THE CONSTRUCTIVE INVERSE GALOIS PROBLEM VIA HILBERT MODULAR FORMS: REALIZING THE TRANSITIVE GROUP 17T7

RAYMOND VAN BOMMEL, EDGAR COSTA, NOAM D. ELKIES, TIMO KELLER, SAM SCHIAVONE, AND JOHN VOIGHT

Abstract. We show how Hilbert modular forms can be used in the constructive inverse Galois problem over the rationals. In particular, we prove that the transitive permutation group 17T7, isomorphic to a split extension of C_2 by $\mathrm{PSL}_2(\mathbb{F}_{16})$, is a Galois group over the rationals and exhibit an explicit degree 17 polynomial with this Galois group. The group arises from the field of definition of the 2-torsion on an abelian fourfold with real multiplication defined over a real quadratic field; we find such a fourfold attached to a Hilbert modular form. Building upon work of Dembélé, we describe a method for reconstructing a period matrix attached to a Hilbert modular form, and we use it to construct the 2-isogeny polynomial. We also rigorously identify the relevant fourfold as the Jacobian of a genus 4 Shimura curve and compute explicit equations for this curve.

Contents

1. Introduction

1.1. **Motivation and first results.** A question of enduring fascination, the Inverse Galois Problem (IGP) [Ser08, MM99, JLY02] asks whether every finite group is realizable as a Galois group over $\mathbb{Q}$. Here we will be interested in the effective IGP, where given a transitive subgroup $G \leq S_d$ (up to conjugation), one asks further for an explicit polynomial $f(x) \in \mathbb{Q}[x]$ of degree d whose Galois group, as a permutation group via the action on the roots, is equivalent to G.

Except for two intransigent groups, the effective IGP has a positive answer for every transitive group $G \leq S_d$ with $d \leq 23$ [Dok21, KM01, KM24]. Of these two exceptions, the most notorious is the sporadic simple group M_{23}, the Mathieu group of order 10 200 960. Although not realized over $\mathbb{Q}$, the group M_{23} has been realized as a Galois group over any number field K where -1 is a sum of two squares in K [Gra96].

Date: June 1, 2026.
2020 *Mathematics Subject Classification.* 12F12 (Primary) 11F80, 11F41, 14G10.
Key words and phrases. inverse Galois theory, Galois representations, Hilbert modular forms, Shimura curves.

The remaining exception, the one of smallest transitive degree, is the group G with label 17T7 and order $\#G = 8160 = 2^5 3^1 5^1 17^1$. The group G is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_{16}) \rtimes C_2$ and so fits into a split exact sequence

$$1 \to \mathrm{PSL}_2(\mathbb{F}_{16}) \to G \to C_2 \to 1, \tag{1.1.1}$$

where the nontrivial element σ of C_2 acts entrywise by the element of $\mathrm{Gal}(\mathbb{F}_{16} \,|\, \mathbb{F}_2)$ of order 2 (i.e., by $a \mapsto a^4$). We obtain a permutation representation $G \hookrightarrow S_{17}$ via the natural action on $\mathbb{P}^1(\mathbb{F}_{16})$, with σ again acting entrywise.

We first record a general criterion that can be used to solve the inverse Galois problem for groups of the shape $\mathrm{GL}_n(k) \rtimes C_m$ and $\mathrm{SL}_n(k) \rtimes C_m$, where k is a finite field of characteristic ℓ. For notation, we refer to §2.3.

Theorem 1.1.2 (Theorem 2.3.6)**.** *Let $F_0 \subseteq F$ be a Galois extension of number fields. Let $\rho\colon \mathrm{Gal}_F \to \mathrm{GL}_n(k)$ be a Galois representation, let $G := \rho(\mathrm{Gal}_F)$ be the image and suppose $G = \mathrm{GL}_n(k)$ or $G = \mathrm{SL}_n(k)$. Suppose that there exists an injective group homomorphism $\tau\colon \mathrm{Gal}(F \,|\, F_0) \to \mathrm{Aut}(k)$ such that $\rho^\sigma \simeq \tau_\sigma(\rho)$ for all $\sigma \in \mathrm{Gal}(F \,|\, F_0)$. If $G = \mathrm{SL}_n(k)$, further suppose that $\gcd([F : F_0], n)$ is a power of ℓ.*

Then the extension $L = F(\rho) \supseteq F_0$ is Galois with $\mathrm{Gal}(L \,|\, F_0) \cong G \rtimes \mathrm{Gal}(F \,|\, F_0)$, where $\mathrm{Gal}(F \,|\, F_0)$ acts on $G \leq \mathrm{GL}_n(k)$ entrywise via the map τ.

Specializing to the case where ρ is the semisimple mod $\mathfrak{l}$ Galois representation attached to a Hilbert modular form f and applying the Brauer–Nesbitt theorem, we obtain a criterion purely in terms of the Hecke eigenvalues of f (Theorem 2.4.4). In order to realize 17T7 as a Galois group, we find a suitable Hilbert modular form and apply the criterion to its associated mod 2 Galois representation.

We go beyond an existence proof and construct such an extension explicitly.

Theorem 1.1.3. *The group $G =$ 17T7 is a Galois group over $\mathbb{Q}$. More precisely, the polynomial*

$$\begin{aligned} x^{17} - 2x^{16} + 12x^{15} - 28x^{14} + 60x^{13} - 160x^{12} + 200x^{11} - 500x^{10} + 705x^9 - 886x^8 \\ + 2024x^7 - 604x^6 + 2146x^5 + 80x^4 - 1376x^3 - 496x^2 - 1013x - 490 \in \mathbb{Q}[x] \end{aligned} \tag{1.1.4}$$

has Galois group G.

The polynomial (1.1.4) was found by constructing the mod 2 Galois representation attached to a Hilbert modular form; more precisely, we have the following relation.

Theorem 1.1.5. *Let X_0 be the smooth projective curve of genus 4 over $\mathbb{Q}$ birational to the affine curve defined by the equation*

$$\begin{aligned} 8x^4y + 8x^3y^2 + 10x^2y^3 + 4xy^4 + 2y^5 - 8x^4 + 24x^3y + 6x^2y^2 + 12xy^3 \\ - 2y^4 - 2x^3 - 3x^2y + 6xy^2 - 11y^3 + 14x^2 - 6xy - 4y^2 - 7x + 2y + 1 = 0. \end{aligned} \tag{1.1.6}$$

Then the Jacobian of X_0 is isogenous over $F = \mathbb{Q}(\sqrt{3})$ to the abelian variety A attached to the Hilbert modular form 2.2.12.1-578.1-d, and $\mathbb{Q}(A[2])$ is the splitting field of the polynomial (1.1.4).

In the rest of the paper, we will explain the methods, which rely on the theory of Hilbert modular forms and Oda's conjecture, used to find the polynomials in (1.1.4) and (1.1.6).

1.2. **Overview.** There has been substantial work using classical modular forms to solve the IGP for simple groups of the form $\mathrm{PSL}_2(\mathbb{F}_q)$; see e.g., Zywina [Zyw23] for a recent advance and many references. In principle, these methods are also effective (computable in deterministic polynomial time), due to work of Edixhoven [Edi11, Theorem 14.1.1] and others; calculations have been carried out by Bosman [Bos11], Mascot [Mas18], and again many others. Although this approach to the IGP admits many variations, a recurring theme is to exhibit Galois groups over $\mathbb{Q}$ via their action on torsion points of modular abelian varieties over $\mathbb{Q}$, which appear as quotients of the Jacobian of a modular curve.

A natural extension of this method works with abelian varieties and modular forms over number fields F. When F is a totally real field, we may work with Hilbert modular forms in a manner analogous to the classical case [DeV09]. This gives rise to Galois extensions of F. However, in general the Galois groups over $\mathbb{Q}$ obtained from the normal closure are wreath products rather than semidirect products.

The aforementioned explicit criterion (Theorem 2.4.4) allows us to descend from F to $\mathbb{Q}$, yielding Galois groups that are (subgroups of) semidirect products. This criterion takes advantage of additional symmetries observed by Gross in work of Dembélé [Dem09] and appearing in work of Dembélé–Greenberg–Voight [DGV11, § 1]; see Remark 2.4.9. We then use this to solve the IGP for 17T7 by exhibiting certain Hilbert modular forms over abelian totally real fields F, see Theorem 2.5.4. Moreover, this method applies to many other groups G that are split extensions of finite cyclic groups by $\mathrm{PGL}_2(\mathbb{F}_q)$; see Remark 2.5.6.

Our final task then is the effective resolution of the IGP for these groups. In principle, when the Hilbert modular form arises via the Jacquet–Langlands correspondence on a Shimura curve, it should be possible to generalize the work above from the case of classical modular curves. However, such an approach in practice poses theoretical limitations and substantial computational challenges (some aspects of which we hope to return to in future work). Instead, what is needed is a version of the Eichler–Shimura construction for Hilbert modular forms suitable for computation, attaching to a Hilbert modular newform f of weight 2 an abelian variety A_f with matching Galois representation and L-function. In work of Dembélé [Dem08], a numerical approach was outlined in the special case where F is a real quadratic field of narrow class number one and f has rational coefficients, so that A_f is an elliptic curve. This algorithm computes the period lattice assuming a conjecture of Oda [Oda82] as refined by Darmon–Logan [DL03]; see Theorem 3.4.6.

One of our contributions is to generalize this approach, allowing arbitrary narrow class number and coefficient field. Given the Hilbert modular newform f over the Galois totally real field F, with coefficient field K_f of degree $g = [K_f : \mathbb{Q}]$, the rough outline is as follows.

1. Compute periods for A_f by computing $L(f, 1, \chi)$ for many quadratic characters χ.
2. Construct the moduli point $z \in (\mathbb{C} \smallsetminus \mathbb{R})^g$ corresponding to A_f as ratios of the periods, and form the corresponding period matrix Π.
3. Repeat for the conjugates of f under $\mathrm{Gal}(F \,|\, \mathbb{Q})$.

We then form suitable polynomials in the theta constants with characteristic evaluated at Π and its conjugates. Moreover, when the period matrix lies in the Schottky locus, we can also seek to reconstruct the abelian variety as the Jacobian of a curve. Several new features arise in this generalization, as is perhaps clear from this description.

