# SPLITTING FIELDS OF $X^n - X - 1$ (PARTICULARLY FOR $n = 5$), PRIME DECOMPOSITION AND MODULAR FORMS

CHANDRASHEKHAR B. KHARE, ALFIO FABIO LA ROSA, GABOR WIESE

*Dedicated to the memory of Bas Edixhoven.*

ABSTRACT. We study the splitting fields of the family of polynomials $f_n(X) = X^n - X - 1$. This family of polynomials has been much studied in the literature and has some remarkable properties. In [Ser03], Serre related the function on primes $N_p(f_n)$, for a fixed $n \le 4$ and $p$ a varying prime, which counts the number of roots of $f_n(X)$ in $\mathbb{F}_p$ to coefficients of modular forms. We study the case $n = 5$, and relate $N_p(f_5)$ to mod 5 modular forms over $\mathbb{Q}$, and to characteristic 0, parallel weight 1 Hilbert modular forms over $\mathbb{Q}(\sqrt{19 \cdot 151})$.

## 1. INTRODUCTION

Serre in [Ser03] considers the family of polynomials $f_n(X) = X^n - X - 1 \in \mathbb{Z}[X]$ for integers $n \ge 2$.

This is a fascinating family in a number of ways. The irreducibility of $f_n$ was established by Selmer in [Sel56]. The discriminant of $f_n$ equals $d_{f_n} = (-1)^{(n-1)(n-2)/2} \cdot (n^n - (1-n)^{n-1})$. The first remarkable fact is that the discriminant of the associated number field $K_{f_n} = \mathbb{Q}[X]/(f_n(X))$ is squarefree and that the residue degree of any ramified prime is 1.[1] By work of Kondo [Kon95] (Theorems 1 and 2) this implies that the Galois group of $f_n(X)$, *i.e.* the Galois group of the Galois closure $K$ of $K_{f_n}$ over $\mathbb{Q}$, is the symmetric group $S_n$, that $K$ contains the quadratic field $E = \mathbb{Q}(\sqrt{d_{f_n}})$ and that the extension $K/E$ is unramified at all finite primes. It should be stressed that constructing polynomials (and number fields) with squarefree discriminants is a hard problem. Kedlaya [Ked12] gave a construction, whose crucial point is that the signature of the field can be prescribed. In our case, the signature of $K_{f_n}$ is $(1, n-1)$ if $n$ is odd[2] and $(2, n-2)$ if $n$ is even.[3] Consequently, the image of any complex conjugation of $K/\mathbb{Q}$ in $S_n$ is a product of $\lfloor \frac{n-1}{2} \rfloor$ transpositions with disjoint supports and $E$ is real if and only if $n$ is congruent to 1 or 2 modulo 4.

It might be useful to mention that the polynomials $f_n$ themselves do not always have a squarefree discriminant. These have been studied on their own in a number of papers, for instance in [BMT15]. The first $n$ for which $d_{f_n}$ is not squarefree is 130.[4] It is important to point out that the squarefreeness

[1] This follows immediately from [LNV91, Theorems 1,2]. It can also be proved directly as follows. Let $p$ be a prime dividing $d_{f_n}$. Then $p \nmid n(n-1)$, in particular $p \neq 2$. Suppose $a \in \overline{\mathbb{F}}_p$ is a multiple root of $f_n(X)$ modulo $p$. Then it is also a root of $f_n'(X) = nX^{n-1} - 1$ modulo $p$, from which $a = n/(1-n)$ follows. As $f_n''(a) \neq 0$ we see that $f_n(X)$ factors as $f_n(X) \equiv (X - \frac{n}{1-n})^2 \cdot g(X) \mod p$ with $g(X)$ being squarefree and coprime to $(X - \frac{n}{1-n})$ modulo $p$. From this it follows that there is at most one ramified prime above $p$ and then that prime has residue degree 1 and ramification index 2. Consequently, the discriminant of the number field is squarefree.

[2] Indeed, $f_n$ has exactly one real root if $n$ is odd because $f_n(x) < 0$ for all $x \le 1$ and it does not possess any local extremum at any $x \ge 1$.

[3] Indeed, if $n$ is even, then $f_n$ has exactly two real roots because it has a unique local minimum and takes a negative value there.

[4] See `https://oeis.org/A238194`

of $d_{f_n}$ implies that $\mathbb{Z}[X]/(f_n(X))$ is the ring of integers of $K_{f_n}$ because in general the square of the index divides discriminant. We will exploit this for $n = 5$.

In [Ser03], Serre asks for information about the number of roots $N_p(f_n)$ of these polynomials in $\mathbb{F}_p$. In other words he considers the point counting function $\#A_{f_n}(\mathbb{F}_p)$ where $A_{f_n}$ is the zero-dimensional affine scheme $\mathbb{Z}[X]/(f_n(X))$. We let $\theta_n^{\mathrm{st}}$ be the $n-1$-dimensional standard representation defined as the quotient of the natural $n$-dimensional permutation representation of $S_n$ modulo the trivial one. Then we have for all unramified primes $p$

$$N_p(f) = \mathrm{tr}(\theta_n^{\mathrm{st}}(\mathrm{Frob}_p)) + 1.$$

For $n \leq 4$, Serre relates the $N_p(f_n)$'s to coefficients of modular forms, as follows.

$n = 3$**.** (See [Ser03, §5.3 and corresponding notes].) For $n = 3$ the splitting field of $f_3$ is an $S_3$-extension $K$ of $\mathbb{Q}$ and $\zeta_{K_{f_3}}(s)/\zeta(s)$ is a holomorphic function, equal to the Artin $L$-function $L(\theta_3^{\mathrm{st}}, s)$. The representation $\theta_3^{\mathrm{st}}$ arises by induction of an order 3 character of $\mathrm{Gal}(K/E)$ where $E$ is $\mathbb{Q}(\sqrt{-23})$. It turns out that $K$ is the Hilbert class field of $E$, and in fact is the maximal unramified extension of $E$. Thus the representation $\theta_3^{\mathrm{st}}$ arises from the weight one (dihedral or CM) modular form $F(z) \in S_1(\Gamma_0(23), (\frac{\cdot}{23}))$ given by the product formula (with $q = e^{2\pi i z}$)

$$F(z) = q \cdot \prod_{k=1}^{\infty}(1-q^k) \cdot \prod_{k=1}^{\infty}(1-q^{23k}).$$

It can also be written in terms of $\Theta$-series as

$$\frac{1}{2}\sum_{x,y\in\mathbb{Z}} q^{x^2+xy+6y^2} - \frac{1}{2}\sum_{x,y\in\mathbb{Z}} q^{2x^2+6xy+3y^2}.$$

The $S_3$-extension $K/\mathbb{Q}$ is also the field cut out by the Galois representation associated to the Ramanujan $\Delta$-function mod 23. This is explained by the congruence

$$\Delta(q) = q \cdot \prod_{k=1}^{\infty}(1-q^k)^{24} \equiv q \cdot \prod_{k=1}^{\infty}(1-q^k) \cdot \prod_{k=1}^{\infty}(1-q^{23k}) \pmod{23}.$$

$n = 4$**.** (See [Ser03, §5.4 and corresponding notes].) For degree $n = 4$ the picture to relate $N_p(f_4)$ to a weight one modular form is more complicated. Serre observes that:

(i) The $S_4 = \mathrm{PGL}_2(\mathbb{F}_3)$-extension is embedded in $\tilde{K} = K(\sqrt{7-4x^2})$, where $K$ is the splitting field of $f_4$ over $\mathbb{Q}$ and $x$ is a root of $f_4(X)$, of degree 2 over $K$ and the resulting Galois group is isomorphic to $\mathrm{GL}_2(\mathbb{F}_3)$, which embeds in $\mathrm{GL}_2(\mathbb{Z}[\sqrt{-2}])$. Furthermore the field $\tilde{K}$ turns out to be the maximal unramified extension of the quadratic field $E = \mathbb{Q}(\sqrt{-283})$.

(ii) From this one gets a 2-dimensional odd representation $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{C})$ with fixed field $\tilde{K}$ such that

$$\rho \otimes \rho = \epsilon \oplus \theta_4^{\mathrm{st}},$$

factoring through a representation of $\mathrm{Gal}(K/\mathbb{Q}) = S_4$, where $\epsilon$ is the sign character of a permutation. The representation $\rho$ arises by the Deligne-Serre construction from a modular form $f \in S_1(\Gamma_0(283), \chi)$ with $\chi$ the order 2 Dirichlet character of conductor 283. This also gives $N_p(f) - 1 = a_p(f)^2 - \epsilon(p)$.

$n = 5$. In this article, we look at the $n = 5$ case of the question and try to respond to the gauntlet implicitly thrown down by Serre:

> *The case $n \geq 5$. Here the only known result seems to be that $f_n = x^n - x - 1$ is irreducible (Selmer [15]) and that its Galois group is the symmetric group $S_n$. No explicit connection with modular forms (or modular representations) is known, although some must exist because of the Langlands program.*

The paper partly arose from graduate courses one of us (CBK) has taught at UCLA partly based on Serre's paper [Ser03] in which he suggested that students try and tackle Serre's challenge.

