{\rho}_\lambda$ is reducible. Then if $\ell > k, \ell \nmid N$, $\overline{\rho}_\lambda = \epsilon_1 \oplus \epsilon_2 \overline{\chi}_\ell$, with the characters ϵ_i unramified outside N.*

Carayol and Livné ([C89] , [L89]) have given bounds for the conductors of modular Galois representations. Using this result, together with theorem 2.1, we have (cf. [FJ95], pages 13 and 46) :

Corollary 2.2. *Let f be a newform of weight 2 and level N and $\lambda \mid \ell$ a prime in $\mathcal{O}$ such that $\overline{\rho}_\lambda$ is reducible. Then if $\ell > 2, \ell \nmid N$, we have, for every $p \nmid \ell N$:*

$$a_p \equiv \epsilon(p) + p\, \epsilon^{-1}(p) \pmod{\lambda},$$

with ϵ a character unramified outside N whose conductor c verifies: $c^2 \mid N$.

In particular if $p \neq \ell, p \equiv 1 \pmod{c}$, then: $a_p \equiv 1 + p \pmod{\lambda}$ and if $p \neq \ell, p \equiv -1 \pmod{c}$, then: $a_p \equiv \pm(1 + p) \pmod{\lambda}$.
These congruences cannot be equalities, because: $|a_p| \leq 2\sqrt{p}$, so that only finitely many λ can satisfy them.

2.2. The second condition. We now turn to the second condition in theorem 1.1.
Let λ and ℓ be as before and suppose that the order of $\overline{G}_\lambda$ is not divisible by ℓ. Its image $P(\overline{G}_\lambda)$ in $\mathrm{PGL}(2,\mathbb{F}_\lambda)$ has to be :

1) cyclic,
2) dihedral, or
3) isomorphic to one of the following: A_4, S_4, A_5.

1) In this case, using the fact that the representation $\overline{\rho}_\lambda$ is odd, we conclude that it would be reducible, so it is covered by the above results.

2) In this case there exists a Cartan subgroup C_λ of $\mathrm{GL}(2,\mathbb{F}_\lambda)$ such that $\overline{G}_\lambda$ is contained in the normalizer N_λ of C_λ, but not in C_λ.
Let $\varphi_\lambda : G \to \{\pm 1\}$ be the composition:

$$G \to \overline{G}_\lambda \subseteq N_\lambda \twoheadrightarrow N_\lambda / C_\lambda \cong \{\pm 1\}.$$

The kernel of φ_λ is then an open subgroup of G of index 2, so its fixed field K_λ is a quadratic field unramified outside ℓN. We impose: $\ell \nmid N$.
Suppose that K_λ ramifies at ℓ. Let $\beta = \left(\frac{*}{\ell}\right) \cdot \alpha$ be the Dirichlet character corresponding to K_λ, with α unramified outside N.
We have, for every $p \nmid \ell N$

$$a_p \equiv \left(\frac{p}{\ell}\right) \cdot \alpha(p) \cdot a_p \pmod{\lambda}. \tag{2.1}$$

As in [S73], page 17, we will use these congruences to restrict the possible values of ℓ. The problem is that we need (2.1) to hold also for the primes $p \mid N$. They obviously do if $p^2 \mid N$, because $a_p = 0$ for these p ([AL70]). The trick for dealing with the other prime factors of N is to raise the level to reduce the situation again to the case $a_p = 0$. More precisely, for a prime $p \parallel N$ we replace f by : $f' = \sum_{(n,p)>1} a_n q^n$. Applying theorem 3.64 of [S71] we conclude that f' has level pN. Repeating these procedure for every such prime factor of N we see that we can suppose that:
For every prime $p \mid N$, $a_p = 0$ and $p^2 \mid N$.
Therefore, we can (and will) assume that (2.1) holds for every $p \neq \ell$.
Let $\theta = q\frac{d}{dq}$ be the derivation for mod ℓ modular forms introduced by Serre and Swinnerton-Dyer. The existence of an operator satisfying the same properties in the general case of level N mod ℓ modular forms was proved by Katz in [K77] , provided that $\ell \nmid N$.
Applying θ to both sides of (2.1) we obtain the equality, as modular forms over $\mathbb{F}_\lambda$:

$$\theta\, f = \theta^{\frac{\ell+1}{2}}\, (\alpha f)$$

for $\ell \nmid N$. Comparing the filtration of both sides of this equality we conclude that $\ell \leq 3$ (see [S73]).