We carry out this approach to solve the effective IGP for 17T7. Specifically, we choose a Hilbert modular form over $\mathbb{Q}(\sqrt{3})$ with LMFDB label 2.2.12.1-578.1-d of level norm 578.

In this case, there is a Shimura curve (Proposition 4.3.1) whose Jacobian is isogenous over F to the abelian fourfold A attached to this form, and we give the explicit realization in Theorem 1.1.5, combining Proposition 4.3.6 and Proposition 4.3.11.

1.3. **Structure of the article.** In §2, we dive into our descent approach to the IGP. We then exhibit our general method for the Eichler–Shimura construction in §3. We conclude in §4 by applying our methods to the particular modular form that produced the 17T7-polynomial in Theorem 1.1.3.

1.4. **Acknowledgements.** The authors thank the organizers, Jennifer Balakrishnan, Bjorn Poonen, and Akshay Venkatesh, of the PCMI 2022 program on Number Theory Informed by Computation. The idea to use Hilbert modular forms was also noted early by Pip Goodman, and an initial list of candidates was compiled in collaboration with him; we acknowledge and thank him for his contribution. We also thank Maarten Derickx for his initial contribution to the project, specifically regarding his work determining the necessary properties of Hilbert modular forms used in our method. We thank Thomas Bouchet for his help in computing the curve (4.3.3), Lassina Dembélé for suggesting the argument that proves modularity of this curve (Proposition 4.3.6), and Andreas-Stephan Elsenhans for help with a Galois group computation (Proposition 4.3.11). We also thank the inspiring lectures of Tim Dokchitser in the PCMI 2021 Graduate Summer School, Number Theory Informed by Computation, which brought this problem to the authors' attention. We thank Nicolas Mascot for his computational verification in Remark 4.3.13 and for his comments on Proposition 4.3.11. We also thank Sachi Hashimoto, Adam Logan, and many other participants of the PCMI 2022 program who contributed to the early stages of the project. Finally, we thank the anonymous referees for their valuable suggestions leading to several improvements of this article.

Van Bommel, Costa, and Schiavone were supported by a Simons Collaboration grant (550033). Van Bommel has additionally been supported by Céline Maistret's Royal Society Dorothy Hodgkin Fellowship. Costa has additionally been supported by a Simons Foundation grant (SFI-MPS-Infrastructure-00008651, AS). Elkies was supported by a Simons Collaboration grant (550031). Keller was supported by the 2021 MSCA Postdoctoral Fellowship 01064790 – ExplicitRatPoints. Voight was supported by grants from the Simons Foundation: (550029, JV) and (SFI-MPS-Infrastructure-00008650, JV).

2. Inverse Galois problem via Hilbert modular forms

In this section, we describe an approach to the Inverse Galois Problem for groups that are split extensions of finite cyclic groups by $\mathrm{GL}_2(\mathbb{F}_q)$, as well as certain subgroups and quotients, using Hilbert modular forms. The main result is the criterion in Theorem 2.4.4.

2.1. **Group theory setup.** Let k be a finite field of characteristic $\operatorname{char} k = \ell$ with prime field $k_0 \subseteq k$. Let $A \leq k^\times$ be a subgroup. We define

$$\mathrm{GL}_2(k)_A := \{g \in \mathrm{GL}_2(k) : \det g \in A\} \tag{2.1.1}$$

for the subgroup of matrices whose determinant lies in A. We write

$$\mathrm{P}\colon\ \mathrm{GL}_2(k) \to \mathrm{PGL}_2(k) \tag{2.1.2}$$

for the canonical projection, and for $G \leq \mathrm{GL}_2(k)$, we write $\mathrm{P}G \leq \mathrm{PGL}_2(k)$ for the projective image. The map $u\colon \mathrm{GL}_2(k) \to k$ defined by

$$u(g) := (\operatorname{tr} g)^2/(\det g) \tag{2.1.3}$$

satisfies $u(cg) = u(g)$ for all $c \in k^*$ and $g \in \mathrm{GL}_2(k)$, and thus descends to a map $\mathrm{PGL}_2(k) \to k$ that we also denote by u. This map is constant on conjugacy classes, and is surjective because $u\Big(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\Big) = 0$ and $u\Big(\begin{pmatrix} v & -v \\ 1 & 0 \end{pmatrix}\Big) = v$ for any $v \in k^*$.

As usual, we write $\mathrm{SL}_2(k) \trianglelefteq \mathrm{GL}_2(k)$ (taking $A = \{1\}$) for the determinant 1 subgroup and $\mathrm{PSL}_2(k) = \mathrm{SL}_2(k)/\{\pm 1\}$. When ℓ is odd, we have $\mathrm{PSL}_2(k) \leq \mathrm{PGL}_2(k)$ of index 2; otherwise (when $\ell = 2$) we have $\mathrm{SL}_2(k) = \mathrm{PSL}_2(k) = \mathrm{PGL}_2(k)$. Finally, we have $\mathrm{PGL}_2(k)_A = \mathrm{PSL}_2(k)$ if $A \leq (k^\times)^2$; otherwise $\mathrm{PGL}_2(k)_A = \mathrm{PGL}_2(k)$.

Lemma 2.1.4. *We have* $\mathrm{GL}_2(k)_A = \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} \mathrm{SL}_2(k)$. *Moreover,* $G \leq \mathrm{GL}_2(k)$ *contains* $\mathrm{SL}_2(k)$ *if and only if* $\mathrm{P}G$ *contains* $\mathrm{PSL}_2(k)$ *if and only if* $G = \mathrm{GL}_2(k)_A$ *where* $A = \det G$.

Proof. If $g \in \mathrm{GL}_2(k)$ has $\det g = a \in A$, then $g = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} g'$ with the first factor in $\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}$ and the second in $\mathrm{SL}_2(k)$; this proves the first statement. For the first equivalence, we check directly for $\#k \leq 3$, so we may suppose that $\#k \geq 4$. Of course if G contains $\mathrm{SL}_2(k)$ then $\mathrm{P}G$ contains $\mathrm{PSL}_2(k)$; for the converse, if $\mathrm{P}G \geq \mathrm{PSL}_2(k)$ then $G \cap \mathrm{SL}_2(k) \leq \mathrm{SL}_2(k)$ has index at most 2 and since $\mathrm{SL}_2(k)$ is equal to its commutator subgroup it has no subgroup of index 2, thus $G \cap \mathrm{SL}_2(k) = \mathrm{SL}_2(k)$ and so $G \geq \mathrm{SL}_2(k)$. For the second equivalence, the containment $G \leq \mathrm{GL}_2(k)_A$ is an equality since $\#G = \#A \# \mathrm{SL}_2(k) = \# \mathrm{GL}_2(k)_A$. □

The group $\mathrm{Gal}(k \,|\, \mathbb{F}_\ell)$ is cyclic, generated by the Frobenius automorphism $x \mapsto x^\ell$; it acts on $\mathrm{GL}_2(k)$ entrywise, giving an injective homomorphism $\mathrm{Gal}(k \,|\, \mathbb{F}_\ell) \hookrightarrow \mathrm{Aut}(\mathrm{GL}_2(k))$, and this action descends to $\mathrm{PGL}_2(k)$. Similarly, the stabilizer of A (in the sense of mapping A to itself, not necessarily fixing its elements pointwise) in $\mathrm{Gal}(k \,|\, \mathbb{F}_\ell)$ acts on $\mathrm{GL}_2(k)_A$ and $\mathrm{PGL}_2(k)_A$. More generally, if $G \leq \mathrm{GL}_2(k)$ has stabilizer $C \leq \mathrm{Gal}(k \,|\, \mathbb{F}_\ell)$, then the natural projection also gives a well-defined homomorphism

$$\mathrm{P}\colon G \rtimes C \to \mathrm{P}G \rtimes C \tag{2.1.5}$$

(as C must also stabilize the scalar subgroup of G).

Finally, the natural action of $\mathrm{PGL}_2(k)$ on $\mathbb{P}^1(k)$ extends to an action by $\mathrm{P\Gamma L}_2(k) := \mathrm{PGL}_2(k) \rtimes \mathrm{Gal}(k \,|\, \mathbb{F}_\ell)$ via

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \sigma\right) \cdot (x : y) = (a\sigma(x) + b\sigma(y) : c\sigma(x) + d\sigma(y)); \tag{2.1.6}$$

the action is faithful, so we obtain an injective homomorphism $\mathrm{P\Gamma L}_2(k) \hookrightarrow S_n$ where $n = \#\mathbb{P}^1(k) = \#k + 1$. (We similarly obtain a permutation representation of $\Gamma\mathrm{L}_2(k) := \mathrm{GL}_2(k) \rtimes \mathrm{Gal}(k \,|\, \mathbb{F}_\ell)$ on $\mathbb{A}^2(k) \smallsetminus \{(0,0)\}$ of degree $(\#k)^2 - 1$.)

Example 2.1.7. Taking $k = \mathbb{F}_{16}$, we have the subgroup

$$\mathrm{SL}_2(\mathbb{F}_{16}) \rtimes \mathrm{Gal}(\mathbb{F}_{16} \,|\, \mathbb{F}_4) \leq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes \mathrm{Gal}(\mathbb{F}_{16} \,|\, \mathbb{F}_2) \hookrightarrow \mathrm{Sym}(\mathbb{P}^1(\mathbb{F}_{16})) \cong S_{17}$$

via the above permutation representation, which as a subgroup of S_{17} is the group 17T7 (up to conjugacy).

2.2. **Large image.** We quickly indicate a few statements that together allow us to conclude that a subgroup $G \leq \mathrm{GL}_2(k)$ contains $\mathrm{SL}_2(k)$.

Proposition 2.2.1. *Let $G \leq \mathrm{GL}_2(k)$ be a subgroup with $\#k \geq 7$. Then G contains $\mathrm{SL}_2(k)$ if and only if G contains:*

(i) *a non-scalar split semisimple element with nonzero trace (its characteristic polynomial splits into distinct linear factors in k);*
(ii) *a nonsplit semisimple element with nonzero trace (its characteristic polynomial is irreducible);*
(iii) *an element whose projective order (i.e., order in $\mathrm{PGL}_2(k)$) exceeds 5; and*
(iv) *an element g such that $k = \mathbb{F}_\ell(u(g))$.*

Proof. The implication ($\Rightarrow$) is direct, so we prove ($\Leftarrow$). By Lemma 2.1.4, it is enough to show that $PG \geq \mathrm{PSL}_2(k)$. By Dickson's classification (see e.g., King [Kin05, Corollaries 2.2–2.3]), the maximal subgroups of $\mathrm{PGL}_2(k)$ are affine, dihedral, exceptional (isomorphic to S_4, A_4, or A_5), or projective (i.e., up to conjugacy, we have $PG = \mathrm{PSL}_2(k_0)$ or $PG = \mathrm{PGL}_2(k_0)$ for some subfield $k_0 \subseteq k$). The stabilizer of a point and the stabilizer of a pair of points are ruled out by (ii), the stabilizer of a pair of imaginary points is ruled out by (i), and the exceptional groups are rules out by (iii).