We propose two approaches to answer Serre's challenge. The first one is computational in nature. The key point is that we explore the exceptional isomorphism $S_5 \cong \mathrm{PGL}_2(\mathbb{F}_5)$ and, instead of $K_{f_5}$, work with a degree 6 polynomial $g \in \mathbb{Q}[X]$ on which the Galois group acts via the natural action of $\mathrm{PGL}_2(\mathbb{F}_5)$ on the projective line $\mathbb{P}^1(\mathbb{F}_5)$, leading to an 'exotic' embedding of $S_5$ into $S_6$. Serre pointed out to us that in classical terms, this was called the *sextic resolvent* and that this 'exotic' $S_5$ may also be viewed as the image of the standard $S_5$ under an outer automorphism of $S_6$.

Explicit class field theory then allows us to explicitly solve a Galois embedding problem for the group $C_4 \cdot_6 S_5 = 4_{-}\mathrm{PGL}_2(\mathbb{F}_5)$ (in notation of Tim Dokchiter's project GroupNames [Dok] and Quer's article [Que95], respectively). That group can be characterised as the unique central extension of $\mathrm{PGL}_2(\mathbb{F}_5)$ by $C_4$ which restricts to the unique non-trivial central extension of $\mathrm{PSL}_2(\mathbb{F}_5)$ by $C_4$ and which is not $\mathrm{GL}_2(\mathbb{F}_5)$. We solve the embedding problem by computing a polynomial $h \in \mathbb{Q}[X]$ of degree 48 describing a cyclic $C_8$ extension of $K_g = \mathbb{Q}[X]/(g(X))$. It corresponds to a subgroup of $C_4 \cdot_6 S_5$ which is isomorphic to the dihedral group $D_5$. An explicit polynomial $h(X)$ is included in §3.3.

This leads to the following result, linking $f_5$ to a modular form $F$ of weight one in characteristic 5. Its Hecke eigenvalues at primes $p \neq 19, 151$ can be explicitly computed from the polynomial $h(X)$, for instance, using Magma [BCP97].

**Theorem 1.1.** *There is a Hecke eigenform $F$ in $S_1(19 \cdot 151^2, \chi_{-19}, \overline{\mathbb{F}}_5)$, the space of weight one cuspidal Katz modular forms*[5] *of level $19 \cdot 151^2$ and Dirichlet character $\chi_{-19}$ corresponding to $\mathbb{Q}(\sqrt{-19})/\mathbb{Q}$ enjoying the following properties. The attached Galois representation*

$$\rho : G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_5)$$

*has conductor $19 \cdot 151^2$, its image is isomorphic to $C_4 \cdot_6 S_5 = 4_{-}\mathrm{PGL}_2(\mathbb{F}_5)$, its projectivisation*

$$\rho^{\mathrm{proj}} : G_{\mathbb{Q}} \xrightarrow{\rho} \mathrm{GL}_2(\overline{\mathbb{F}}_5) \to \mathrm{PGL}_2(\overline{\mathbb{F}}_5)$$

*has image $\mathrm{PGL}_2(\mathbb{F}_5) \cong S_5$ and $\ker(\rho^{\mathrm{proj}})$ is the absolute Galois group of $K$, the splitting field of $f_5$. The modular form $F$ is not the reduction of any holomorphic modular form of weight one in any level.*

*Moreover, the restriction of $\rho$ to the absolute Galois group $G_E$ of $E = \mathbb{Q}(\sqrt{19 \cdot 151})$ is unramified at 19, but ramifies at 151. However, there is a character $\delta$ of $G_E$ such that $\rho|_{G_E} \otimes \delta$ is unramified at all finite places.*

The second approach consists in showing the existence of a cuspidal Hilbert eigenform of parallel weight 1 defined over the real quadratic field $E$, denoted by $G$, such that a twist of its Asai transfer to

[5] Katz modular forms were defined by Katz in [Kat73]. A comprehensive account of them is given in [Gor02] and a short summary can be found in [Edi97].

$\mathrm{GL}_4(\mathbb{A}_\mathbb{Q})$ is attached to an Artin representation which factors through $\theta_5^{\mathrm{st}}$. Let us record for completeness that the conductor of $\theta_5^{\mathrm{st}}$ equals $19 \cdot 151$.[6] This uniquely identifies the representation as [LMF22, Artin representation 4.2869.5t5.b.a].

We prove the following general result, which slightly improves on a theorem of Calegari [Cal13]. The improvement results from using stronger modularity results due to Pilloni and Stroh [PS16] than were available when [Cal13] was written.

**Theorem 1.2.** *Let $K/\mathbb{Q}$ be a Galois extension with Galois group $\mathrm{Gal}(K/\mathbb{Q}) \cong S_5$ and let $E$ be the subfield of $K$ fixed by the subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ isomorphic to $A_5$. We assume that $K$ is totally imaginary and $E$ is real.*

*(a) There is a Hilbert modular eigenform $G$ over $E$ of parallel weight one with attached Galois representation $\eta : G_E \to \mathrm{GL}_2(\mathbb{C})$ and there is a character $\chi : G_\mathbb{Q} \to \mathbb{C}^\times$ such that*

$$\theta_5^{\mathrm{st}} \cong \mathrm{Asai}_{G_E}^{G_\mathbb{Q}}(\eta) \otimes \chi.$$

*(b) Let $\Pi = \Pi_\infty \otimes \bigotimes_p \Pi_p$ be the automorphic form on $\mathrm{GL}_4(\mathbb{A}_\mathbb{Q})$ obtained by twisting the Asai transfer of $G$ from $E$ to $\mathbb{Q}$ by the Hecke character corresponding to $\chi$. Then the L-function of $\Pi$ coincides with that of $\theta_5^{\mathrm{st}}$ at all but finitely many primes $p$:*

$$L_p(s, \Pi)^{-1} = \det(I - \theta_5^{\mathrm{st}}(\mathrm{Frob}_p)p^{-s}).$$

We remark that Calegari's original theorem depended on the local condition that the Frobenius element at 5 should be conjugate to the double transposition $(1,2)(3,4)$. We note that this is not satisfied if $K$ is the splitting field of $f_5$ because $f_5$ is irreducible modulo 5, whence the Frobenius element is a 5-cycle. We further point out that it was also remarked in [Dwy14] that this condition is superfluous.

We now elaborate more on how our results respond to Serre's challenge, which we interpret in various ways:

(1) Vaguely, we see it as asking about a relation between the polynomial $f_5$ and 'automorphic objects'.
(2) More precisely, we see it as relating conjugacy classes of unramified Frobenius elements in $\mathrm{Gal}(K/\mathbb{Q})$ to Hecke eigenvalues of 'automorphic objects'.
(3) We also consider the original question about expressing $N_p(f_5)$ explicitly via an automorphic form.

The vague interpretation (1) can be answered affirmatively in a number of ways and in different characteristics. For instance, in characteristic 5, the projective Galois representation attached to the weight one form $F$ over $\overline{\mathbb{F}}_5$ cuts out the field $K/\mathbb{Q}$. This is also true for the Hilbert modular form $G$ over $E$ in characteristic 0. One can also reduce $G$ modulo (a prime above) 2. The image of the attached Galois representation will be $\mathrm{SL}_2(\mathbb{F}_4) \cong A_5$ and $K$ will again be the field cut out by it. In that sense, $F$, $G$ and the reduction of $G$ modulo 2 are automorphic objects giving rise to $K/\mathbb{Q}$, and their Galois representations 'control' $K/\mathbb{Q}$ and, hence, the arithmetic of the polynomial $f_5$.

Concerning the more precise interpretation (2), from Theorem 1.1 we obtain the following result.

**Corollary 1.3.** *Let $F$ be the weight one Katz modular eigenform over $\overline{\mathbb{F}}_5$ from Theorem 1.1. For any prime $p$, denote by $a_p(F)$ the eigenvalue of the Hecke operator $T_p$ on $F$.*

[6] This follows because the only ramified primes in $K/\mathbb{Q}$ are 19 and 151 and, as $K/E$ is unramified at all finite places, the inertia groups at both these primes are cyclic of order 2. Moreover, they are generated by a transposition since they are not contained in $A_5$. As a consequence they fix a 3-dimensional subspace of vector space underlying $\theta_5^{\mathrm{st}}$, leading to the claimed conductor.