Lemma 2.3. *Suppose that λ is such that $P(\overline{G}_\lambda)$ is dihedral. Then if $\ell > 3$ and $\ell \nmid N$, we have:*

$$a_p \equiv \alpha(p)\; a_p \pmod{\lambda}$$

for every $p \nmid \ell N$; where α is a quadratic character unramified outside N.

3) In this case it is known (see [R85], page 189) that for every $p \nmid \ell N$,

$$a_p^2 \equiv 0, p, 2p \text{ or } 4p \pmod{\lambda}, \quad \text{or } a_p^4 - 3pa_p^2 + p^2 \equiv 0 \pmod{\lambda}. \tag{2.2}$$

In [R85] it is proved that this can hold only for finitely many ℓ. For us, formula (2.2) will suffice in the examples to detect the finitely many inert primes that fall in this case.

3. The Examples

We will apply the last two results of section 1 to the realization of projective linear groups over finite fields as Galois groups over $\mathbb{Q}$. We are going to study two examples of newforms without CM having a single inner twist. Our goal is to check the conditions of theorem 1.4 for the inert primes in the extension $F_f/\mathbb{Q}$. In our examples F_f will be a quadratic or a real cyclotomic field, in order to obtain an expression of these inert primes in terms of congruences. In the first example, the existence of the inner twist given by an odd character, and the fact that the inert primes in F_f remain inert in $\mathbb{Q}_f$, will allow us to apply corollary 2.2 without using the bound for the conductor of ϵ.

The same method could have been applied in the second example, but only to those primes that remain inert in $\mathbb{Q}_f$.

The examples below have been computed with an algorithm implemented by W. Stein [St] based on ideas of J. Cremona.

3.1. First Example. Computing the characteristic polynomials of the Hecke operators we found in $S_2^{new}(1024)$ a newform f with

$$\mathbb{Q}_f = \mathbb{Q}(\sqrt{2+\sqrt{2}})$$

and $a_2 = 0$ (because $4 \mid N$, see [AL70]) and with the following coefficients, given by their minimal polynomials:

a_3: $x^4 - 8x^2 + 8$,

a_5 : $x^2 - 4x + 2$,

a_7 : $x^4 - 16x^2 + 32$,

a_{11} : $x^4 - 40x^2 + 392$,

a_{13} : $x^2 - 4x + 2$.

The level being a power of 2, if f had CM it should be given by a quadratic character α unramified outside 2 so that either $\alpha(3) = -1$ or $\alpha(5) = -1$. But a_3, a_5 are both non-zero, so we have a contradiction.

The fact that in the case of a newform of level N with CM the quadratic character α is unramified outside N can be proved as in the case of the characters giving an inner twist (see the discussion after theorem 1.1), and is immediate taking the definition of modular forms with CM in terms of Grossencharacters given in [S71b] .

When we computed the characteristic polynomial of the Hecke operator T_3 acting on $S_2^{new}(1024)$ we observed also that the polynomial defining a_3 appears in this characteristic polynomial with multiplicity 2.

This means that the eigenspaces corresponding to the eigenvalue a_3 and its

Galois conjugates are each 2-dimensional.
The list of coefficients of f suggests that f has the inner twist given by the involution $\sigma \in \mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q}(\sqrt{2}))$ and with $\chi_\sigma = \chi$ the mod 4 character corresponding to $\mathbb{Q}(i)$. In fact, if $p \leq 13$, $a_p^\sigma = \chi(p)a_p$, and this fails for the other characters unramified outside 2, namely: ψ corresponding to $\mathbb{Q}(\sqrt{2})$ and φ to $\mathbb{Q}(\sqrt{-2})$.
We remark that f has at most one inner twist, because:

$$F_f = \mathbb{Q}(\{a_p^2\}_{p>2}) \supseteq \mathbb{Q}(a_3^2) = \mathbb{Q}(\sqrt{2}).$$