It follows that G is projective. But then $u(g) \in k_0$ for all $g \in G$. By (iv), we conclude $k = k_0$, so $G \geq \mathrm{PSL}_2(k)$. □

We may also work just with traces, as follows.

Proposition 2.2.2 (Trace lemma)**.** *Let $G \leq \mathrm{SL}_2(k)$ with $\#k \geq 4$ and $\#k \neq 5$. Then $G = \mathrm{SL}_2(k)$ if and only if $\operatorname{tr} G = k$.*

Proof. For $\#k = 4$, we verify the claim with a direct calculation. So we may suppose that $\#k \geq 7$, and apply Proposition 2.2.1.

(i) Let $\lambda \in k^\times \smallsetminus \{\pm 1\}$. Then by hypothesis there exists $g \in G$ such that $\operatorname{tr}(g) = \lambda + \lambda^{-1}$, whence its characteristic polynomial is $x^2 - (\lambda + \lambda^{-1})x + 1 = (x - \lambda)(x - \lambda^{-1})$, so g is split semisimple.
(ii) There exists $a \in k^\times$ such that $x^2 - ax + 1 \in k[x]$ is irreducible, since the map $k^\times \smallsetminus \{\pm 1\} \to k^\times$ given by $\lambda \mapsto \lambda + \lambda^{-1}$ is not surjective: it has fibers of cardinality 2 and hence image of cardinality at most $(\#k - 3)/2 < \#k - 2$. Any $g \in G$ with $\operatorname{tr}(g) = a$ is therefore nonsplit semisimple.
(iii) An element g of projective order ≤ 5 has $\operatorname{tr} g = a \in \{\pm 2, \pm 1, 0\}$ or $a^2 \pm a - 1 = 0 \in k$. This removes at most 7 elements from k, and when $k = \mathbb{F}_7$ there is no $a \in k$ with $a^2 \pm a - 1 = 0$. Any $g \in G$ with trace among the remaining elements of k satisfies (iii).
(iv) Let $a \in k^\times$ generate $k^\times$ as an abelian group. We claim that $\mathbb{F}_\ell(a^2) = \mathbb{F}_\ell(a)$. Indeed, if $\ell = 2$ then $\mathbb{F}_\ell(a^2) = \mathbb{F}_\ell(a)$ (as squaring is a Galois automorphism). If instead ℓ is odd, then $\langle a^2 \rangle \leq \mathbb{F}_\ell(a^2)$, so $\#\mathbb{F}_\ell(a^2) \geq (\#k - 1)/2 > \#k/\ell \geq \#k_0$ for all subfields $k_0 \subsetneq k$. Using the claim, any $g \in G$ with $\operatorname{tr} g = a$ will suffice, since then $u(g) = (\operatorname{tr} g)^2 = a^2$.

This completes the proof because the conditions in Proposition 2.2.1 are all satisfied. □

Remark 2.2.3. Proposition 2.2.2 is false for $\#k = 2, 3, 5$ by the counterexamples $C_3 \leq \mathrm{SL}_2(\mathbb{F}_2)$, $Q_8 \leq \mathrm{SL}_2(\mathbb{F}_3)$, and $\mathrm{SL}_2(\mathbb{F}_3) \hookrightarrow \mathrm{SL}_2(\mathbb{F}_5)$. However, we can consider an upgraded

statement asking for subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ such the set of characteristic polynomials of elements of G coincides with that of $\mathrm{GL}_2(\mathbb{F}_p)$. Unfortunately, there is again a counterexample for $p = 3$, namely $Q_8 \rtimes C_2 \hookrightarrow \mathrm{GL}_2(\mathbb{F}_3)$; but the result now holds for $\mathrm{GL}_2(\mathbb{F}_5)$ again by a direct calculation.

2.3. **Descent.** Now let $F \supseteq F_0$ be a finite Galois extension of number fields inside an algebraic closure $\mathbb{Q}^{\mathrm{al}}$, with absolute Galois group $\mathrm{Gal}_F := \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}} \mid F)$. Let k be a finite field and let

$$\rho\colon \mathrm{Gal}_F \to \mathrm{GL}_n(k) \tag{2.3.1}$$

be a Galois representation. Then $\ker \rho$ cuts out a Galois extension $L := F(\rho) \supseteq F$ with Galois group $\mathrm{Gal}(L \mid F) = G := \operatorname{img} \rho \leq \mathrm{GL}_n(k)$. Let $S(\rho)$ be the set of (nonzero) primes $\mathfrak{p}$ of the ring of integers $\mathbb{Z}_F \subseteq F$ above any prime number p that ramifies in L.

The group $\mathrm{Aut}(k)$ acts on $\mathrm{GL}_n(k)$ entrywise, so for $\tau \in \mathrm{Aut}(k)$ we obtain another Galois representation

$$\begin{aligned} \tau(\rho)\colon \mathrm{Gal}_F &\to \mathrm{GL}_n(k) \\ \tau(\rho)(\xi) &= \tau(\rho(\xi)). \end{aligned} \tag{2.3.2}$$

There is a second Galois action coming from $G_0 := \mathrm{Gal}(F \mid F_0)$, defined as follows. Let $\sigma \in \mathrm{Gal}(F \mid F_0)$. Choose a lift $\widetilde{\sigma} \in \mathrm{Gal}_{F_0}$. We then obtain a new Galois representation defined by

$$\begin{aligned} \rho^\sigma\colon \mathrm{Gal}_F &\to \mathrm{GL}_n(k) \\ \rho^\sigma(\xi) &= \rho(\widetilde{\sigma}^{-1}\xi\widetilde{\sigma}) \end{aligned} \tag{2.3.3}$$

which is well-defined up to isomorphism, independent of the choice of lift. In particular, if $\mathfrak{p} \notin S(\rho)$ is a prime of $\mathbb{Z}_F$ and $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}_F$ a Frobenius automorphism at $\mathfrak{p}$, then

$$\det(1 - \rho^\sigma(\mathrm{Frob}_\mathfrak{p})T) = \det(1 - \rho(\mathrm{Frob}_{\sigma(\mathfrak{p})})T) \in k[T], \tag{2.3.4}$$

well-defined up to conjugacy.

We organize these according to σ as follows. We say that ρ descends to F_0 via a group homomorphism

$$\begin{aligned} \tau\colon \mathrm{Gal}(F \mid F_0) &\to \mathrm{Aut}(k) \\ \sigma &\mapsto \tau_\sigma \end{aligned} \tag{2.3.5}$$

if there exists an isomorphism $\rho^\sigma \simeq \tau_\sigma(\rho)$ of representations for all $\sigma \in \mathrm{Gal}(F \mid F_0)$. The name is justified by the following theorem.

Theorem 2.3.6 (Galois descent law)**.** *Suppose that ρ descends via τ. Then the extension $L = F(\rho) \supseteq F_0$ is Galois, fitting in an exact sequence*

$$1 \to \mathrm{Gal}(L \mid F) \to \mathrm{Gal}(L \mid F_0) \to \mathrm{Gal}(F \mid F_0) \to 1. \tag{2.3.7}$$

Let $G := \operatorname{img} \rho$, and suppose further that τ is injective and one of the following holds:

(i) *$G = \mathrm{GL}_n(k)$; or*
(ii) *$G = \mathrm{SL}_n(k)$ with $\gcd([F : F_0], n)$ equal to a power of ℓ (including 1).*

Then (2.3.7) splits and $\mathrm{Gal}(L \mid F_0) \simeq G \rtimes \mathrm{Gal}(F \mid F_0)$, where $\mathrm{Gal}(F \mid F_0)$ acts on $G \leq \mathrm{GL}_n(k)$ entrywise via the map τ.

To begin with the proof of Theorem 2.3.6, we record a proof of the first statement. For all $\sigma \in \mathrm{Gal}(F \mid F_0)$, the given isomorphism $\rho^\sigma \simeq \tau_\sigma(\rho)$ in particular implies that $\ker \rho^\sigma = \ker \tau_\sigma(\rho) = \ker \rho$, i.e., $L^\sigma = L$. But $\ker \rho^\sigma = \widetilde{\sigma}(\ker \rho)\widetilde{\sigma}^{-1}$, so we conclude that $L = N$ is normal over F_0. The exact sequence (2.3.7) then follows by restriction.

To go further, we recall the following general setup.

Proposition 2.3.8. *Let G_0 and G be groups with G_0 finite. Let*

$$1 \to G \to E \to G_0 \to 1 \tag{2.3.9}$$

be a short exact sequence. Then there is an outer action

$$\bar{\alpha} \colon G_0 \to \mathrm{Out}(G). \tag{2.3.10}$$

Suppose $\bar{\alpha}$ lifts to

$$\alpha \colon G_0 \to \mathrm{Aut}(G). \tag{2.3.11}$$

Then the extension (2.3.9) determines a class

$$[c_E] \in H^2(G_0, Z(G)), \tag{2.3.12}$$

where G_0 acts on $Z(G)$ through α. The extension splits, giving $E \simeq G \rtimes_\alpha G_0$, if and only if $[c_E] = 1$; in particular, this holds if $Z(G) = \{1\}$.

Proof. See Brown [Bro82, Ch. IV, §6] or Rotman [Rot95, Ch 7]. □

Referring to Proposition 2.3.8, we now consider the situation of Theorem 2.3.6 with $G_0 := \mathrm{Gal}(F \mid F_0)$ and $E := \mathrm{Gal}(L \mid F_0)$.