*Then for every prime* $p \nmid 19 \cdot 151$, *we have the formula*

$$N_p(f_5) \equiv 1 + \left(\frac{19 \cdot 151}{p}\right) \cdot \left(\left(\frac{-19}{p}\right) a_p(F)^2 + \left(\frac{19 \cdot 151}{p}\right) - 1\right) \bmod 5.$$

*Moreover, for every prime* $p \nmid 19 \cdot 151$, *the triple* $(a_p(F), \left(\frac{-19}{p}\right), \left(\frac{-151}{p}\right))$ *uniquely determines the conjugacy class of any Frobenius element at* $p$ *in* $\mathrm{Gal}(K/\mathbb{Q}) \cong S_5$ *with the exception that* 5*-cycles cannot be distinguished from the identity.*

The exception is due to the fact that order 5 elements are non-semisimple in characteristic 5. Since the determinant of $\rho$ is $\chi_{-19} = \left(\frac{-19}{\cdot}\right)$, we recognise that $\left(\frac{-19}{p}\right) a_p(F)^2 = \frac{a_p(F)^2}{\left(\frac{-19}{p}\right)}$ indeed only depends on the projective representation $\rho^{\mathrm{proj}}$.

Concerning (3), Serre's original question is completely answered by the following corollary of Theorem 1.2, which also gives the strongest form of (2).

**Corollary 1.4.** *Let* $K$ *be the splitting field of* $f_5$ *over* $\mathbb{Q}$. *There exists a Hilbert modular eigenform* $G$ *over* $E = \mathbb{Q}(\sqrt{19 \cdot 151})$ *of parallel weight one, the* $T_{\mathfrak{p}}$*-eigenvalues of which are denoted* $a_{\mathfrak{p}}(G)$, *such that for every prime* $p \nmid 19 \cdot 151$, *we have the formula*

$$N_p(f_5) = 1 + \left(\frac{-151}{p}\right) \cdot \prod_{\mathfrak{p} | p} a_{\mathfrak{p}}(G),$$

*where* $\mathfrak{p}$ *runs through the primes of* $E$ *above* $p$.

*Moreover, for every prime* $p \nmid 19 \cdot 151$, *the triple* $((a_{\mathfrak{p}}(G))_{\mathfrak{p}|p}, \left(\frac{-19}{p}\right), \left(\frac{-151}{p}\right))$ *uniquely determines the conjugacy class of any Frobenius element at* $p$ *in* $\mathrm{Gal}(K/\mathbb{Q}) \cong S_5$.

We remark that holomorphic cuspidal Hilbert modular forms over $E$ of parallel weight 1 and level 1 were constructed by Bryk, who used them to express the square of $N_p(f_5)$ (see [Bry12, Prop. 6.3.5]). Bryk's forms are different from the modular form $G$ of Corollary 1.4 because the level of $G$ is non-trivial. However, the Artin representation attached to any of Bryk's forms cuts out an everywhere unramified extension of $E$. Its projectivisation is the same as that of $G$, namely the one cutting out $K/E$. This implies that our form $G$ is a twist of one of Bryk's forms by a Hecke character of $E$.

Finally, as we remarked at the beginning of the introduction, the splitting field $K$ of $f_n$ is an $A_n$-extension of its quadratic subfield $E$ that is unramified at all finite places. For $n = 3$ and $n = 4$, one knows the maximal extension $L/E$ that is unramified at all finite places explicitly. In both these cases, $L$ is the field cut out by a linear Galois representation with projectivisation corresponding to the $A_n$-extension $K/E$. This pattern does not continue for $n = 5$. Indeed, $K_f(\sqrt{-151})$ has class number 7 and $EK_f(\sqrt{-151})$ is an unramified extension of $E$; its class number is hence divisible by 7 (in fact, it equals 21 under GRH). So, there is a cyclic extension of $K$ of order 7, which is unramified over $E$, but not accounted for by the Artin representations in question because the orders of their images are coprime to 7.

**Acknowledgements.** We would like to thank the anonymous referee for useful suggestions improving the exposition of the paper. We also thank J-P. Serre for helpful remarks on the manuscript. We also thank Jürgen Klüners for significantly reducing the size of the polynomial $h(X)$. G.W. thanks Sara Arias-de-Reyna for very helpful suggestions, Jordi Guàrdia and Enric Nart for helpful communication about maximal orders as well as Frank Calegari for recalling the article [Dwy14] to us.

## 2. Certain central extensions and embedding problems

We start with a very brief outline of the general theory relating lifts of projective representations, Galois embedding problems and group cohomology.

Let $\pi : G \twoheadrightarrow \overline{G}$ be a surjective group homomorphism and assume $C = \ker(\pi)$ lies in the centre of $G$. We are interested in lifting a *projective representation*

$$\rho^{\mathrm{proj}} : \overline{G} \to \mathrm{PGL}_n(K)$$

to a linear representation $\rho : G \to \mathrm{GL}_n(K)$, where $K$ is any field and $n \in \mathbb{Z}_{\geq 1}$.

We will use (continuous) cochains in (continuous) group cohomology, which are for instance explained in [NSW08, Chapter 1]. We consider the multiplicative group $K^\times$ as a trivial module for $G$ and $\overline{G}$ and start by associating with $\rho^{\mathrm{proj}}$ an inhomogeneous 2-cocycle $\gamma \in \mathrm{Z}^2(\overline{G}, K^\times)$ as follows: for each $\overline{g} \in \overline{G}$, choose once and for all a lift $\widetilde{\rho}(\overline{g}) \in \mathrm{GL}_n(K)$ of $\rho^{\mathrm{proj}}(\overline{g})$ such that $\widetilde{\rho}(1) = 1$ and let

$$\gamma(\overline{g}, \overline{h}) := \widetilde{\rho}(\overline{g}) \cdot \widetilde{\rho}(\overline{h}) \cdot \widetilde{\rho}(\overline{g}\overline{h})^{-1}.$$

One easily checks that $\gamma$ is indeed an inhomogeneous 2-cocycle, *i.e.* that it satisfies $\gamma(\overline{g}\overline{h}, \overline{i}) \cdot \gamma(\overline{g}, \overline{h}) = \gamma(\overline{h}, \overline{i}) \cdot \gamma(\overline{g}, \overline{h}\overline{i})$ for all $\overline{g}, \overline{h}, \overline{i} \in \overline{G}$. Via inflation along $\pi$ (*i.e.* by precomposing with $\pi$), we also consider $\gamma$ as a 2-cocycle of $G$, *i.e.* as an element of $\mathrm{Z}^2(G, K^\times)$. By definition, the inflation of $\gamma$ is a 2-coboundary if and only if there is a map of sets $\sigma : G \to K^\times$ such that $\gamma(g,h) = \sigma(g) \cdot \sigma(h) \cdot \sigma(gh)^{-1}$ for $g, h \in G$. If this is the case, by equating the two expressions for $\gamma$, we have for all $g, h \in G$:

$$\big(\widetilde{\rho}(\pi(g))\sigma(g)^{-1}\big) \cdot \big(\widetilde{\rho}(\pi(h))\sigma(h)^{-1}\big) = \big(\widetilde{\rho}(\pi(gh))\sigma(gh)^{-1}\big),$$

showing that $\rho : G \to \mathrm{GL}_n(K)$ with $\rho(g) = \widetilde{\rho}(\pi(g))\sigma(g)^{-1}$ is a linear representation of $G$ lifting $\rho^{\mathrm{proj}}$. These arguments can be read backwards, showing that the triviality of the cocycle class in $\mathrm{H}^2(G, K^\times)$ exactly characterises the liftability of $\rho^{\mathrm{proj}}$ to a linear representation $G \to \mathrm{GL}_n(K)$.

We analyse this a bit further and see that $\sigma|_C$ is a group homomorphism $C \to K^\times$ as $\gamma(c_1, c_2) = 1$ for all $c_1, c_2 \in C$. Moreover, we can replace $\sigma$ by $\sigma \cdot \varphi$ for any character $\varphi : G \to K^\times$. This leads to twisting $\rho$ by $\varphi$. Conversely, if $\sigma' : G \to K^\times$ is a map of sets that satisfies the relation $\gamma(g,h) = \sigma'(g) \cdot \sigma'(h) \cdot \sigma'(gh)^{-1}$, then $\sigma\sigma'^{-1}$ is a character, showing that the ambiguity exactly comes from twisting. We summarise this as follows.

**Proposition 2.1.** *Let $\gamma \in \mathrm{Z}^2(\overline{G}, K^\times)$ be the 2-cocycle associated with $\rho^{\mathrm{proj}}$. Then the inflation of $\gamma$ is a 2-coboundary in $\mathrm{Z}^2(G, K^\times)$ if and only if $\rho^{\mathrm{proj}}$ admits a linear lift $\rho : G \to \mathrm{GL}_n(K)$. Different linear lifts are twists of each other by characters $G \to K^\times$.*

We remark that this can also be elegantly rephrased in the language of group cohomology via the following four terms of the so-called 5-*term exact sequence* (see e.g. [NSW08, (1.6.7)])

$$\mathrm{Hom}(G, K^\times) \xrightarrow{\mathrm{res}} \mathrm{Hom}(C, K^\times) \xrightarrow{\mathrm{tg}} \mathrm{H}^2(\overline{G}, K^\times) \xrightarrow{\mathrm{infl}} \mathrm{H}^2(G, K^\times),$$

using that $\mathrm{H}^1 = \mathrm{Hom}$ for trivial modules. Here $\mathrm{tg}$ is the transgression map, which for a character $\delta : C \to K^\times$ can be explicitly described by $\mathrm{tg}(\delta)(\pi(g), \pi(h)) = \sigma(g) \cdot \sigma(h) \cdot \sigma(gh)^{-1}$ for $g, h \in G$ and $\sigma : G \to K^\times$ the map defined by $\sigma(cs(\overline{g})) = \delta(c)$ for $\overline{g} \in \overline{G}$ and $c \in C$ where $s : \overline{G} \to G$ is any fixed set-theoretic split of $\pi$ sending 1 to 1.