To prove the equality: $f^\sigma = \chi f$ (we equate coefficients even for $p = 2$ because $a_2 = 0$) we use the fact that $\chi f \in S_2(1024)$, because the conductor of χ divides 1024, the conductor of f (see theorem 3.64 of [S71]). Note that for the same reason also $\psi f \in S_2(1024)$. The coefficients a_{2j} being all equal to 0, we have: $\chi\chi f = f$ and $\psi\psi f = f$. It follows that both χf and ψf are new of level 1024, because if not another application of [S71], theorem 3.64, would imply that $\chi\chi f$ (or $\psi\psi f$) is an oldform in $S_2(1024)$, contradicting the above equalities.
The modular forms: $f^\sigma, \chi f, \psi f$ have, with respect to the action of the Hecke operator T_3, the common eigenvalue $-a_3$, whose corresponding eigenspace in $S_2^{new}(1024)$ is 2-dimensional. Thus, two of these modular forms must be equal. Finally, $\chi(5) = 1$, $\psi(5) = -1$ and $a_5^\sigma = a_5$ imply that the only possible equality is

$$f^\sigma = \chi f,$$

and this proves that f has a (single) inner twist, so that $F_f = \mathbb{Q}(\sqrt{2})$.

Now we will apply theorem 1.4 to this newform, but restricted to the inert primes in $F_f/\mathbb{Q}$, which are: $\ell \equiv 3, 5 \pmod 8$. We will show that they remain inert in the extension $\mathbb{Q}_f/\mathbb{Q}$. Let ℓ be one of these primes, $\lambda \mid \ell$ a prime in $\mathcal{O}$ and $\lambda' = \lambda \cap R$.
We know that $\mathbb{F}_{\lambda'} = \mathbb{F}_{\ell^2}$, and that after reducing mod λ' the following holds: $\overline{a}_3^2 \in \mathbb{F}_{\ell^2} \setminus \mathbb{F}_\ell$.
What we want to know is whether in the quadratic extension $\mathbb{Q}_f = \mathbb{Q}(a_3)$ over $F_f = \mathbb{Q}(a_3^2)$ the element $\overline{a}_3$ is in $\mathbb{F}_{\ell^2}$ or not, or equivalently, whether $\overline{a}_3^2 \in \mathbb{F}_{\ell^2}^2$ or not.
Suppose that $\overline{a}_3^2 \in \mathbb{F}_{\ell^2}^2$. Then taking norms with respect to $\mathbb{F}_{\ell^2}/\mathbb{F}_\ell$ we should have:
$\mathcal{N}(\overline{a}_3^2) = 8 \in \mathbb{F}_\ell^2$, and then: $(\frac{2}{\ell}) = 1$. This is false for the primes $\ell \equiv 3, 5 \pmod 8$, therefore: $\overline{a}_3 \notin \mathbb{F}_{\ell^2}$ and then:

$$\text{(3.1)} \qquad \text{for every} \quad \ell \equiv 3,5 \pmod 8, \quad \ell \quad \text{is inert in} \quad \mathbb{Q}_f/\mathbb{Q}.$$

We start by checking for which of these $\overline{G}_\lambda$ is irreducible of order a multiple of ℓ, with λ a prime in $\mathcal{O}$ dividing ℓ.
Irreducibility is verified using corollary 2.2, but in this case we will not need

to use the bound for the conductor c nor to compute a coefficient a_p for a prime $p \equiv \pm 1 \pmod{c}$. In the present case, if the representation $\overline{\rho}_\lambda$ were reducible the character ϵ defined in section 2.1 would be unramified outside 2, thus:

$$\epsilon : (\mathbb{Z}/2^u\mathbb{Z})^* \to \mathbb{F}_\lambda^*$$

with $u \in \mathbb{Z}, u > 0$.
Take a prime $p \equiv -1 \pmod{2^u}, p \not\equiv -1, 0 \pmod{\ell}$ (in case $u = 1$, impose also $p \equiv -1 \pmod{4}$). Then, $\epsilon(p) = \pm 1$ and corollary 2.2 implies:

$$a_p \equiv \pm(1+p) \not\equiv 0 \pmod{\lambda}. \tag{3.2}$$

Because of the inner twist, $a_p^\sigma = \chi(p)a_p = -a_p$ so that $a_p \in \mathbb{Q}_f \setminus F_f$. Thus, its minimal polynomial has degree 4.
Using the fact that both a_p and a_3 are square roots of elements of F_f that generate the same field, we see that: $a_p = z \cdot a_3$, $\quad z \in F_f$. Replacing in (3.2) we obtain:

$$a_3 \equiv \pm z^{-1} \cdot (1+p) \pmod{\lambda}. \tag{3.2$'$}$$

The prime ℓ being inert in $\mathbb{Q}_f$, and the minimal polynomial of a_3 having discriminant a power of 2 we conclude that, after reducing mod λ, a_3 is a primitive element of $\mathbb{F}_\lambda = \mathbb{F}_{\ell^4}$, and this contradicts (3.2') because $z^{-1} \in F_f$.
So far, we have proved:

Lemma 3.1. *There exists a newform $f \in S_2(1024)$ with:*

$$\mathbb{Q}_f = \mathbb{Q}\Big(\sqrt{2+\sqrt{2}}\Big), \quad F_f = \mathbb{Q}(\sqrt{2}),$$

such that for every prime ℓ inert in $F_f/\mathbb{Q}$ ($\ell \equiv 3, 5 \pmod{8}$, and ℓ remains inert in $\mathbb{Q}_f$) and $\lambda \in \mathcal{O}$ the prime dividing ℓ, the representation $\overline{\rho}_\lambda(G)$ is irreducible.

Let us now compute the inert primes $\ell \geq 5$ such that $\overline{\rho}_\lambda$ has order not divisible by ℓ, by means of lemma 2.3 and formula (2.2). Applying the lemma we see that if the residual representation is in the dihedral case:
$a_p \equiv \alpha(p)a_p \pmod{\lambda}$, for every $p \nmid 2\ell$, with α a quadratic character unramified outside 2. Independently of which of the 3 possible characters α is we know that either $\alpha(3) = -1$ or $\alpha(7) = -1$ (observe that $\ell \neq 3, 7$).
So that for $p = 3$ or 7 we have: $a_p \equiv -a_p$ and then $a_p \equiv 0 \pmod{\lambda}$.
This is false for every inert prime ℓ because the norms of a_3 and a_7 are powers of 2.

We have to find the inert primes falling in case (3) of section 2.2. Take $\ell > 3$ an inert prime in $F_f/\mathbb{Q}$ and put $p = 3$ in formula (2.2). Because ℓ remains inert in $\mathbb{Q}_f/\mathbb{Q}$ we know that:

$$x^4 - 8x^2 + 8$$

is the minimal polynomial for $\overline{a}_3 \in \mathbb{F}_\lambda$.
This is incompatible with (2.2) unless this polynomial agrees with:

$$x^4 - 9x^2 + 9$$

on $\mathbb{F}_\lambda$; but this is never the case. This concludes the proof of the following

Lemma 3.2. *For the newform in lemma 3.1 it also holds:*
for every $\ell > 3$ inert in $\mathbb{Q}_f/\mathbb{Q}$ the order of $\overline{\rho}_\lambda(G)$ is multiple of ℓ; where λ is the prime in $\mathcal{O}$ dividing ℓ.

Therefore, it only remains to check the technical conditions (i),(ii) and (iii) on these primes to conclude that they satisfy the hypothesis of theorem 1.4.
Applying the results of [Q98] to deal with condition (i) we see that D, the quaternion division algebra over F_f, is given by $(a_3^2, -1)$. The -1 comes from the fact that the inner twist is given by the quadratic character corresponding to $\mathbb{Q}(i)$. We have $a_3^2 = 4 + 2\sqrt{2}$, so that using Hilbert symbols we see that condition (i) for an inert prime ℓ is equivalent to the existence of a non-trivial solution of the equation:

$$(4 + 2\sqrt{2})x^2 - y^2 = z^2 \quad \text{in} \quad F_{f,\lambda'}.$$

But this equation has the global solution $(x, y, z) = (1, 1 + \sqrt{2}, 1)$, so that (i) holds for every ℓ. In fact, in this case D is itself a matrix algebra (because no prime ramifies): $D \cong M(2, F_f)$.
Condition (ii) is easy to check because there is a single inner twist. From the definition of the elements $\alpha(g)$ we see that we can take as $\alpha(g)$ for $g \notin H$ the coefficient a_3.
Then a prime $\lambda \in \mathcal{O}$ over a prime ℓ for which (ii) fails must divide a_3, but this is impossible for an inert prime.
Finally, it remains to check condition (iii). We have to choose v such that Frob $v \in H$, i.e., $\mathbb{Q}(i)$ must be fixed by Frob v. Thus, we can take as v any odd prime that decomposes in $\mathbb{Q}(i)$, i.e., such that $(\frac{-1}{v}) = 1$ or equivalently: $v \equiv 1 \pmod 4$.
Choosing $v = 5$ the other conditions of (iii) are satisfied because $5 \nmid N = 1024$ and $a_5^2 = 6 + 4\sqrt{2}$ generates $F_f/\mathbb{Q}$. Besides, for every $\ell \neq 5$ inert in $F_f/\mathbb{Q}$, a_5^2 generates R_ℓ as a $\mathbb{Z}_\ell$-algebra, so that (iii) is satisfied for these primes.
To rescue the prime $\ell = 5$ observe that we can also take $v = 13$ because a_{13}^2 is equal or conjugate to a_5^2.
From this discussion and the previous two lemmas, we can apply theorem 1.4 and conclude:

Theorem 3.3. *There is a newform $f \in S_2(1024)$ with*

$$\mathbb{Q}_f = \mathbb{Q}\Big(\sqrt{2 + \sqrt{2}}\Big), \quad F_f = \mathbb{Q}(\sqrt{2})$$

such that for every $\ell \equiv 3,5 \pmod 8$, $\ell > 3$, the image G_ℓ of ρ_ℓ is the subgroup of $\mathrm{GL}(2, \mathcal{O}_\ell)$ *generated by the group A_ℓ defined in section 1 and the matrix:*

$$\begin{pmatrix} a_3 & 0 \\ 0 & 1/a_3 \end{pmatrix}.$$

Now we apply proposition 1.5 to these primes. For $g \notin H$ (there is only one coset) we have taken $\alpha(g) = a_3$. In the proof of formula (3.1) it was shown that $\overline{a}_3^2 \notin \mathbb{F}_{\ell^2}^2$ so that proposition 1.5 gives:

Theorem 3.4. *For the newform of the previous theorem, for every $\ell \equiv 3,5$ $\pmod 8$, $\ell > 3$ and $\lambda \in \mathcal{O}$, $\lambda \mid \ell$, we have:*

$$P(\overline{\rho}_\lambda(G)) = \mathrm{PGL}(2, \mathbb{F}_{\ell^2}).$$

Corollary 3.5. *For every $\ell \equiv 3,5 \pmod 8$, $\ell > 3$, $\mathrm{PGL}(2, \mathbb{F}_{\ell^2})$ is a Galois group over $\mathbb{Q}$.*

3.2. Second Example. Looking in the space $S_2^{new}(1331)$ we found a newform f with $\mathbb{Q}_f$ a quadratic extension of the real cyclotomic field $L_{11} = \mathbb{Q}(\zeta + \zeta^{-1})$, where ζ is a primitive 11-th root of unity.
We will prove below that $F_f = L_{11}$ (and this is precisely the field where we wanted to work), the choice of the level $1331 = 11^3$ was motivated by the following result of Brumer ([B95]):

Theorem 3.6. *Let $f \in S_2(N)$ be a newform without CM. Suppose that $p^{r_p} \parallel N$. Let $s_p = \left\lceil \frac{r_p}{2} - 1 - \frac{1}{p-1} \right\rceil$ and ζ a primitive p^{s_p}-root of unity. Then $F_f \supseteq \mathbb{Q}(\zeta + \zeta^{-1})$ if $p > 2$ (resp. $\mathbb{Q}(\zeta^2 + \zeta^{-2})$ if $p = 2$).*