Lemma 2.3.13. *If ρ descends via τ and $\tau_\sigma(\rho)(\mathrm{Gal}_F) = \rho(\mathrm{Gal}_F) = G$ for all $\sigma \in G_0$, then $\tau \colon G_0 \to \mathrm{Aut}(k)$ lifts to a homomorphism $G_0 \to \mathrm{Aut}(G)$; in particular, this holds if $G = \mathrm{GL}_n(k)$ or $G = \mathrm{SL}_n(k)$.*

Proof. If $\tau_\sigma(\rho)(\mathrm{Gal}_F) = \rho(\mathrm{Gal}_F) = G$, the map $\tau_\sigma \in \mathrm{Aut}(k)$ acting entrywise on $\mathrm{GL}_n(k)$ lifts to an automorphism of G and these combine to a homomorphism $G_0 \to \mathrm{Aut}(G)$.

If $G = \mathrm{GL}_n(k)$ then equality of images is clear; if $G = \mathrm{SL}_n(k)$, then from $\rho^\sigma(\mathrm{Gal}_F)$ being *conjugate* to $\tau_\sigma(\rho)$ in $\mathrm{GL}_n(k)$ we may again conclude equality. □

For the second part of Proposition 2.3.8, when $n = p$ for $G = \mathrm{SL}_n(k)$ already we have $Z(G) = \{1\}$.

Lemma 2.3.14. *Let $G_0 \leq \mathrm{Aut}(k)$. Then the following statements hold.*

(a) *$H^2(G_0, k^\times) = \{1\}$ under the natural action.*
(b) *Suppose $\gcd(\#G_0, \#\mu_n(k)) = 1$. Then $H^2(G_0, \mu_n(k)) = 1$.*

Proof. Let $k_0 := k^{G_0}$ be the fixed field, so $G_0 := \mathrm{Gal}(k \mid k_0)$. Then (using 2-periodicity of Tate cohomology of finite cyclic groups)

$$H^2(G_0, k^\times) = (k^\times)^{G_0} / \mathrm{Nm}_{k|k_0}(k^\times) = \{1\} \tag{2.3.15}$$

handling (a). Part (b) follows immediately from a restriction/corestriction argument. □

Proof of Theorem 2.3.6. We proved the first part right below the statement; for the rest, combine Proposition 2.3.8 with Lemma 2.3.13 and Lemma 2.3.14, noting that $Z(\mathrm{SL}_n(k)) = \mu_n(k)$ and $\#\mu_n(k) \mid n'$ where $n = p^e n'$ with $p \nmid n'$. □

Remark 2.3.16. The converse of Theorem 2.3.6 may not be true, since the condition of being Galois concerns only abstract Galois groups, which may or may not be equivalent as linear representations.

Moreover, the extra conditions on the group G are necessary for the exact sequence to split. Indeed, if $F_0 = \mathbb{Q}$, $F = \mathbb{Q}(\sqrt{5})$, and $\rho\colon \mathrm{Gal}_F \to \mathrm{GL}_1(\mathbb{F}_3)$ is the quadratic character factoring through $\mathrm{Gal}(\mathbb{Q}(\zeta_5) \mid F)$, then the descent criterion is easily seen to be verified, but the exact sequence does not split.

Corollary 2.3.17. *Suppose that ρ is semisimple. If $\tau\colon \mathrm{Gal}(F \mid F_0) \to \mathrm{Aut}(k)$ is an injective group homomorphism such that*

$$\det(1 - \rho(\mathrm{Frob}_{\sigma(\mathfrak{p})})T) = \det(1 - \tau_\sigma(\rho)(\mathrm{Frob}_{\mathfrak{p}})T) \in k[T] \tag{2.3.18}$$

for all primes $\mathfrak{p} \notin S(\rho)$, then the extension $L = F(\rho) \supseteq F_0$ is Galois and its Galois group fits in an exact sequence (2.3.7), and the Galois group is isomorphic $\mathrm{Gal}(L \mid F_0) \simeq G \rtimes \mathrm{Gal}(F \mid F_0)$ if G satisfies one of the additional conditions in Theorem 2.3.6.

Proof. Since ρ is semisimple, we just combine Theorem 2.3.6 with the Brauer–Nesbitt theorem [CR06, Theorem 30.16] and the Chebotarev density theorem. □

2.4. **Hilbert descent.** We now apply the Galois descent law (Theorem 2.3.6) to the situation of a Galois representation attached to a Hilbert modular form, our case of interest. (The results could also just as easily specialize to any setting where we can attach Galois representations to modular forms.)

Let F be a Galois totally real field of degree $n = [F : \mathbb{Q}]$, and let f be a Hilbert newform over F with level $\mathfrak{N}$ and paritious weight $(k_i)_i$ with $k_i \geq 2$ for all $i = 1, \dots, n$ and Nebentypus character χ. Let $k_0 := \max(k_1, \dots, k_n)$. For $\mathfrak{p} \nmid \mathfrak{N}$, let $a_{\mathfrak{p}}(f)$ be the Hecke eigenvalue of f at $\mathfrak{p}$, and let $K_f := \mathbb{Q}(\{a_{\mathfrak{p}}(f)\}_{\mathfrak{p}})$ be the number field generated by its Hecke eigenvalues (which are themselves algebraic integers in K_f). Let $\mathfrak{l}$ be a prime of $\mathbb{Z}_{K_f}$ with residue field $\mathbb{F}_{\mathfrak{l}}$ and characteristic $\mathrm{char}\, \mathbb{F}_{\mathfrak{l}} = \ell$.

Theorem 2.4.1. *There exists an irreducible Galois reprentation*

$$\rho_{f,\mathfrak{l}^\infty}\colon \mathrm{Gal}_F \to \mathrm{GL}_2(K_{f,\mathfrak{l}})$$

such that

$$\begin{aligned} \mathrm{tr}(\rho_{f,\mathfrak{l}^\infty}(\mathrm{Frob}_{\mathfrak{p}})) &= a_{\mathfrak{p}}(f) \\ \det(\rho_{f,\mathfrak{l}}(\mathrm{Frob}_{\mathfrak{p}})) &= \chi(\mathfrak{p})\,\mathrm{Nm}(\mathfrak{p})^{k_0-1} \end{aligned} \tag{2.4.2}$$

for all (nonzero) prime ideals $\mathfrak{p}$ of $\mathbb{Z}_F$ with $\mathfrak{p} \nmid \ell\mathfrak{N}$.

Proof. Combine work of Carayol [Car86], Taylor [Tay89], and Blasius–Rogawski [BR89]. □

As usual, choosing an integral lattice, reducing modulo $\mathfrak{l}$, and taking the semisimplification, we obtain a representation

$$\rho_{f,\mathfrak{l}}^{\mathrm{ss}}\colon \mathrm{Gal}_F \to \mathrm{GL}_2(\mathbb{F}_{\mathfrak{l}}) \tag{2.4.3}$$

where now (2.4.2) holds as congruences modulo $\mathfrak{l}$. To simplify notation, we drop the superscript and write just $\rho_{f,\mathfrak{l}}$.

In particular, the image of $\rho_{f,\mathfrak{l}}$ lies in the subgroup $\mathrm{GL}_2(\mathbb{F}_{\mathfrak{l}})_A$ (defined in (2.1.1)) where $A \leq \mathbb{F}_{\mathfrak{l}}^\times$ is the subgroup generated by $\mathbb{F}_\ell^\times$ and the values of χ modulo $\mathfrak{l}$.

Let $D_{\mathfrak{l}} := \{\sigma \in \mathrm{Aut}(K_f) : \sigma(\mathfrak{l}) = \mathfrak{l}\}$ and $I_{\mathfrak{l}} := \{\sigma \in D_{\mathfrak{l}} : \sigma(a) \equiv a \pmod{\mathfrak{l}} \text{ for all } a \in K_f\}$. (If K_f is Galois, these are the decomposition and inertia groups.)

Theorem 2.4.4. *Suppose there is an injective group homomorphism*

$$\tau\colon \operatorname{Gal}(F\,|\,\mathbb{Q}) \hookrightarrow D_{\mathfrak{l}}/I_{\mathfrak{l}}$$

such that for every prime $\mathfrak{p} \nmid \ell\mathfrak{N}$ *and for every* $\sigma \in \operatorname{Gal}(F\,|\,\mathbb{Q})$*, we have both*

$$\begin{aligned} \tau_\sigma(a_{\mathfrak{p}}(f)) &\equiv a_{\sigma(\mathfrak{p})}(f) \pmod{\mathfrak{l}}, \\ \tau_\sigma(\chi(\mathfrak{p})) &\equiv \chi(\sigma(\mathfrak{p})) \pmod{\mathfrak{l}}. \end{aligned} \tag{2.4.5}$$

Then the field $L = F(\rho_{f,\mathfrak{l}})$ *is Galois over* $\mathbb{Q}$ *with the Galois group fitting in an exact sequence as in* (2.3.7)*. If additionally* $G := \operatorname{img}\rho_{f,\mathfrak{l}}$ *satisfies the additional conditions in Theorem 2.3.6, then* $\operatorname{Gal}(L\,|\,\mathbb{Q})$ *is isomorphic to* $G \rtimes \operatorname{Gal}(F\,|\,\mathbb{Q})$ *with* $\operatorname{Gal}(F\,|\,\mathbb{Q})$ *acting through* τ *on* $G \subset \mathrm{GL}_2(\mathbb{F}_{\mathfrak{l}})$ *coefficientwise.*

Proof. We apply the form of the Galois descent law (Theorem 2.3.6) given in Corollary 2.3.17. □

Remark 2.4.6. Since the group $D_{\mathfrak{l}}/I_{\mathfrak{l}} \hookrightarrow \operatorname{Gal}(\mathbb{F}_{\mathfrak{l}}\,|\,\mathbb{F}_\ell)$ is cyclic, Theorem 2.4.4 applies only when F is cyclic over $\mathbb{Q}$. It of course also admits a generalization to the situation where $F \supseteq F_0$ is a cyclic extension of totally real fields, giving a descent to F_0 instead of $\mathbb{Q}$.

As a corollary, we also descend the projective representation.