For Galois representations, we have the following fundamental result of Tate's (see [Que95, §4]).

**Theorem 2.2.** *Let $G$ be the absolute Galois group of a global or a local field (non-Archimedean local fields are assumed to have finite residue field) and assume $K$ algebraically closed. Then $\mathrm{H}^2(G, K^\times) = 1$.*

Applying the above with an absolute Galois group $G$ as in the theorem and $\overline{G} = G$, we see that every projective representation $\rho^{\mathrm{proj}} : G \to \mathrm{PGL}_n(K)$ admits a (unique up to twisting) lift to a linear representation $\rho : G \to \mathrm{GL}_n(K)$. Passing to images leads to a central extension

$$1 \to A \to \rho(G) \to \rho^{\mathrm{proj}}(G) \to 1, \tag{1}$$

where $A$ is a subgroup of $K^\times$, upon identifying $K^\times$ with the group of scalar matrices. Every central extension corresponds to a 2-cocycle class (see [NSW08, (1.2.4)]), in this case lying in $\mathrm{H}^2(\rho^{\mathrm{proj}}(G), A)$. Applying the map

$$\alpha : \mathrm{H}^2(\rho^{\mathrm{proj}}(G), A) \to \mathrm{H}^2(\rho^{\mathrm{proj}}(G), K^\times)$$

induced from the inclusion $A \to K^\times$ returns the 2-cocycle class attached with $\rho^{\mathrm{proj}}$ seen as a representation of its image via inclusion. We remark explicitly that the map $\alpha$ need not be injective; its kernel is isomorphic to $\mathrm{Hom}(\rho^{\mathrm{proj}}(G), K^\times/A)/\mathrm{Hom}(\rho^{\mathrm{proj}}(G), K^\times)$. This means that more than one central extension with kernel $A$ can be associated with the same projective representation.

Next, we explain how to construct a lift $\rho : G \to \mathrm{GL}_n(K)$ of a given projective representation $\rho^{\mathrm{proj}} : G \to \mathrm{PGL}_n(K)$ with attached 2-cocycle class $\gamma \in \mathrm{H}^2(\rho^{\mathrm{proj}}(G), K^\times)$. Start with a central extension $\mathcal{G}$ of $\rho^{\mathrm{proj}}(G)$ by $A$, a finite subgroup of $K^\times$ as in (1). It corresponds to the class of a cocycle $\delta \in \mathrm{H}^2(\rho^{\mathrm{proj}}(G), A)$ and we assume $\alpha(\delta) = \gamma$. We further have by Proposition 2.1 that the inflation of $\gamma$ to $\mathrm{H}^2(\mathcal{G}, K^\times)$ is trivial if and only if $\rho^{\mathrm{proj}}$ can be lifted to a representation $\mathcal{G} \to \mathrm{GL}_n(K)$. If $G$ is an absolute Galois group as above, the question to decide whether a map $\pi : G \twoheadrightarrow \mathcal{G}$ exists such that the diagram

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & \overset{\pi}{\swarrow} & \downarrow \rho^{\mathrm{proj}} & & \\ 1 & \longrightarrow & A & \longrightarrow & \mathcal{G} & \longrightarrow & \rho^{\mathrm{proj}}(G) & \longrightarrow & 1 \end{array}$$

commutes, is called a *Galois embedding problem.*

In the cases of interest to us, namely the groups $\rho^{\mathrm{proj}}(G) = \mathrm{PGL}_2(\mathbb{F}_q)$ with an odd prime power $q$ and $A = C_{2^r}$, this problem was studied by Quer in [Que95], building on work by Serre [Ser84]. By Propositions 2.1(i) and 2.4 (i)-(ii) in [Que95], we have the commutative diagram

$$\begin{array}{ccc} \mathrm{H}^2(\mathrm{PGL}_2(\mathbb{F}_q), C_{2^r}) & \xrightarrow{\sim} & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ \downarrow \mathrm{res} & & \downarrow \\ \mathrm{H}^2(\mathrm{PSL}_2(\mathbb{F}_q), C_{2^r}) & \xrightarrow{\sim} & \mathbb{Z}/2\mathbb{Z}. \end{array}$$

There are thus three non-trivial central extensions of $\mathrm{PGL}_2(\mathbb{F}_q)$ by $C_{2^r}$, two of which restrict to the unique non-trivial central extension $2^r\mathrm{PSL}_2(\mathbb{F}_q)$ of $\mathrm{PSL}_2(\mathbb{F}_q)$ by $C_{2^r}$. For $r = 1$, the latter is simply $\mathrm{SL}_2(\mathbb{F}_q)$. Following [Que95, p. 549], the extension $2\_\mathrm{PGL}_2(\mathbb{F}_q)$ is defined by the pull-back of the exact sequence

$$1 \to C_2 \hookrightarrow \mathrm{SL}_2(\overline{\mathbb{F}}_q) \twoheadrightarrow \mathrm{PSL}_2(\overline{\mathbb{F}}_q) \to 1$$

under the embedding $\mathrm{PGL}_2(\mathbb{F}_q) \hookrightarrow \mathrm{PGL}_2(\overline{\mathbb{F}}_q) = \mathrm{PSL}_2(\overline{\mathbb{F}}_q)$. For every $r > 1$, let $2^r\_\mathrm{PGL}_2(\mathbb{F}_q)$ be defined as the image of $2\_\mathrm{PGL}_2(\mathbb{F}_q)$ under the map

$$\mathrm{H}^2(\mathrm{PGL}_2(\mathbb{F}_q), C_2) \to \mathrm{H}^2(\mathrm{PGL}_2(\mathbb{F}_q), C_{2^r})$$

induced by the embedding $C_2 \hookrightarrow C_{2^r}$. Concretely,

$$2\_\mathrm{PGL}_2(\mathbb{F}_q) = \{M \in \mathrm{SL}_2(\overline{\mathbb{F}}_q) \mid \exists\, \lambda \in \overline{\mathbb{F}}_q^\times : \lambda \cdot M \in \mathrm{GL}_2(\mathbb{F}_q)\} = \langle \mathrm{SL}_2(\mathbb{F}_q), \left(\begin{smallmatrix} 0 & -y \\ y^{-1} & 0 \end{smallmatrix}\right) \rangle$$

for any fixed $y \in \mathbb{F}_{q^2}$ such that $y^2$ is a non-square in $\mathbb{F}_q^\times$. As furthermore $C_{2^r}$ lies in the centre, we have

$$2^r\_\mathrm{PGL}_2(\mathbb{F}_q) = \langle \mathrm{SL}_2(\mathbb{F}_q), \begin{pmatrix} 0 & -y \\ y^{-1} & 0 \end{pmatrix}, \left(\begin{smallmatrix} u & 0 \\ 0 & u \end{smallmatrix}\right) \rangle \subset \mathrm{GL}_2(\overline{\mathbb{F}}_q),$$

where $u \in \overline{\mathbb{F}}_q^\times$ is a fixed element of order $2^r$.

We now assume $G = G_\mathbb{Q}$ and $q = 5$, but point out explicitly that Quer's results cover all $q$ (but with modified formulas). We exploit the exceptional isomorphism $S_5 \cong \mathrm{PGL}_2(\mathbb{F}_5)$. Let $K_1$ be the fixed field of the stabiliser group of one element for the action of $\rho^{\mathrm{proj}}(G_\mathbb{Q}) \cong \mathrm{PGL}_2(\mathbb{F}_5) \cong S_5$ on 5 letters and let $d_{K_1}$ be its discriminant. For any prime $p$, let $w(K_1)_p$ be the Hasse–Witt invariant associated with the trace form $\mathrm{tr}_{K_1/\mathbb{Q}}(x^2)$ viewed as a quadratic form over $\mathbb{Q}_p$, and, further, denote by $(-,-)_p$ the Hilbert symbol over $\mathbb{Q}_p$. Now, let $P(K_1)$ be the finite set of primes $p$ such that $w(K_1)_p \cdot (-2, d_{K_1})_p \neq 1$. Finally, in order to finish the set-up, let $\mu(p)$ denote the exponent of the highest power of 2 dividing $p-1$ with the convention $\mu(2) = 1$. Set $\mu(\rho^{\mathrm{proj}}) = \max\{\mu(p) \mid p \in P(K_1)\}$ (or 0 if $P(K_1) = \emptyset$). We have the following proposition of Quer's ([Que95, Prop. 4.1(ii), Theorem 3.7]).