Remark. This theorem also helped us to find the example in section 3.1.
The coefficient a_2 is given by the polynomial:

$$t^{10} - 16t^8 + 98t^6 - 285t^4 + 390t^2 - 199$$

and the following holds: $\mathbb{Q}(a_2^2) = L_{11}$, in fact:

$$a_2^2 = 3 - (\zeta + \zeta^{-1}).$$

And $a_3 = (\zeta + \zeta^{-1})$, so that $a_3 \in L_{11}$.
We also know that $a_{11} = 0$ because $11^2 \mid N$ (see [AL70]).
If f had CM, it should be given by the character ω corresponding to $\mathbb{Q}(\sqrt{-11})$, but this is ruled out by the fact that: $a_2 \neq 0$, $(\frac{2}{11}) = -1$.
The computation of the characteristic polynomial of the Hecke operator T_2 on the space $S_2^{new}(1331)$ shows that the factor corresponding to a_2 is a simple factor. As in the section 3.1, we prove that $\omega f \in S_2^{new}(1331)$ and if we call σ the involution in $\mathrm{Gal}(\mathbb{Q}_f/L_{11})$, we observe that the modular forms: f^σ and ωf have the common eigenvalue $-a_2$ with respect to the action of T_2. But the eigenspace of $-a_2$ is 1-dimensional, so that we have:

$$f^\sigma = \omega f.$$

Therefore, f has an inner twist and we easily see that it is unique, so that: $F_f = L_{11}$.

The application of theorem 1.4 to this newform f is as in section 3.1, except for the fact that we will apply corollary 2.2 in its full strength.

Recall that we are only interested in the inert primes in $F_f/\mathbb{Q}$, which are the primitive roots mod 11 and their squares, i.e:

$$\ell \not\equiv \pm 1 \pmod{11}, \quad \ell \neq 11.$$

When applying corollary 2.2 to deal with the reducible case, the character ϵ must be unramified outside 11, provided $\ell > 2$, and its conductor c must verify: $c^2 \mid 1331$, thus $c \mid 11$. So the values of ϵ are 10-roots of unity, contained in $\mathbb{F}_{\ell^{10}}$. We know that if $10 \mid \ell^{10} - 1$ then $10 \mid \ell^2 - 1$, so that the image of ϵ is contained in $\mathbb{F}_{\ell^2}$. Then, applying the formula in corollary 2.2 to $p = 2$ we conclude that $\overline{a}_2 \in \mathbb{F}_{\ell^2}$.

But we also know that the residue class degree of ℓ in $\mathbb{Q}_f$ is 5 or 10 ; a_2 generates $\mathbb{Q}_f$ and the discriminant of the minimal polynomial of a_2 ($= 2^{10} \cdot 11^8 \cdot 199$) is not divisible by ℓ.

Therefore $\overline{a}_2$ has degree at least 5 over $\mathbb{F}_\ell$, and we have a contradiction.

We conclude that the representations are irreducible for every odd ℓ inert in $F_f/\mathbb{Q}$.

Let us now treat the dihedral case. If $\ell > 3$ is in this case, we have:

$$a_p \equiv \omega(p) a_p \pmod{\lambda}$$

for every $p \nmid 11\ell$. Taking $p = 2$ we have $\omega(p) = -1$ and then $\lambda \mid a_2$. The norm of a_2 over $\mathbb{Q}$ is -199, so that we get $\lambda \mid 199$, and 199 is not inert in $F_f/\mathbb{Q}$.

The next step is the application of formula (2.2) to find the odd inert primes such that case (3) of section 2.2 holds. Applying formula (2.2) to $p = 2$, from the fact that $a_2 \mod \lambda$ has a minimal polynomial of degree at least 5, we obtain a contradiction.

Therefore, for every $\ell > 3$ inert in $L_{11}/\mathbb{Q}$ and $\lambda \in \mathcal{O}$ dividing ℓ, we conclude that the order of $\overline{\rho}_\lambda(G)$ is divisible by ℓ.

It remains to check conditions (i), (ii) and (iii) in order to apply theorem 1.4. In condition (i) the quaternion algebra D is given by (see [Q98]): $(a_2^2, -11)$. It is known that condition (i) is satisfied if ℓ is such that both a_2^2 and -11 are units in $F_{f,\lambda'}$ (here $\lambda' = \lambda \cap R$). But from the equation of a_2^2 and the fact that ℓ is inert in F_f, we conclude that this holds for all these ℓ.

In condition (ii), let us take as $\alpha(g)$ for $g \notin H$ the coefficient a_2.Then condition (ii) holds for every ℓ inert in F_f, because none of these can divide a_2.