Corollary 2.4.7. *Under the hypotheses of Theorem 2.4.4 and the additional conditions of Theorem 2.3.6, the field* $F(\mathrm{P}\rho_{f,\mathfrak{l}})$ *cut out by the projective representation* $\mathrm{P}\rho_{f,\mathfrak{l}}$ *is Galois over* $\mathbb{Q}$ *with Galois group* $\mathrm{P}G \rtimes \operatorname{Gal}(F\,|\,\mathbb{Q})$*.*

Proof. The projection is well-defined on the semidirect product as in (2.1.5). □

Remark 2.4.8. The transitive groups 17T6 and 17T8 are closely related to 17T7: 17T6 is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_{16})$ and 17T8 is isomorphic to

$$\mathrm{PSL}_2(\mathbb{F}_{16}) \rtimes \operatorname{Gal}(\mathbb{F}_{16}\,|\,\mathbb{F}_2) \simeq \mathrm{PSL}_2(\mathbb{F}_{16}) \rtimes C_4\,.$$

As explicit polynomials for 17T6- [Bos11] and 17T8-extensions [JR07] were already known, one might wonder why the case of 17T7 remained open.

The construction used by Bosman in [Bos11] is in fact similar to our construction for 17T7, except that it uses classical modular forms instead of Hilbert modular forms. In the classical case, one can use modular symbols to reconstruct the abelian variety instead of Oda's conjecture.

Jones–Roberts [JR07, § 13] exhibit two infinite families of 17T8-extensions, both arising from Belyi maps defined over $\mathbb{Q}$. Each of these families produces a tower of extensions $L \supseteq K \supseteq \mathbb{Q}(t)$ such that

$$\operatorname{Gal}(L\,|\,K) \simeq \mathrm{PSL}_2(\mathbb{F}_{16}) \quad \text{and} \quad \operatorname{Gal}(K\,|\,\mathbb{Q}(t)) \simeq C_4\,.$$

However, as they remark, for each of these families there is a constant field extension contained in K (containing $\mathbb{Q}(\sqrt{5})$ in each case). This prevents us from obtaining a 17T7-extension by specialization of either of these 17T8 families.

Remark 2.4.9. In work of Dembélé [Dem09] and Dembélé–Greenberg–Voight [DGV11], nonsolvable Galois extensions of $\mathbb{Q}$ unramified outside $p = 2, 3, 5$ were found using Hilbert modular forms over abelian extensions of $\mathbb{Q}$, as above. Gross explained why in many cases

the Galois groups over $\mathbb{Q}$ were semidirect products [DGV11, §1]; this observation is encoded in the descent law above.

See also work of Cunningham–Dembélé [CD17] and Booker–Sijsling–Sutherland–Voight–Yasaki [BSSVY24], who also study the same situation and relate this to abelian varieties of potential GL_2-type.

2.5. **Application to the IGP.** We may now put the pieces from the previous subsections together to obtain our application to the Inverse Galois Problem (IGP): we look for Hilbert modular forms f where the mod $\mathfrak{l}$ image is large (using §2.2) and f satisfies the descent condition (2.4.5).

We first focus on the proof of the (ineffective) version of Theorem 1.1.3, realizing 17T7, given as in Example 2.1.7. Looking at Theorem 1.1.2:

- We need a base field F such that $\mathrm{Gal}(F \mid \mathbb{Q}) = \langle \sigma \rangle \simeq C_2$, so we take F a real quadratic field.
- We need a prime $\mathfrak{l}$ with residue field $\mathbb{F}_{16}$, so for simplicity we take coefficient field K_f of degree 4 with 2 inert. (There are also fields K_f of degree > 4 with a prime of residue field $\mathbb{F}_{16}$, but using such f would make it even harder to compute an explicit polynomial.)
- We need the image of the determinant to be trivial, so we take trivial Nebentypus character χ. (Again this is for simplicity; we could take any χ whose order is a power of 2.)
- We must check that (2.4.5) holds; in our case this condition reads
$$a_{\sigma(\mathfrak{p})}(f) \equiv a_{\mathfrak{p}}(f)^4 \pmod 2. \tag{2.5.1}$$
- Finally, we need the eigenvalues $a_{\mathfrak{p}}(f)$ modulo 2 to hit every element of $\mathbb{F}_{16}$, so that we can apply Proposition 2.2.2 to deduce that the representation has image $\mathrm{SL}_2(k)$.

To find such forms, we search the database of Hilbert modular forms [DoV21] available at the L-functions and Modular Forms Database (LMFDB) [LMFDB]. We restrict to Galois-stable level $\mathfrak{N}$.

Remark 2.5.2. Since τ is nontrivial, we cannot have f arising as a base change from $\mathbb{Q}$. We also cannot manufacture such forms from twisted base change. To see this, suppose the form comes from twisted base change, say $f = f_0 \otimes \psi$ with f_0 from $\mathbb{Q}$ (i.e. $a_p(f_0) = a_{\sigma(p)}(f_0)$) and f non-CM. Then for $\mathfrak{p}$ a split prime, we have $a_{\mathfrak{p}}(f) = a_p(f)\psi(\mathfrak{p})$, so the congruence
$$\tau(a_{\mathfrak{p}}(f)) \equiv a_{\sigma(\mathfrak{p})}(f) \pmod 2$$
becomes
$$\tau(\psi(\mathfrak{p}))\tau(a_p(f)) \equiv \psi(\sigma(\mathfrak{p}))a_p(f) \pmod 2.$$
Of course if ψ is quadratic, then $\tau(a_p(f)) \equiv a_p(f) \pmod 2$ so in particular we do not have surjective trace modulo 2. Thus ψ must have order at least 3, so $K_f(\psi) = K_f$ is a CM field. But then we cannot have trivial Nebentypus character, since then the Hecke field is totally real.

In principle the congruence modulo 2 could be proved with a finite computation using Hecke–Sturm bounds [GP17]; however, the relevant bound here would be quite large. When the congruence lifts to an equality $\tau(f) = f^\sigma$ of eigenforms, with $\tau \in \mathrm{Gal}(K_f \mid F)$ the

nontrivial involution and $\sigma \in \mathrm{Gal}(F \mid \mathbb{Q})$ the nontrivial element, this can be proved almost instantly from the list of eigenforms by using just the first few Hecke eigenvalues.

We found 18 Hilbert newforms in the LMFDB with these properties. We group them according to quadratic twist—since these yield the same mod 2 Galois representation—and order by (absolute) conductor. In all cases, it turns out that the desired congruence is in fact an equality.

Remark 2.5.3. More generally, we would seek to prove an equality $\tau(f) - f^\sigma = 2h$ where $h \in S_2(\mathfrak{N})$ has algebraic integer Fourier coefficients, as this implies the desired congruence $\tau(a_\mathfrak{p}(f)) \equiv a_{\sigma(\mathfrak{p})}(f) \pmod 2$ for all good $\mathfrak{p}$. More generally, if there is a number ring $R \subseteq \mathbb{C}$, a Hecke module M over R (i.e., a set of pairwise computing maps $T_\mathfrak{p} \in \mathrm{End}_R(M)$ for all good $\mathfrak{p}$) and an isomorphism of Hecke modules $M_\mathbb{C} \to S_2(\mathfrak{N})$, then identifying $v \leftrightarrow f$ with $v \in M$ up to rescaling by $R^\times$, it is sufficient to prove that $\tau(v) - v^\sigma \in 2M$, which then becomes a congruence between entries in a pseudobasis for M.

This mechanism is particularly convenient working with forms on a definite quaternion order $\mathcal{O}$, using the Jacquet–Langlands correspondence (indeed, this is one way they can be computed; see Dembélé–Voight [DeV09]). In this case, the vector v is a linear combination of functions on the class set of a definite quaternion order [Voi21, Chapter 17], having its natural integral structure. We also verified the congruence (indeed, the equality) this way for all of our forms.

The forms found are as follows.

Field	Field label	Forms
$\mathbb{Q}(\sqrt{3})$	2.2.12.1	578.1-c, 578.1-d
$\mathbb{Q}(\sqrt{3})$	2.2.12.1	722.1-i, 722.1-j, 722.1-k, 722.1-l
$\mathbb{Q}(\sqrt{2})$	2.2.8.1	2601.1-j, 2601.1-k
$\mathbb{Q}(\sqrt{2})$	2.2.8.1	2738.1-e, 2738.1-f
$\mathbb{Q}(\sqrt{3})$	2.2.12.1	1587.1-i, 1587.1-l, 1587.1-m, 1587.1-n
$\mathbb{Q}(\sqrt{6})$	2.2.24.1	726.1-i, 726.1-j, 726.1-k, 726.1-l

Theorem 2.5.4. *The group $G = 17\mathsf{T}7$ is a Galois group over $\mathbb{Q}$.*

Proof. Applying Proposition 2.2.2 and Theorem 2.4.4 to the Hilbert modular forms above, we find at least 6 different number fields. □

Remark 2.5.5. We later also found the Hilbert modular form 2.2.77.1-99.1-j as an example of $f^\sigma \equiv \tau(f) \pmod 2$ but $f^\sigma \neq \tau(f)$.

Remark 2.5.6. While the main focus of this article is $G = 17\mathsf{T}7$, our methods also apply to other groups similarly arising as semidirect products. For example, one can realize $\mathrm{PSL}_2(\mathbb{F}_{64}) \rtimes C_i$ for $i \in \{2, 6\}$ as a Galois group over $\mathbb{Q}$ by exhibiting the forms 2.2.12.1-1250.1-m and 6.6.1229312.1-64.1-f.

3. (Re)constructive approach

In this section, we show how to explicitly go from a modular form f, as in §2, to an explicit polynomial that realizes the desired Galois group, e.g., 17T7. We first note in §3.2 that there is an abelian variety A_f associated to f whose L-function is related to that of f. In §3.3, we then define a conjectural period lattice attached to $A_f(\mathbb{C})$. Next, in §3.4, we use Oda's

conjecture, which can be viewed as an analogue of the BSD formula, to guess the period lattice from the central value of the (twisted) L-function of f. Finally, in §3.5, from this period lattice, we construct a polynomial whose roots correspond to $\mathfrak{l}$-isogenies from A_f, and which has the desired Galois group.

3.1. **Notation.** In the remainder of the paper, we discuss a constructive method to realize the Galois groups obtained from Hilbert modular forms as in the previous section, and in particular those in Theorem 2.5.4 realizing 17T7. To accomplish this task, we proceed as outlined in §1.2: we (conjecturally) compute periods via twists and construct a moduli point from ratios of these periods, and repeat for the Galois conjugates. We could then try to reconstruct an abelian variety as a (quotient of a) Jacobian; here, we instead evaluate modular functions to obtain the 2-isogeny polynomial.