**Proposition 2.3** (Quer). *Let $\rho^{\mathrm{proj}} : G_\mathbb{Q} \to \mathrm{PGL}_2(\mathbb{F}_5)$ be a surjective projective Galois representation. It has a lifting $\rho : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_5)$ with image $2^r\_\mathrm{PGL}_2(\mathbb{F}_5)$ if and only if $r > \mu(\rho^{\mathrm{proj}})$.*

We apply this now with $K_1 = K_{f_5}$. Then we have $d_{K_1} = 19 \cdot 151$ and the trace form $\mathrm{tr}_{K_{f_5}/\mathbb{Q}}(x^2)$ is equivalent to the quadratic form $X_1^2 + 4X_2^2 - 4d_{K_1}X_3^2 + X_4X_5$ by [Ser84, Appendix II, Proposition 6]. It can therefore be represented by the matrix $\mathrm{diag}(4, -1, -4d_{K_{f_5}}, 1, 1)$ and we compute for its Hasse-Witt invariant at the prime $p$: $w(Q_{K_{f_5}})_p = (-1, d)_p$ and so $w(Q_{K_{f_5}})_p \cdot (-2, d_{K_{f_5}})_p = (2, d_{K_{f_5}})_p = (2, 19)_p \cdot (2, 151)_p$. Thus, the only primes that could be in $P(K_{f_5})$ are $2, 19, 151$. For each of them $\mu(p) = 1$, whence $\mu(\rho^{\mathrm{proj}}) \leq 1$, showing that a lift of $\rho^{\mathrm{proj}}$ exists for $C_4$. In fact, a short computation with Hilbert symbols gives us $P(\rho^{\mathrm{proj}}) = \{19\}$ and so $\mu(\rho^{\mathrm{proj}}) = 1$.

## 3. Computational Solution in Characteristic 5

3.1. **An explicit embedding problem.** In this section, we give a concrete computational construction of the lift provided by Proposition 2.3 in our case. All computations were carried out using Magma [BCP97] and we state the results of these computations here without recalling every time how they were obtained.

In view of the exceptional isomorphism $S_5 \cong \mathrm{PGL}_2(\mathbb{F}_5)$, the basic idea is to work with a degree 6 extension of $\mathbb{Q}$ instead of $K_{f_5}$. This is natural because $\mathrm{PGL}_2(\mathbb{F}_5)$ acts on the six elements of $\mathbb{P}^1(\mathbb{F}_5)$. Concretely, the field $K$, originally defined as the splitting field of $f_5$ over $\mathbb{Q}$, is also the splitting field of the polynomial $g(X) = x^6 - x^5 - 10x^4 + 30x^3 - 31x^2 + 7x + 9 \in \mathbb{Z}[x]$. We let $K_g := \mathbb{Q}[x]/(g(x))$[7] and consider the projective Galois representation

$$\rho^{\mathrm{proj}} : G_\mathbb{Q} \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{PGL}_2(\mathbb{F}_5).$$

We know from §2 that there is a linear lift with kernel $C_4$. Now, we will construct a polynomial the splitting field of which corresponds to such a lift. By §2, there are three non-trivial group extensions of $\mathrm{PGL}_2(\mathbb{F}_5)$ by $C_4$, but only two of them restrict to the unique non-split extension of $A_5 = \mathrm{PSL}_2(\mathbb{F}_5)$ by $C_4$. The split extension of $A_5$ by $C_4$ cannot correspond to a linear lift of the projective representation. The other two extensions are $\mathrm{GL}_2(\mathbb{F}_5)$ and $C_4{\cdot}_6S_5$ in the notation of Tim Dokchitser's project GroupNames [Dok]. The former cannot occur either since in that case the determinant of $\rho$ would be a Dirichlet character of order 4 ramifying only at 19 and 151, which does not exist because

[7] [LMF22, Number Field 6.2.23615200909.1]

| Conjugacy class in $S_5$ | tr in $\theta_5^{\mathrm{st}}$ | $(\mathrm{tr}, \det)$ in $\mathcal{G} \subset \mathrm{GL}_2(\overline{\mathbb{F}}_5)$ | sgn |
|---|---|---|---|
| $(1)$ | $4$ | $(1,4),(2,1),(3,1),(4,4)$ | $1$ |
| $(1,3,5,4,2)$ | $-1$ | $(1,4),(2,1),(3,1),(4,4)$ | $1$ |
| $(2,5)(3,4)$ | $0$ | $(0,1),(0,4)$ | $1$ |
| $(1,4)$ | $2$ | $(0,1),(0,4)$ | $-1$ |
| $(1,4,5)$ | $1$ | $(1,1),(2,4),(3,4),(4,1)$ | $1$ |
| $(1,5)(2,3,4)$ | $-1$ | $(\zeta,4),(2\zeta,1),(-\zeta,4),(-2\zeta,1)$ | $-1$ |
| $(1,2,5,3)$ | $0$ | $(\zeta,1),(2\zeta,4),(-\zeta,1),(-2\zeta,4)$ | $-1$ |

TABLE 1. Data on representations

$(\mathbb{Z}/19 \cdot 151\mathbb{Z})^\times$ does not possess any element of order 4. Consequently, $C_4{\cdot}_6S_5$ is the extension $4\_\mathrm{PGL}_2(\mathbb{F}_5)$ (this can also be verified explicitly).

The group $\mathcal{G} = C_4{\cdot}_6S_5$ is a transitive permutation group on 48 letters, and this is the minimum. One finds that $\mathcal{G}$ has a unique conjugacy class of subgroups $[H]$ of order 80. Furthermore, $H$ contains a unique normal subgroup $U$ of order 5. The quotient $H/U$ is isomorphic to $C_8 \times C_2$. There are hence also two normal subgroups $N_1, N_2$ of $H$ of order 10 having $C_8$ as quotient. None of them contains a non-trivial normal subgroup of $G$.

If there is a Galois extension $\tilde{K}$ of $\mathbb{Q}$ with Galois group $\mathcal{G}$ such that $K_g = \tilde{K}^H$, then by the preceding group theory discussion, $K_g$ admits two cyclic extensions of degree 8 contained in $\tilde{K}$ and both these extensions have $\tilde{K}$ as splitting field. This necessary condition leads us to look for $C_8$-extensions of $K_g$ in order to construct $\tilde{K}$. One can use explicit class field theory in Magma to find a cyclic extension of degree 8 of $K_g$ inside the ray class field of conductor 151 if one allows one of the two infinite places to ramify. One can compute a polynomial $h \in \mathbb{Z}[x]$ of degree 48 describing it and computationally check that its Galois group is indeed $\mathcal{G}$. See the appendix §3.3 for an example of such a polynomial. We remark that it is not enough to include only one of the two primes above 151 into the conductor. This is in accordance with the computations at the inertia groups at 19 and 151 below.

3.2. **A linear Galois representation.** By the explicit matrix description of $4\_\mathrm{PGL}_2(\mathbb{F}_5) \cong C_4{\cdot}_6S_5$ given in §2, we obtain a Galois representation

$$\rho : G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(\tilde{K}/\mathbb{Q}) = \mathcal{G} \subset \mathrm{GL}_2(\overline{\mathbb{F}}_5)$$

lifting $\rho^{\mathrm{proj}}$ with image the subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_5)$ generated by $\mathrm{SL}_2(\mathbb{F}_5)$, the scalar $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$ and the order 2 matrix $\left(\begin{smallmatrix} 0 & \zeta \\ -\zeta^{-1} & 0 \end{smallmatrix}\right)$, where we take $\zeta \in \mathbb{F}_{5^2}^\times$ of order 8 satisfying $\zeta^2 = 2$. This explicit description allows us to relate the cycle type of an element in $S_5 \cong \mathrm{PGL}_2(\mathbb{F}_5)$ to the trace and determinant of all possible lifts. Table 1 contains all pairs of trace and determinant that occur for a given cycle type as well as other information.