Finally, for condition (iii) we take $v = 3$ because:

$(\frac{-11}{3}) = 1$, and then Frob 3 fixes $\mathbb{Q}(\sqrt{-11})$.

$3 \nmid N = 1331$.

$a_3^2 = 2 + \zeta^2 + \zeta^{-2}$ generates F_f over $\mathbb{Q}$.
Moreover, for every $\ell \neq 3$ inert in F_f , a_3^2 generates R_ℓ as a $\mathbb{Z}_\ell$-algebra.
Applying theorem 1.4 we obtain

Theorem 3.7. *There is a newform f in $S_2(1331)$ with $\mathbb{Q}_f$ a quadratic extension of*

$$L_{11} = \mathbb{Q}(\zeta + \zeta^{-1})$$

(ζ a primitive 11-th root of unity) and $F_f = L_{11}$ such that for every $\ell \not\equiv \pm 1 \pmod{11}$, $\ell \neq 2, 3, 11$, the image G_ℓ of ρ_ℓ is the subgroup of $\mathrm{GL}(2, \mathcal{O}_\ell)$ generated by the group A_ℓ defined in section 1 and the matrix:

$$\begin{pmatrix} a_2 & 0 \\ 0 & 1/a_2 \end{pmatrix}.$$

To apply proposition 1.5 observe that F_f is a degree 5 extension of $\mathbb{Q}$, so that $r = 5$ is odd and then we have

Theorem 3.8. *For the newform of the previous theorem, for every $\ell \not\equiv \pm 1 \pmod{11}$, $\ell \neq 2, 3, 11$ and $\lambda \in \mathcal{O}$, $\lambda \mid \ell$, we have:*

$$P(\overline{\rho}_\lambda(G)) = \mathrm{PGL}(2, \mathbb{F}_{\ell^5}).$$

Corollary 3.9. *For every $\ell \not\equiv \pm 1 \pmod{11}$, $\ell \neq 2, 3, 11$, $\mathrm{PGL}(2, \mathbb{F}_{\ell^5})$ is a Galois group over $\mathbb{Q}$.*

4. Concluding Remarks

The conditions of 1.4 can be effectively verified for any newform without CM having a single inner twist using the results of section 2.
The method used to deal with the reducible case in the first example only works if we have an odd inner twist, and applies only to those primes inert in $\mathbb{Q}_f/F_f$, but it has the advantage of avoiding the computation of a coefficient a_p with p as described after corollary 2.2 (p grows as a function of q and w).
Though these conditions may seem highly restrictive, we have found other examples verifying them. For instance, there is a newform $f \in S_2(4096)$ whose first coefficients have minimal polynomials ($a_2 = 0$):

$$a_3 : x^8 - 16x^6 + 72x^4 - 96x^2 + 8, \quad a_5 : x^4 - 8x^2 + 8x - 2.$$

This newform has an inner twist, given by the mod 4 character χ, so that $F_f = \mathbb{Q}(a_5) = \mathbb{Q}\left(\sqrt{2 + \sqrt{2}}\right)$. Let us consider the primes ℓ with residue class degree 2 in $F_f/\mathbb{Q}$, i.e., $\ell \equiv 7, 9 \pmod{16}$. It can be shown that the 2 places of F_f lying above ℓ are inert in $\mathbb{Q}_f/F_f$. The verification of the conditions of theorem 1.4 for these primes is exactly as in section 3.1, and again no exceptional prime appears. This step consists in computing some discriminants, norms and resultants involving only the coefficients a_3 and a_5. It follows that for every $\ell \equiv 7, 9 \pmod{16}$, and $\lambda \in \mathcal{O}$, $\lambda \mid \ell$,

$$P(\overline{\rho}_\lambda(G)) = \mathrm{PGL}(2, \mathbb{F}_{\ell^2}).$$

This, together with corollary 3.5, proves that $\mathrm{PGL}(2, \mathbb{F}_{\ell^2})$ is a Galois group over $\mathbb{Q}$, for every $\ell \not\equiv \pm 1 \pmod{16}$, $\ell > 3$.