As before, let f be a Hilbert newform of parallel weight 2 and level $\mathfrak{N}$ over the totally real field F, and let $n = [F : \mathbb{Q}]$. Let $K_f := \mathbb{Q}(\{a_\mathfrak{p}(f)\}_\mathfrak{p})$ be the field generated by its Hecke eigenvalues, and let $g = [K_f : \mathbb{Q}]$. Fix orderings of the embeddings $\sigma_i \colon F \hookrightarrow \mathbb{R}$ where $i = 1, \dots, n$, and $\tau_j \colon K_f \hookrightarrow \mathbb{C}$ where $j = 1, \dots, g$.

3.2. **Eichler–Shimura construction.** We begin with the following fundamental conjecture.

Conjecture 3.2.1 (Eichler–Shimura conjecture)**.** *Let f be a Hilbert newform over F of parallel weight 2 and level $\mathfrak{N}$ and Hecke field K_f. Then there exists an abelian variety A_f over F such that*

$$L(A_f, s) = \prod_{j=1}^{g} L(\tau_j(f), s).$$

More precisely, for every prime $\mathfrak{p} \nmid \mathfrak{N}$, we have

$$L_\mathfrak{p}(A_f, T) = \prod_j L_\mathfrak{p}(\tau_j(f), T) = \prod_j \left(1 - \tau_j(a_\mathfrak{p}(f))T + \mathrm{Nm}(\mathfrak{p})T^2\right)$$

where $a_\mathfrak{p}(f) \in K_f$ is the $\mathfrak{p}$-Hecke eigenvalue of f.

Theorem 3.2.2. *Suppose that either there exists a prime $\mathfrak{q} \parallel \mathfrak{N}$ or that $[F : \mathbb{Q}]$ is odd. Then Conjecture 3.2.1 holds.*

Proof. Under the given hypothesis, the Eichler–Shimizu–Jacquet–Langlands correspondence holds, and A_f is realized up to isogeny as a quotient of the Jacobian of a Shimura curve [Z01, Theorem B]. For further references, discussion, and examples, see Dembélé–Voight [DeV09, Theorem 3.9]. □

We note that the abelian variety A_f is only well-defined up to isogeny over F. The cases of Conjecture 3.2.1 missing from Theorem 3.2.2 are still open, for example when F is a real quadratic field and $\mathfrak{N}$ is a square.

When $F = \mathbb{Q}$, we can take the Shimura curve to be a modular curve, in which case we can integrate the modular form against a basis of modular symbols to get an analytic realization, giving a big period matrix for A_f (over $\mathbb{C}$). By contrast, the construction via Shimura curves is a bit oblique: although effective methods are available [GV11, VW14], it is still desirable to find an effective way to go more directly from the Hecke eigenvalues (equivalently, the q-expansions) of a Hilbert newform to an analytic realization.

3.3. **Period lattice.** In this section, we define a conjectural period lattice attached to a normalized Hilbert newform of parallel weight 2, following Oda [Oda82, Oda90], Darmon–Logan [DL03], Bertolini–Darmon–Green [BDG04, §7], and others, which was made effective for elliptic curves over real quadratic fields by Dembélé [Dem08].

From now on, to simplify notation we abbreviate $K = K_f$. Recall that F is a totally real field of degree n and let $\mathbb{Z}_F$ be its ring of integers. Moreover, let $F_{>0}^\times < F^\times$ be the subgroup of totally positive elements, let

$$\widehat{F} := \prod_{\mathfrak{p}}{}' F_{\mathfrak{p}} \tag{3.3.1}$$

be the finite adeles of F, and let $\widehat{\mathbb{Z}}_F := \prod_{\mathfrak{p}} \mathbb{Z}_{F,\mathfrak{p}} \subset \widehat{F}$ be the profinite completion of $\mathbb{Z}_F$ inside $\widehat{F}$. Let $\widehat{\Gamma} \leq \mathrm{GL}_2(\widehat{\mathbb{Z}}_F)$ be a finite index subgroup, let $\mathfrak{h}_\pm^n := (\mathbb{C} \smallsetminus \mathbb{R})^n$, and let

$$Y(\widehat{\Gamma}) := \mathrm{GL}_2(F) \backslash \mathrm{GL}_2(\widehat{F}) \times \mathfrak{h}_\pm^n / \widehat{\Gamma} \tag{3.3.2}$$

where $\mathrm{GL}_2(F)$ acts on the first factor by left multiplication and by linear fractional transformations on $\mathfrak{h}_\pm^n$, with the action on the i-th component of $\mathfrak{h}_\pm^n$ induced by the embedding σ_i, and where $\widehat{\Gamma}$ acts by right multiplication on $\mathrm{GL}_2(\widehat{F})$. Then

$$Y(\widehat{\Gamma}) = \bigsqcup_{[\mathfrak{b}]} \Gamma_{\mathfrak{b}} \backslash \mathfrak{h}^n \tag{3.3.3}$$

where $\mathfrak{h}^n \subseteq \mathfrak{h}_\pm^n$ is the connected component of $(i, \dots, i)$ (the product of n upper half-planes), the set $[\mathfrak{b}]$ ranges over the class group $F_{>0}^\times \backslash \widehat{F}^\times / \det(\widehat{\Gamma})$, and $\Gamma_{\mathfrak{b}}$ is idelically conjugate to $\Gamma := \widehat{\Gamma} \cap \mathrm{GL}_2(F)_{>0}$, a discrete group acting properly on $\mathfrak{h}^n$ [Voi21, 38.7.15]. Finally, let $X(\widehat{\Gamma}) \to Y(\widehat{\Gamma})$ be a smooth (toroidal) compactification of $Y(\widehat{\Gamma})$. Then $X(\widehat{\Gamma})$ is a disjoint union of smooth complex projective varieties of dimension n.

Example 3.3.4. In our case, we are interested in particular in the following special case: $\widehat{\Gamma} = \widehat{\Gamma}_1(\mathfrak{N})$, the standard congruence subgroup such that in the components with $\mathfrak{p}^e \parallel \mathfrak{N}$, the matrix is congruent to $\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$ modulo $\mathfrak{p}^e$. Then $\det(\widehat{\Gamma}) = \widehat{\mathbb{Z}}_F^\times$, so the components are indexed by elements $[\mathfrak{b}] \in \mathrm{Cl}^+ \mathbb{Z}_F$ in the narrow class group of F.

We now define Frobenius elements at infinity as follows. Let $W_\infty := \{\pm 1\}^n$. Write $s_i = (1, \dots, 1, -1, 1, \dots, 1) \in W_\infty$ with -1 in the i-th place. Define

$$\varepsilon_{s_i}(z_1, \dots, z_n) = (z_1, \dots, z_{i-1}, \overline{z_i}, z_{i+1}, \dots, z_n)$$

for $z = (z_1, \dots, z_n) \in \mathfrak{h}_\pm^n$, and extend to $s \in W_\infty$. Then the action of W_∞ descends to $Y(\widehat{\Gamma})$ and then extends to $X(\widehat{\Gamma})$ [Oda90, (1.3)].

Example 3.3.5. If there exists $\eta \in \mathbb{Z}_F^\times$ such that $\mathrm{sgn}(\eta) = s$, then we may take $\varepsilon_s((z_i)_i) = (s_i \eta_i z_i)_i$ —this is the star involution in the case of modular curves ($z \mapsto -\overline{z}$, the unit being -1).

Then W_∞ acts on $H^n(X, \mathbb{Q})$ by pullback, and we get ε_s^*-eigenspaces. The operators ε_s^* also commute with the action of the Hecke operators $T_{\mathfrak{n}}$ for ideals $\mathfrak{n}$ coprime to $\mathfrak{N}$.

Suppose now that $\widehat{\Gamma}$ is a standard congruence subgroup and f is a Hilbert newform on $X(\widehat{\Gamma})$ with parallel weight 2. The eigenspace for the Hecke operators $T_{\mathfrak{n}}$ acting on $H^n(X, \mathbb{Q})$

matching f is a $\mathbb{Q}$-subspace $V_f \subseteq H^n(X, \mathbb{Q})$ with an action of K such that $\dim_K V_f = 2^n$, for example containing

$$\omega_{\tau_j(f)} := (2\pi i)^n \tau_j(f)(z_1, \dots, z_n)\, \mathrm{d}z_1 \dots \mathrm{d}z_n \in H^n_{\mathrm{dR}}(X(\widehat{\Gamma}), \mathbb{C})\,, \tag{3.3.6}$$

for any embedding $\tau_j \colon K \hookrightarrow \mathbb{C}$ [Oda90, (2.1)]. Moreover, V_f inherits an action of W_∞.

Theorem 3.3.7. *The K-vector space V_f can be equipped with a polarized K-Hodge structure, with*

$$V_f \otimes_{\mathbb{Q}} \mathbb{C} \simeq \bigoplus_j V_f \otimes_{\tau_j} \mathbb{C} \tag{3.3.8}$$

such that for all $1 \le j \le g$ and all $0 \ne p \le n$,

$$(V_f \otimes_{\tau_j} \mathbb{C})^{p,n-p} = \bigoplus_s \mathbb{C}\varepsilon_s^*(\omega_{\tau_j(f)}) \tag{3.3.9}$$

where we sum over $s \in W_\infty$ with p plus signs.

Proof. See Oda [Oda90, Construction (3.23) (iii)]. □

Let $\gamma_s \in H_n(X, \mathbb{Q})$ be a dual basis to $\varepsilon_s^* \omega_{\tau_1(f)}$ where s ranges over W_∞. Define

$$\Omega_j^s := \int_{\gamma_s} \omega_{\tau_j(f)} \in \mathbb{C}. \tag{3.3.10}$$

for $j = 1, \dots, g$. We map

$$K \hookrightarrow \mathrm{M}_g(\mathbb{C})$$

by diagonal matrices taking the embeddings $\tau_1, \dots, \tau_g$. For $s \in \{s_1, \dots, s_n\}$, let

$$V_{f,s} := K \begin{pmatrix} \Omega_1^s \\ \vdots \\ \Omega_g^s \end{pmatrix} \oplus K \begin{pmatrix} \Omega_1^+ \\ \vdots \\ \Omega_g^+ \end{pmatrix} \subsetneq \mathbb{C}^g \tag{3.3.11}$$

where we abbreviate $+ = (+1, \dots, +1)$.