We next determine the conductor of $\rho$. As only 19 and 151 ramify, the ramification is tame and inertia groups are cyclic. Recall that at both primes the inertia groups in $K/\mathbb{Q}$ are of order 2 generated by transpositions. Each one of the corresponding inertia groups of $\tilde{K}/\mathbb{Q}$ will hence be generated by a lift of a transposition. According to Table 1, such lifts have characteristic polynomials $X^2 - 1$ or $X^2 + 1$ and thus the inertia orders are 2 or 4. Recall further that the polynomial $h$ was obtained via a ray class field unramified at 19. Consequently, the order of inertia at 19 in $\tilde{K}/\mathbb{Q}$ is still 2 and, moreover, it fixes a line since 1 is an eigenvalue of the inertia generator. As the extension $\tilde{K}/K$

| Character | Quadratic Field | Group Name [Dok] of ker | Generators |
|---|---|---|---|
| sgn | $E = \mathbb{Q}(\sqrt{19 \cdot 151})$ | $C_4.A_5$ | $\mathrm{SL}_2(\mathbb{F}_5)$, $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$ |
| det | $\mathbb{Q}(\sqrt{-19})$ | $\mathrm{CSU}_2(\mathbb{F}_5) \cong 2\_\mathrm{PGL}_2(\mathbb{F}_5)$ | $\mathrm{SL}_2(\mathbb{F}_5)$, $\left(\begin{smallmatrix} 0 & \zeta \\ -\zeta^{-1} & 0 \end{smallmatrix}\right)$ |
| det ·sgn | $\mathbb{Q}(\sqrt{-151})$ | $C_2.S_5$ | $\mathrm{SL}_2(\mathbb{F}_5)$, $\left(\begin{smallmatrix} 0 & \zeta \\ \zeta^{-1} & 0 \end{smallmatrix}\right)$ |

TABLE 2. Normal subgroups of index 2 in $\mathcal{G}$

ramifies at 151, the inertia group at 151 of $\tilde{K}/\mathbb{Q}$ is of order 4 and does not fix any line. This implies that the conductor of $\rho$ is $19 \cdot 151^2 = 433219$.

The group $\mathcal{G}$ admits three surjective group homomorphisms $\mathcal{G} \to C_2$, namely: the determinant det (via the embedding of $\mathcal{G}$ in $\mathrm{GL}_2(\overline{\mathbb{F}}_p)$ described above), the sign of a permutation sgn via the projection $\mathcal{G} \to S_5$ and the product det ·sgn. As $\mathbb{Q}(\sqrt{19 \cdot 151})$ is fixed by the sign, we have $\mathrm{sgn} = \chi_{19 \cdot 151} = \left(\frac{19 \cdot 151}{\cdot}\right)$. As the characteristic polynomial of a generator of the inertia group of 151 is $X^2 + 1$, the character $\det \circ \rho$ is unramified at 151; it does ramify at 19. Consequently, $\det \circ \rho = \chi_{-19} = \left(\frac{-19}{\cdot}\right)$ and $\det \circ \mathrm{sgn} = \left(\frac{-151}{\cdot}\right)$. Table 2 summarises this information and names the three normal subgroups of $\mathcal{G}$ of index 2.

Let $L = \mathbb{Q}(\sqrt{-19}, \sqrt{-151}) \subset \tilde{K}$ be the compositum of the three corresponding quadratic fields. We first remark that $L/E$ is an unramified CM extension. It hence corresponds to a quadratic character $\epsilon : G_E \to \{\pm 1\} \subset \mathbb{F}_5^\times$, which is unramified at all finite places and totally odd.

Another character will be of importance to us. Let $\mathfrak{p}$ be the prime of $E$ lying above 151. The ray class group of $E$ of conductor $\mathfrak{p}\infty_1$ is cyclic of order 150. Thus, $E$ admits a $C_2$-extension ramifying only at $\mathfrak{p}$ and one of the two (real) places. Let $\delta : G_E \to \{\pm 1\} \subset \mathbb{F}_5^\times$ be the corresponding character. It is not the restriction of any character of $G_{\mathbb{Q}}$.

The restriction to $G_E$ of $\rho$ is unramified at 19 (as $I(\tilde{K}/\mathbb{Q})_{19} = C_2$ and $E/\mathbb{Q}$ ramifies at 19), but it does ramify at 151. The inertia group $I(\tilde{K}/\mathbb{Q})_{151}$ is generated by an order 4 matrix of determinant 1 lifting a transposition, whence it is conjugate to $\left(\begin{smallmatrix} 0 & 2\zeta \\ 2\zeta^{-1} & 0 \end{smallmatrix}\right)$, so that $I(\tilde{K}/E)_{151}$ is generated by its square, i.e. by $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Consequently, the twist $\rho|_E \otimes \delta$ is unramified at all finite places. It is a lift of the projective representation $G_E \to A_5$.

*Proof of Theorem 1.1.* Let $\rho$ be the Galois representation constructed in this section. By Serre's Modularity Conjecture proved in [KW09, Theorem 1.2] and [Kis09, Corollary 0.2], together with results on the optimal weight due to Edixhoven [Edi92, Theorem 4.5], there exists a Hecke eigenform $F \in S_1(19 \cdot 151^2, \chi_{-19}, \overline{\mathbb{F}}_5)$ such that its attached Galois representation $\rho_F$ is isomorphic to $\rho$. The other assertions have been established above except for the non-liftability to a holomorphic weight one modular form. This simply follows from the well-known group theoretic result already known to Klein [Kle93] that $S_5$ is not a subquotient of $\mathrm{PGL}_2(\mathbb{C})$, contradicting the existence of any attached Artin representation. □

As its level is very big, we do not see how to compute the weight one modular form $F$ explicitly on the computer without using its Galois representation $\rho$.

*Proof of Corollary 1.3.* All statements can be verified using Tables 1 and 2 together with the relation $a_p(F) = \mathrm{tr}(\rho(\mathrm{Frob}_p))$ and $\mathrm{sgn} = \left(\frac{19 \cdot 151}{\cdot}\right)$ as well as $\det \circ \rho = \chi_{-19} = \left(\frac{-19}{\cdot}\right)$. More conceptually, the congruence of $\theta_5^{\mathrm{st}}$ can also be derived from Corollary 1.4. □

3.3. **Appendix.** Here is a polynomial the splitting field of which is the field cut out by $\rho$ in characteristic 5 from Theorem 1.1.

$h(X) = x^{48} - 10x^{47} - 13x^{46} + 173x^{45} - 1278x^{44} + 27542x^{43} - 113958x^{42} - 286430x^{41} + 4655329x^{40}$
$- 26503188x^{39} + 81919958x^{38} + 32368110x^{37} - 2439071195x^{36} + 10669493052x^{35} - 26002615844x^{34}$
$+ 164051953843x^{33} - 205565265490x^{32} - 3098320327510x^{31} + 15580543347067x^{30} - 72094759904784x^{29}$
$+ 145352373756651x^{28} + 1124294833301773x^{27} - 4736762045102396x^{26} - 4428623245164253x^{25}$
$+ 46182217850444449x^{24} - 135621698076328862x^{23} + 69305601476994468x^{22} + 379191012516246341 8x^{21}$
$- 14065814910470191337x^{20} - 13348365591179322148x^{19} + 124088837951469551773x^{18}$
$- 286160102141567453230x^{17} + 886712293571081863675x^{16} + 114904493659853603221 3x^{15}$
$- 1471966066489243078742 4x^{14} + 1053262494425365352823 2x^{13} + 5678683027519135655223 9x^{12}$
$- 5240615300931473179716 2x^{11} - 14932346725150344578361 4x^{10} + 66925661616771272410331 5x^{9}$
$- 89950043166195920578775 6x^{8} - 31084874023461936716594 83x^{7} + 41342258168387714929971 25x^{6}$
$+ 14451282311965453942468438x^{5} - 63382262062301701225908 26x^{4} - 39455974427388666795289 25x^{3}$
$- 30466901209941980350644125x^{2} + 70704214646412544819950625x + 7289456832813562784567562 5$

## 4. Solution via Asai transfer

4.1. **The standard representation via the Asai transfer.** In this section we work with complex representations. For the convenience of the reader, we recall the construction of the Asai transfer (also called tensor induction or multiplicative induction) of a group representation. We follow [Pra92]. Let $G$ be a group and $H$ a subgroup of $G$ of index $m$. Let $V$ be an $n$-dimensional representation of $H$. Let $g_1, \ldots, g_m$ be a set of representatives for the left cosets of $H$ in $G$. For $g \in G$ and for each $j \in \{1, \ldots, m\}$, choose $i \in \{1, \ldots, m\}$ such that $gg_i \in g_jH$ and define $h(g, i) \in H$ by $gg_i = g_jh(g, i)$. The Asai transfer of $V$ from $H$ to $G$, denoted $\mathrm{Asai}_H^G(V)$, is the vector space $V^{\otimes m}$ equipped with the action defined by

$$g(v_1 \otimes \ldots \otimes v_m) = w_1 \otimes \ldots \otimes w_m$$

where, for each $j \in \{1, \ldots, m\}$, $w_j = h(g, i)v_i$.