The same conditions are also satisfied by the following two examples:

- $f \in S_2(19^2)$ with an inner twist and $F_f = \mathbb{Q}(\sqrt{5})$. Applying our method to this newform, we find no exceptional inert prime so that the groups $\mathrm{PGL}(2, \mathbb{F}_{\ell^2})$ are Galois groups over $\mathbb{Q}$ for every $\ell \equiv 2, 3 \pmod 5$, $\ell > 3$.
- $f \in S_2(333)$ with an inner twist and $F_f = \mathbb{Q}(\sqrt{6})$. Applying our method to this newform and combining with the result obtained using the examples of level 1024 and 4096 we conclude that the groups $\mathrm{PGL}(2, \mathbb{F}_{\ell^2})$ are Galois group over $\mathbb{Q}$, for every $\ell \not\equiv \pm 1 \pmod{48}$, $\ell > 3$.

References

[AL70] A. Atkin, J. Lehner, *Hecke operators on* $\Gamma_0(m)$. Math. Ann. **185** (1970), 134–160.

[B95] A. Brumer, *The rank of* $J_0(N)$. Astérisque **228** (1995), 41–68.

[C89] H. Carayol, *Sur les représentations galoisiennes modulo l attachées aux formes modulaires.* Duke Math. J. **59** (1989), 785–801.

[C92] J. Cremona, *Abelian varieties with extra twist, cusp forms, and elliptic curves over imaginary quadratic fields.* J. London Math. Soc. **45** (1992), 404–416.

[D71] P. Deligne, *Formes modulaires et représentations ℓ-adiques.* Lecture Notes in Mathematics **179** Springer-Verlag, Berlin-New York, 1971, 139–172.

[FJ95] G. Faltings, B. Jordan, *Crystalline cohomology and* $\mathrm{GL}(2, \mathbb{Q})$. Israel J. Math. **90** (1995), 1–66.

[K77] N. Katz, *A result on modular forms in characteristic p.* Lecture Notes in Math. **601**, 53–61, Springer, Berlin, 1977.

[L89] R. Livné, *On the conductors of* mod ℓ *Galois representations coming from modular forms.* J. Number Theory **31** (1989), 133–141.

[M81] F. Momose, *On the ℓ-adic representations attached to modular forms.* J. Fac. Sci. Univ. Tokyo, Sect. IA Math. **28**:1 (1981), 89–109.

[Q98] J. Quer, *La classe de Brauer de l'algèbre d'endomorphismes d'une variété abélienne modulaire.* C. R. Acad. Sci. Paris Sér. I Math. **327** (1998), 227–230.

[RV95] A. Reverter, N. Vila, *Some projective linear groups over finite fields as Galois groups over* $\mathbb{Q}$. Contemporary Math. **186** (1995), 51–63.

[R75] K. A. Ribet, *On ℓ-adic representations attached to modular forms.* Invent. Math. **28** (1975), 245–275.

[R77] K. A. Ribet, *Galois representations attached to eigenforms with nebentypus.* Lecture Notes in Math. **601**, 17–51, Springer, Berlin, 1977.

[R80] K. A. Ribet, *Twists of modular forms and endomorphisms of Abelian Varieties*, Math. Ann. **253** (1980), 43–62.

[R85] K. A. Ribet, *On ℓ-adic representations attached to modular forms II*, Glasgow Math. J. **27** (1985), 185–194.

[S71] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions.* Publ. Math. Soc. Japan **11**, 199-208, Princeton University Press, Princeton, N.J., 1971.

[S71b] G. Shimura, *On elliptic curves with complex multiplication as factors of the jacobian of modular function fields.* Nagoya Math. J. **43** (1971), 199–208.

[St] W. Stein, Hecke: The Modular Forms Calculator. Available at: http:// shimura.math. berkeley.edu /~was /Tables /hecke.html.

[S73] H. P. F. SWINNERTON-DYER, *On ℓ-adic representations and congruences for coefficients of modular forms.* Lecture Notes in Math. **350**, 1–55, Springer, Berlin, 1973.

Luis V. DIEULEFAIT
Dept. d'Algebra i Geometria
Universitat de Barcelona
Gran Via de les Corts Catalanes 585
08007 - Barcelona
Spain
E-mail : luisd@cerber.mat.ub.es