Conjecture 3.3.12 ([Oda82, Main Conjecture $\mathrm{A}^{\mathrm{split}}$, p. xii])**.** *For any choice of lattice $\Lambda \subset V_{f,s}$, we have*

$$\mathbb{C}^g/\Lambda \sim A_f(\mathbb{C})$$

for A_f as in Conjecture 3.2.1, under the corresponding embedding $\sigma \colon F \hookrightarrow \mathbb{C}$, i.e., if $s = s_i$, then $\sigma = \sigma_i$.

The choice of lattice is rather unclear at this point: we may start with

$$\Lambda_s(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \begin{pmatrix} \Omega_1^s \\ \vdots \\ \Omega_g^s \end{pmatrix} \oplus \mathfrak{b} \begin{pmatrix} \Omega_1^+ \\ \vdots \\ \Omega_g^+ \end{pmatrix} \tag{3.3.13}$$

with $\mathfrak{a}, \mathfrak{b}$ fractional ideals of K. On the lattice $\mathfrak{a} \oplus \mathfrak{b}$ and $c \in K^\times_{>0}$, we define the alternating $\mathbb{Z}$-linear pairing

$$\begin{aligned} E_c \colon (\mathfrak{a} \oplus \mathfrak{b}) \times (\mathfrak{a} \oplus \mathfrak{b}) &\to \mathbb{Q} \\ (a_1, b_1), (a_2, b_2) &\mapsto \mathrm{Tr}_{K|\mathbb{Q}}(c(a_1 b_2 - a_2 b_1)). \end{aligned} \tag{3.3.14}$$

The pairing can also be considered as a pairing on $\Lambda_s(\mathfrak{a},\mathfrak{b})$. For this pairing to induce a principal polarization, we require

$$c\mathfrak{a}\mathfrak{b} = \mathbb{Z}_K^\sharp, \tag{3.3.15}$$

where $\mathbb{Z}_K^\sharp := \{a \in K : \mathrm{Tr}_{H|\mathbb{Q}}(a\mathbb{Z}_K) \subseteq \mathbb{Z}\}$ is the trace dual (i.e., the codifferent) of $\mathbb{Z}_K$. (Cf. [Gor02, Corollary 2.10].) When $\mathrm{Cl}^+(\mathbb{Z}_K)$ is trivial, we take just $\Lambda_s(\mathbb{Z}_K,\mathbb{Z}_K)$ with c a totally positive generator of the codifferent.

Choosing a symplectic basis for $\Lambda_s(\mathbb{Z}_K,\mathbb{Z}_K)$ with respect to the pairing E_c (3.3.14), one obtains a big period matrix $\Pi_s \in \mathrm{M}_{g,2g}(\mathbb{C})$. The small period matrix $Z \in \mathcal{H}_g$ is the $g \times g$ symmetric matrix with totally positive definite imaginary part defined by the property

$$\Pi_s \sim \begin{pmatrix} Z & 1_g \end{pmatrix}. \tag{3.3.16}$$

In similar fashion we define

$$z_{f,s} := \left(\frac{\Omega_1^s}{\Omega_1^+},\dots,\frac{\Omega_g^s}{\Omega_g^+}\right) \in \mathfrak{h}^g. \tag{3.3.17}$$

With the choices made above, this is the same abelian variety with RM by $\mathbb{Z}_K$ as a point in one component of the Hilbert moduli space. Of course, this moduli point is only unique up to the natural action of $\mathrm{SL}_2(\mathbb{Z}_K)$.

3.4. **Periods and L-values.** Recall that each embedding τ_j gives rise to an L-function

$$L(\tau_j(f),s) = \prod_{\mathfrak{p}|\mathfrak{N}}\left(1-\tau_j(a_\mathfrak{p})\,\mathrm{Nm}(\mathfrak{p})^{-s}\right)^{-1}\prod_{\mathfrak{p}\nmid\mathfrak{N}}\left(1-\tau_j(a_\mathfrak{p})\,\mathrm{Nm}(\mathfrak{p})^{-s}+\mathrm{Nm}(\mathfrak{p})^{1-2s}\right)^{-1}$$

Let $\mathfrak{c} \subseteq \mathbb{Z}_F$ be a nonzero ideal. Let $F_{\mathfrak{c}\infty}$ be the Hilbert class field of F of conductor $\mathfrak{c}\infty$, and let

$$\chi\colon \mathrm{Gal}(F_{\mathfrak{c}\infty}\,|\,F) \to \mathbb{C}^\times \tag{3.4.1}$$

be a (narrow ray class) character. By class field theory, χ corresponds also to a (finite order) Hecke character of modulus $\mathfrak{c}$. Associated to χ is its finite part

$$\chi_0\colon (\mathbb{Z}_F/\mathfrak{c})^\times \to \mathbb{C}^\times \tag{3.4.2}$$

and an infinite part sign

$$\chi_\infty\colon \{\pm1\}^n \to \{\pm1\}, \tag{3.4.3}$$

satisfying the compatibility

$$\chi(a\mathbb{Z}_F)^{-1} = \chi_0(a)\chi_\infty(\mathrm{sgn}(a)) \tag{3.4.4}$$

for all $a \in \mathbb{Z}_F$ coprime to $\mathfrak{c}$, where $\mathrm{sgn}\colon F^\times \to \{\pm1\}^n$ records the signs under the real embeddings of F. In the notation above, we have $\chi_\infty \in W_\infty$.

Denote by $L(\tau_j(f),s,\chi)$ the twist of this L-function by the Hecke character χ. The Euler factors of this twisted L-function at the primes $\mathfrak{p}$ not dividing $\mathfrak{c}+\mathfrak{N}$ are

$$1-\tau_j(a_\mathfrak{p}\chi(\mathfrak{p}))\,\mathrm{Nm}(\mathfrak{p})^{-s}+\tau_j(\chi(\mathfrak{p}))^2\,\mathrm{Nm}(\mathfrak{p})^{1-2s}. \tag{3.4.5}$$

Moreover, it has an analytic continuation to the whole complex plane, and its completed L-function satisfies a functional equation.

The following theorem, originally stated by Oda in [Oda82, Prop. 16.3] for F of narrow class number one, relates the twisted periods with the special values of certain twisted L-functions associated to the Hilbert modular form.

Theorem 3.4.6 ([G88, Theorem VI.7.5]). *Let $\chi\colon (\mathbb{Z}_F/\mathfrak{c})^\times \to \mathbb{C}^\times$ be a quadratic character of sign $s \in W_\infty$. There exists $\alpha_\chi \in K$ such that for all $j = 1, \dots, g$*

$$\tau_j(\alpha_\chi)\Omega_j^s = -4\pi^2\sqrt{\operatorname{disc}(F)}G(\overline{\chi})L(\tau_j(f), 1, \chi),$$

where $G(\chi)$ is the Gauss sum of χ.

Based on the Birch and Swinnerton-Dyer conjecture, it is conjectured that α_χ actually lies in $\mathbb{Z}_K$ for $\operatorname{cond}(\chi) \gg 0$; see [BDG04, § 7] or [Dem08, Conjecture 3.3] (when F has narrow class number 1).

While all the terms on the right hand side of the equality can be computed, the same is not immediately true for α_χ. In comparison with the Birch and Swinnerton-Dyer conjecture, the α_χ correspond to some of the invariants like the Tamagawa numbers that can vary for different characters χ with the same sign s. One can use multiple characters χ for each sign s and use a lattice based method to determine a likely value for α_χ. This trick, also called Cremona's trick, is described in [Dem08, Remark 5.2] and has its origin in [Cre97, Section 2.11].

3.5. **$\mathfrak{l}$-isogeny polynomial.** Let A be an abelian variety defined over $\mathbb{C}$ with real multiplication by an order $\mathcal{O}$ in a number field K. Let $\mathfrak{l}$ be an ideal of $\mathcal{O}$. For simplicity, we assume $\mathfrak{l}$ is principal. We now define a polynomial generating the $\mathfrak{l}$-isogeny field of the corresponding real multiplication abelian variety. We work with $\mathfrak{l}$-isogenies rather than $\mathfrak{l}$-torsion points because the splitting field of the resulting polynomial cuts out the projective representation $\mathrm{P}\rho_{f,\mathfrak{l}}$ (Corollary 2.4.7), which is what we need for our Galois realization.

Let e be a Hilbert modular form of weight k of trivial level (below we will use the restriction of a Siegel Eisenstein series), and $z \in \mathfrak{h}^g$ be a point corresponding to the A in the Hilbert moduli space, see (3.3.17).

For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O})$, we define the factor of automorphy

$$j(\gamma, z) := \prod_{\iota: K \hookrightarrow \mathbb{R}} \frac{(\iota(c) + \iota(d)z)^k}{\det(\iota(\gamma))^k}.$$

Thus, we can define the $\mathfrak{l}$-isogeny polynomial

$$T_{\mathfrak{l}}(x) := \prod_{\gamma} \left(x - j(\gamma, z)^{-1} \frac{e(\gamma z)}{e(z)} \right) \in \mathbb{C}[x],$$

where γ ranges over some elements of $M_2(\mathcal{O}) \cap \mathrm{GL}_2(K)$ whose determinant generates $\mathfrak{l}$, such that $z' = \gamma z$ ranges over points corresponding to all abelian varieties $\mathfrak{l}$-isogenous to A. (If $\mathfrak{l}$ were actually not principal, then this does work, and can be salvaged by doing it adelically.)

This $\mathfrak{l}$-isogeny polynomial simultaneously generalizes the classical modular polynomial in two distinct directions. First, rather than relying on the classical j-invariant, it allows the use of an arbitrary modular function (constructed as a ratio of modular forms) with rational Fourier coefficients. Second, it naturally extends the theory to higher-dimensional abelian varieties with real multiplication, replacing evaluations on the classical j-line with evaluations on the Hilbert moduli space.

For practical purposes, it is convenient to use a modular form e that can be expressed in terms of the Riemann theta function through the natural embedding $\mathfrak{h}^g \hookrightarrow \mathcal{H}_g$, see (3.3.16).