We now describe the special case of tensor induction which we will need. We assume the index of $H$ in $G$ to be 2 and we let $\eta : H \to \mathrm{GL}_n(\mathbb{C})$ be a representation with character $\psi$. For $g \in G \setminus H$ and $h \in H$, we then have (see Lemma 4.1 of [Isa82] and the discussion preceding it)

$$\mathrm{tr}(\mathrm{Asai}_H^G(\eta)(h)) = \psi(h)\psi(g^{-1}hg) \text{ and } \mathrm{tr}(\mathrm{Asai}_H^G(\eta)(g)) = \psi(g^2). \tag{2}$$

Let $r \geq 1$ and $\eta : 2^r\mathrm{PSL}_2(\mathbb{F}_5) \to \mathrm{GL}_2(\mathbb{C})$ be an irreducible representation. Write $\mathrm{Asai}(\eta)$ for $\mathrm{Asai}_{2^r\mathrm{PSL}_2(\mathbb{F}_5)}^{2^r\_\mathrm{PGL}_2(\mathbb{F}_5)}(\eta)$. We now describe it on any element $c$ in the centre of $2^r\_\mathrm{PGL}_2(\mathbb{F}_5)$. Such $c$ lies in $2^r\mathrm{PSL}_2(\mathbb{F}_5)$ and we have $\eta(c) = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda \end{smallmatrix}\right)$. Consequently, from (2) we get

$$\mathrm{tr}\big(\mathrm{Asai}(\eta)(c)\big) = 4\lambda^2 = 4 \cdot \det(\eta(c)). \tag{3}$$

We next aim at twisting the representation appropriately, making it trivial on the centre.

**Lemma 4.1.** *For $r \geq 1$ let $\alpha : C_{2^r} \to \mathbb{C}^\times$ and $\beta : \mathrm{PGL}_2(\mathbb{F}_5) \to \mathbb{C}^\times$ be characters such that $\alpha$ restricted to the subgroup $C_2$ of $C_{2^r}$ is trivial. Then there exists a unique character*

$$\chi : 2^r\_\mathrm{PGL}_2(\mathbb{F}_5) \to \mathbb{C}^\times$$

*such that $\chi|_{C_{2^r}} = \alpha$ and $\chi|_{2\_\mathrm{PGL}_2(\mathbb{F}_5)} = \beta \circ \pi$ for the natural projection $\pi : 2\_\mathrm{PGL}_2(\mathbb{F}_5) \twoheadrightarrow \mathrm{PGL}_2(\mathbb{F}_5)$.*

*Proof.* The point is that the image of the 2-cycle $\gamma \in \mathrm{H}^2(\mathrm{PSL}_2(\mathbb{F}_5), C_{2^r})$ which describes the central extension $2^r\_\mathrm{PGL}_2(\mathbb{F}_5)$ lies in $C_2$ by construction. Writing elements of $2^r\_\mathrm{PGL}_2(\mathbb{F}_5)$ uniquely as $(c, g) \in C_{2^r} \times \mathrm{PGL}_2(\mathbb{F}_5)$, we define $\chi$ uniquely by letting $\chi\big((c, g)\big) = \alpha(c)\beta(g)$. This is indeed a group homomorphism with the desired properties because

$$\chi\big((c, g) \cdot (c', g')\big) = \chi\big((cc'\gamma(g, g'), gg')\big) = \alpha(cc'\gamma(g, g')) \cdot \beta(gg') = \chi\big((c, g)\big) \cdot \chi\big((c', g')\big)$$

since $\alpha(\gamma(g, g')) = 1$ by assumption. □

**Proposition 4.2.** *Let $r \geq 1$, $\eta : 2^r\mathrm{PSL}_2(\mathbb{F}_5) \to \mathrm{GL}_2(\mathbb{C})$ and $\mathrm{Asai}(\eta)$ as above. Let $\chi : 2^r\_\mathrm{PGL}_2(\mathbb{F}_5) \to \mathbb{C}^\times$ be the unique character from Lemma 4.1 such that $\chi|_{C_{2^r}} = \big(\det \circ \eta|_{C_{2^r}}\big)^{-1}$ and $\chi|_{2\_\mathrm{PGL}_2(\mathbb{F}_5)} = \epsilon \circ \pi$ where $\epsilon : \mathrm{PGL}_2(\mathbb{F}_5) \cong S_5 \to \{\pm 1\}$ is the sign character.*

*Then $\mathrm{Asai}(\eta) \otimes \chi$ factors through $\mathrm{PGL}_2(\mathbb{F}_5) \cong S_5$ and*

$$\mathrm{Asai}(\eta) \otimes \chi \cong \theta_5^{\mathrm{st}}.$$

*Proof.* By (3), the restriction of $\mathrm{Asai}(\eta) \otimes \chi$ to $C_{2^r}$ is the trivial 4-dimensional representation, implying that it factors through $\mathrm{PGL}_2(\mathbb{F}_5) \cong S_5$. An inspection of the character table of $S_5$ shows that $\mathrm{Asai}(\eta) \otimes \chi$ is then one of the two irreducible 4-dimensional representations of $S_5$, which are $\theta_5^{\mathrm{st}}$ and $\theta_5^{\mathrm{st}} \otimes \epsilon$. Indeed, if it were a sum of four 1-dimensional representations, then all character values would be even, which is not the case as the trace of $\eta$ is odd on elements of order 3 in $2\mathrm{PSL}_2(\mathbb{F}_5)$.

As in §3.2, consider $g = \begin{pmatrix} 0 & -\zeta \\ \zeta^{-1} & 0 \end{pmatrix} \in 2\_\mathrm{PGL}_2(\mathbb{F}_5)$ for $\zeta \in \mathbb{F}_{5^2}$ such that $\zeta^2 = 2$ is a non-square in $\mathbb{F}_5$. We have $\mathrm{tr}(\eta(g^2)) = \mathrm{tr}(\eta(\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right))) = -2$. As $g$ lies in $2\_\mathrm{PGL}_2(\mathbb{F}_5)$ but not in $2\mathrm{PSL}_2(\mathbb{F}_5)$ its projection to $\mathrm{PGL}_2(\mathbb{F}_5) \cong S_5$ is a transposition, whence $\chi(g) = \epsilon(g) = -1$ and $\mathrm{tr}(\rho^{\mathrm{st}}(g)) = 2$. Thus, this computation proves that $\mathrm{Asai}(\eta) \otimes \chi$ is not isomorphic to $\theta_5^{\mathrm{st}} \otimes \epsilon$, so it is isomorphic to $\theta_5^{\mathrm{st}}$. □

In view of (2), we obtain the following description of the character of $\theta_5^{\mathrm{st}}$.

**Corollary 4.3.** *With notation as in Proposition 4.2 and $\psi = \mathrm{tr} \circ \eta$, for any $g \in S_5 \setminus A_5$ and any $h \in A_5$ we have*

$$\mathrm{tr}(\theta_5^{\mathrm{st}}(h)) = \psi(\hat{h}) \cdot \psi(\hat{g}^{-1}\hat{h}\hat{g}) \cdot \chi(\hat{h}) \text{ and } \mathrm{tr}(\theta_5^{\mathrm{st}}(g)) = \psi(\hat{g}^2) \cdot \chi(\hat{g}),$$

*where $\hat{g} \in 2^r\_\mathrm{PGL}_2(\mathbb{F}_5)$ and $\hat{h} \in 2^r\mathrm{PSL}_2(\mathbb{F}_5)$ are any lifts of $g$ and $h$, respectively.*

4.2. **Automorphy.** In this section, we prove Theorem 1.2. The key input providing the automorphy is the following strong result of Pilloni and Stroh.

**Theorem 4.4** ([PS16], Théorème 0.3)**.** *Let $E$ be a totally real field and $\eta : G_E \to \mathrm{GL}_2(\mathbb{C})$ be a totally odd, irreducible representation. Then $\eta$ is modular, attached to a Hilbert cuspidal eigenform of weight one.*

*Proof of Theorem 1.2* (a). We start by viewing the $S_5$-extension $K/\mathbb{Q}$ as a surjective projective Galois representation $\rho^{\mathrm{proj}} : G_\mathbb{Q} \to \mathrm{PGL}_2(\mathbb{F}_5)$. By Proposition 2.3, it lifts to a linear Galois representation $\rho : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_5)$ with image $2^r\_\mathrm{PGL}_2(\mathbb{F}_5)$ for any fixed choice of $r > \mu(\rho^{\mathrm{proj}})$. Let $\tilde{K}$ be the number field 'cut out' by $\rho$, *i.e.* the one such that its absolute Galois group equals $\ker(\rho)$. Then $\mathrm{Gal}(\tilde{K}/\mathbb{Q}) \cong 2^r\_\mathrm{PGL}_2(\mathbb{F}_5)$, the subgroup $\mathrm{Gal}(\tilde{K}/K)$ is its centre $C_{2^r}$ and $\mathrm{Gal}(\tilde{K}/E) \cong 2^r\mathrm{PSL}_2(\mathbb{F}_5)$.

Let now

$$\eta : G_E \twoheadrightarrow G(\tilde{K}/E) \cong 2^r\mathrm{PSL}_2(\mathbb{F}_5) \to \mathrm{GL}_2(\mathbb{C})$$

be obtained from any two-dimensional irreducible complex representation of $2^r\mathrm{PSL}_2(\mathbb{F}_5)$ (such a representation exists because $2\mathrm{PSL}_2(\mathbb{F}_5)$ admits two of them and the centre can be realised via scalar matrices). Let $c \in G_E$ be any complex conjugation. As $K$ is totally imaginary, $c$ does not lie in the centre of $2^r\mathrm{PSL}_2(\mathbb{F}_5)$. Thus $\eta(c)$ is a non-scalar involution in $\mathrm{GL}_2(\mathbb{C})$ and as such has determinant 1. Consequently, $\eta$ is a totally odd representation. Then Theorem 4.4 shows the existence of the claimed Hilbert modular form $G$.

Seeing $\eta$ alternatively as a representation of $\mathrm{Gal}(\tilde{K}/E)$, we naturally identify $\mathrm{Asai}_{G_E}^{G_\mathbb{Q}}(\eta)$ with $\mathrm{Asai}_{\mathrm{Gal}(\tilde{K}/E)}^{\mathrm{Gal}(\tilde{K}/\mathbb{Q})}(\eta)$. The claimed formula is now the content of Proposition 4.2. □

We next appeal to the functoriality of the Asai transfer. Let $L/F$ be a quadratic extension of number fields and $\pi = \bigotimes_w \pi_w$ be a cuspidal representation of $GL_2(\mathbb{A}_L)$. If $\rho : G_L \to \mathrm{GL}_2(\mathbb{C})$ is a Galois representation such that its Artin $L$-function equals $L(s, \pi)$, except for finitely many places, one can associate an $L$-function to $\pi$, denoted $L_{\mathrm{Asai}}(s, \pi)$, in such a way that the local factors of $L_{\mathrm{Asai}}(s, \pi)$ match the local factors of the Artin $L$-function of $\mathrm{Asai}_{G_L}^{G_F}(\rho)$, again, with the exception of finitely many places. We refer the readers to the articles [Ram02] and to sections 2 and 3 of [Kri12] for the relevant constructions and for the proof of the following result.

**Theorem 4.5** ([Ram02, Theorem 1.4 (a)]). *Let $L/F$ be a quadratic extension of number fields, and let $\pi$ be a cuspidal automorphic representation of* $\mathrm{GL}_2(\mathbb{A}_L)$. *Then there exists an automorphic representation* $\Pi$ *for* $\mathrm{GL}_4(\mathbb{A}_F)$ *such that the L-function of* $\Pi$ *equals* $L_{\mathrm{Asai}}(s, \pi)$ *except at finitely many finite places. We denote by* $\mathrm{Asai}(\pi)$ *the automorphic form* $\Pi$.

*Proof of Theorem 1.2* (b). The Galois representation $\eta$ is attached to a cuspidal automorphic representation for $GL_2(\mathbb{A}_E)$, say $\pi$, corresponding to the Hilbert modular form $G$. By Theorem 4.5 applied with $L = E$ and $F = \mathbb{Q}$, we obtain that the L-function of $\mathrm{Asai}(\pi)$ equals the Artin L-function of $\mathrm{Asai}_{G_E}^{G_\mathbb{Q}}(\eta)$. The result follows by twisting $\mathrm{Asai}(\pi)$ by the Hecke character corresponding to $\chi$ because that twist corresponds to twisting $\mathrm{Asai}_{G_E}^{G_\mathbb{Q}}(\eta)$ by $\chi$. □

*Proof of Corollary 1.4.* We specialise Theorem 1.2 (a) to the splitting field $K$ of $f_5$ over $\mathbb{Q}$. Table 2 shows that $\chi = \left(\frac{-151}{\cdot}\right)$ because $\chi|_{C_4} = \det \circ \eta$ and $\chi|_{2\_\mathrm{PGL}_2(\mathbb{F}_5)}$ factors through $\mathrm{PGL}_2(\mathbb{F}_5) \cong S_5$ as the sign character. Furthermore, if $\psi$ denotes the character of $\eta$, by the properties of $\eta$, for any unramified finite place $\mathfrak{p}$ of $E$ we have $\psi(\mathfrak{p}) = a_\mathfrak{p}(G)$. The proof is now finished by Corollary 4.3 and an inspection of Table 1. □

## REFERENCES


[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. volume 24, pages 235–265. 1997. Computational algebra and number theory (London, 1993).

[BMT15] David W. Boyd, Greg Martin, and Mark Thom. Squarefree values of trinomial discriminants. *LMS J. Comput. Math.*, 18(1):148–169, 2015.

[Bry12] John T. Bryk. *On the roots of polynomials modulo primes*. ProQuest LLC, Ann Arbor, MI, 2012. Thesis (Ph.D.)–Rutgers The State University of New Jersey - New Brunswick.

[Cal13] Frank Calegari. The Artin conjecture for some $S_5$-extensions. *Math. Ann.*, 356(1):191–207, 2013.

[Dok] Tim Dokchitser. groupnames.org.

[Dwy14] J. Dwyer. Real zeros of Artin $L$-functions corresponding to five-dimensional $S_5$-representations. *Bull. Lond. Math. Soc.*, 46(1):51–58, 2014.

[Edi92] Bas Edixhoven. The weight in Serre's conjectures on modular forms. *Invent. Math.*, 109(3):563–594, 1992.

[Edi97] Bas Edixhoven. Serre's conjecture. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 209–242. Springer, New York, 1997.

[Gor02] Eyal Z. Goren. *Lectures on Hilbert modular varieties and modular forms*, volume 14 of *CRM Monograph Series*. American Mathematical Society, Providence, RI, 2002. With the assistance of Marc-Hubert Nicole.

[Isa82] I. M. Isaacs. Character correspondences in solvable groups. *Adv. in Math.*, 43(3):284–306, 1982.

[Kat73] Nicholas M. Katz. $p$-adic properties of modular schemes and modular forms. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, Lecture Notes in Math., Vol. 350, pages 69–190. Springer, Berlin, 1973.

[Ked12] Kiran S. Kedlaya. A construction of polynomials with squarefree discriminants. *Proc. Amer. Math. Soc.*, 140(9):3025–3033, 2012.

[Kis09] Mark Kisin. Modularity of 2-adic Barsotti-Tate representations. *Invent. Math.*, 178(3):587–634, 2009.

[Kle93] Felix Klein. *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade. Hrsg. mit einer Einführung und mit Kommentaren von Peter Slodowy*. Basel: Birkhäuser Verlag; Stuttgart: B. G. Teubner Verlagsgesellschaft, reprogr. Nachdr. d. Ausg. Leipzig 1884, Teubner edition, 1993.

[Kon95] Takeshi Kondo. Algebraic number fields with the discriminant equal to that of a quadratic number field. *J. Math. Soc. Japan*, 47(1):31–36, 1995.

[Kri12] M. Krishnamurthy. Determination of cusp forms on $GL(2)$ by coefficients restricted to quadratic subfields (with an appendix by Dipendra Prasad and Dinakar Ramakrishnan). *J. Number Theory*, 132(6):1359–1384, 2012.

[KW09] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture. I. *Invent. Math.*, 178(3):485–504, 2009.

[LMF22] The LMFDB Collaboration. The L-functions and modular forms database. `http://www.lmfdb.org`, 2022.

[LNV91] P. Llorente, E. Nart, and N. Vila. Decomposition of primes in number fields defined by trinomials. *Sém. Théor. Nombres Bordeaux (2)*, 3(1):27–41, 1991.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[Pra92] Dipendra Prasad. Invariant forms for representations of $\mathrm{GL}_2$ over a local field. *Amer. J. Math.*, 114(6):1317–1363, 1992.

[PS16] Vincent Pilloni and Benoît Stroh. Surconvergence, ramification et modularité. *Astérisque*, (382):195–266, 2016.

[Que95] Jordi Quer. Liftings of projective 2-dimensional Galois representations and embedding problems. *J. Algebra*, 171(2):541–566, 1995.

[Ram02] Dinakar Ramakrishnan. Modularity of solvable Artin representations of $\mathrm{GO}(4)$-type. *Int. Math. Res. Not.*, (1):1–54, 2002.

[Sel56] Ernst S. Selmer. On the irreducibility of certain trinomials. *Math. Scand.*, 4:287–302, 1956.

[Ser84] Jean-Pierre Serre. L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$. *Comment. Math. Helv.*, 59(4):651–676, 1984.

[Ser03] Jean-Pierre Serre. On a theorem of Jordan. *Bull. Amer. Math. Soc. (N.S.)*, 40(4):429–440, 2003.



(C. B. Khare) DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, LOS ANGELES, CA 90095, U.S.A.
*Email address*: `shekhar@math.ucla.edu`

(A. F. La Rosa, G. Wiese) DEPARTMENT OF MATHEMATICS, UNIVERSITY OF LUXEMBOURG, MAISON DU NOMBRE, 6 AVENUE DE LA FONTE, L-4364 ESCH-SUR-ALZETTE, LUXEMBOURG
*Email address*: `fabio.larosa@uni.lu, gabor.wiese@uni.lu`