For $a, b \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$, the Riemann theta function with characteristics a, b is defined as

$$\begin{aligned}\vartheta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right] : \mathbb{C}^g \times \mathcal{H}_g &\to \mathbb{C} \\ (w, Z) &\mapsto \sum_{n\in\mathbb{Z}^g} \exp\left(\pi i(n+a)^t Z(n+a) + 2\pi i(n+a)^t(w+b)\right) .\end{aligned} \tag{3.5.1}$$

For our computations we pick e to be the restriction to $\mathfrak{h}^g$ of the Siegel Eisenstein series of weight 4, which can be expressed as the sum of the eighth powers of the theta constants:

$$E_4(Z) := \sum_{a,b} \vartheta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](0, Z)^8 . \tag{3.5.2}$$

(See [Igu64, p. 405].)

Taking Z to be the small period matrix (3.3.16), the $\mathfrak{l}$-isogeny polynomial $T_\mathfrak{l}(x)$, which can be expressed in terms of the Siegel Eisenstein series evaluated at Z, is defined over F as a consequence of Conjecture 3.3.12.

4. The inverse Galois problem for 17T7

In this section, we explain in detail the calculation that gives the 17T7 polynomial in Theorem 2.4.4. The code used to perform these computations is available at [vB+24a] and [vB+24b].

4.1. **Computing the small period matrix.** Let $F := \mathbb{Q}(\sqrt{3})$ and let $\mathbb{Z}_F = \mathbb{Z}[\sqrt{3}]$ be its ring of integers (of discriminant 12). Then $\mathbb{Z}_F$ has class number 1 but narrow class number 2, with the narrow class group $\mathrm{Cl}^+\mathbb{Z}_F$ generated by the unique prime $(1+\sqrt{3})$ above 2. The narrow Hilbert class field is $F(\sqrt{-1}) = \mathbb{Q}(\zeta_{12})$.

Let f be the Hilbert modular form over F with LMFDB label 2.2.12.1-578.1-c. Then f has level $\mathfrak{N} = 17(1+\sqrt{3})$, trivial Nebentypus character, and Hecke eigenvalue field $K = K_f = \mathbb{Q}(\nu)$ with LMFDB label 4.4.725.1 and defining polynomial

$$x^4 - x^3 - 3x^2 + x + 1 . \tag{4.1.1}$$

Nearby is the form f' with label 2.2.12.1-578.1-d, which is the quadratic twist of f by the nontrivial character of the narrow class group.

Remark 4.1.2. We could equally well compute in this section and the next with the form f'; we just chose to work alphabetically.

Using Magma (see Dembélé–Voight [DeV09] for a description of the algorithms), we compute Hecke eigenvalues $a_\mathfrak{p}$ of f for all prime ideals $\mathfrak{p}$ of F with $\mathrm{Nm}(\mathfrak{p}) < 80\,000$. We form the truncation of the L-function using these $a_\mathfrak{p}$ and, using Hecke characters χ with conductors up to 25, compute twisted periods as described in §3.4 using [Dok04]. In fact, to get more precision for our computation with the $a_\mathfrak{p}$'s that we computed, we use the fact that $\Omega_j^{++}\Omega_j^{--} + \Omega_j^{+-}\Omega_j^{-+} = 0$, which follows from [Oda82, Theorem 4.4]. This yields RM moduli points with 80 decimal digits of precision

$$\begin{aligned} z_{+-} &\approx (2.7829i, 0.75416i, 1.4277i, 5.0448i) \\ z_{-+} &\approx (0.75416i, 2.7829i, 5.0448i, 1.4277i) \end{aligned}$$

as in (3.3.17). Note that z_{+-} and z_{-+} are, up to precision, related by the double transposition (1 2)(3 4). This is because in fact our abelian fourfold descends to $\mathbb{Q}$ (the two conjugates over F are isomorphic), whence it suffices to simply consider the first moduli point $z := z_{+-}$.

We compute that the different ideal $\mathfrak{D}_K = (\mathbb{Z}_K^\sharp)^{-1} = (d)$ of K (cf. §3.3) is narrowly principal with generator $d := -2\nu^3 + 4\nu^2 + 3\nu + 2$. Since the different is narrowly principal, the abelian fourfold $\mathbb{C}^g / \Lambda$ with $\Lambda := \Lambda_{+-}(\mathbb{Z}_K, \mathbb{Z}_K)$ as in (3.3.13) is principally polarizable; see §3.3. We note that Λ is equipped with the pairing

$$E_{d^{-1}} \colon (\mathbb{Z}_K \oplus \mathbb{Z}_K) \times (\mathbb{Z}_K \oplus \mathbb{Z}_K) \to \mathbb{Q}$$
$$(a_1, b_1), (a_2, b_2) \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(d^{-1}(a_1 b_2 - a_2 b_1)),$$

as in (3.3.14).

The periods Ω_j^s obtained from Theorem 3.4.6 are purely imaginary or purely real; thus the same holds for z_s. Consequently, the complex torus constructed above may be off by a 2-isogeny. Indeed, consider any lattice $L \subset \mathbb{C}^g$ invariant under complex conjugating, and let L' be the sublattice generated by the real and totally imaginary parts of L. Then, for every $\lambda \in L$, both $\lambda + \overline{\lambda}$ and $\lambda - \overline{\lambda}$ lie in L'. Hence $2\lambda \in L$, so L/L' is killed by 2. Equivalently, the natural map

$$\mathbb{C}^g/L' \longrightarrow \mathbb{C}^g/L$$

has kernel contained in the 2-torsion. Thus we search over all $2^g + 1 = 17$ abelian varieties that are 2-isogenous to $\mathbb{C}^g/\Lambda$ and have RM by $\mathbb{Z}_K$.

For this particular example, the knowledge that our desired abelian 4-fold is a Jacobian (see §4.3 below) simplifies this step of the calculation. We find a unique 2-neighbor $z' \in \mathfrak{h}^g$ such that the value of the Schottky modular form at its period matrix has absolute value $< 10^{-56}$. Thus this is the only likely Jacobian among the 2-neighbors of z.

4.2. **Finding the 2-isogeny polynomial.** We compute the 2-isogeny polynomial for Z as in §3.5, evaluating theta functions using the fast code of Elkies–Kieffer [EK] available in FLINT [Flint, `acb_theta`]. We find the polynomial

$$T(x) := x^{17} - 581020.41645\ldots x^{16} - 54729032212.54644\ldots x^{15}$$
$$- 2958404450460894.75024\ldots x^{14} + \cdots$$

We are able to recognize the coefficients of x^{16} and x^{15} (which are known to the highest precision) as rational numbers with denominators $D := 267075169$ and D^2, respectively. Replacing $T(x)$ by $T_D := D^{17}T(x/D)$ in order to clear this denominator, we are then able to recognize the coefficients of x^{16}, x^{15}, x^{14}, and x^{13} as integers a_1, a_2, a_3, and a_4. In order to obtain higher precision approximations for the rest of the coefficients of T_D, we use Newton's method on the function that takes a point $z \in \mathfrak{h}^4$ to the coefficients of x^{16}, x^{15}, x^{14}, and x^{13} of its 2-isogeny polynomial. This produces a normalized 2-isogeny polynomial T_D with coefficients that are easily recognized as integers:

$$\begin{aligned} T(x) = x^{17} &- 155176125916688x^{16} - 39037751234563273371263727 44x^{15} - \ldots \\ &- 153702846916677613155795943357742165422510948 26\cdots 14304 \end{aligned} \tag{4.2.1}$$

where the constant term has 204 decimal digits.

Applying the PARI/GP [Pari] command `polredabs` [CDD91], we find the simplified polynomial given in (1.1.4) that defines an isomorphic number field. We verify that this polynomial has Galois group 17T7 using the Magma commands `GaloisGroup` and `GaloisProof`; this

uses the method of relative invariants due to Stauduhar [Sta73], and the implementation is elaborated upon in Fieker–Klüners [FK14]. The ring of integers of the number field L defined by this polynomial has discriminant $2^{44} \cdot 3^6 \cdot 17^8$ and has now been included in the LMFDB with label 17.1.894620217503348347361034 24.1.

The total CPU time was dominated by the computation of the eigenvalues of the Hilbert modular form—we did not keep a precise count of this time (we computed more than we needed), but it was on the order of a few CPU years.

Remark 4.2.2. In general, the polynomial $T(x)$ will have coefficients in F and not necessarily in $\mathbb{Q}$. In that case, we can recognize its coefficients by considering all embeddings of T into $\mathbb{C}$ simultaneously. Then the extension as in Theorem 2.4.4 can be found by taking the splitting field of T over F, and then taking its normal closure over $\mathbb{Q}$.

Remark 4.2.3. Our number field L has class number 3, a fact which may seem quite remarkable. Using Magma, we can explicitly construct this Hilbert class field. In fact, there is some structure behind this unramified extension, as follows.

Let S be the stabilizer of an element in $\mathbb{P}^1(\mathbb{F}_{16})$ under the action of 17T7 by linear fractional transformations, and let L be the fixed field of S. (Its commutator subgroup $S' \trianglelefteq S$ in fact has index 6.) There is an index 3 subgroup coming from the natural further scaling action on the fixed vector: it is the subgroup $\mathbb{F}_4^\times \leq \mathbb{F}_{16}^\times$ stabilized by the order 2 subgroup of $\mathrm{Gal}(\mathbb{F}_{16} \,|\, \mathbb{F}_2)$. In this way, we obtain a cyclic extension $L' \supseteq L$ of degree 3 for all 17T7 extensions. In our case, the abelian variety is semistable, so the inertia groups at 2 and 17 act through a unipotent subgroup and hence the extension $L' \supseteq L$ is unramified. (See also the proof of Proposition 4.3.6 below.)

4.3. **Relation to Shimura curves.** Although it is not necessary for our method, it is natural to wonder why the abelian fourfold we have constructed numerically seems to be (isogenous to) a Jacobian. Indeed, in this special case, we have a very exceptional situation and can prove that this is the case.

First, we set up the notation and do some preliminary calculations. Let $\mathfrak{p}_2 = (1+\sqrt{3})$ be the unique prime above 2 in $\mathbb{Z}_F$. Then $\mathfrak{p}_2$ generates the narrow class group $\mathrm{Cl}^+ \mathbb{Z}_F \simeq \mathbb{Z}/2\mathbb{Z}$. Let B be the quaternion algebra over $F = \mathbb{Q}(\sqrt{3})$ ramified at $\mathfrak{p}_2$ and at one of the two real places.

Let $\mathcal{O}$ be an Eichler order of prime level (17). We claim that $\mathcal{O}$ is unique up to conjugation in $B^\times$ (i.e., the type set of $\mathcal{O}$ is trivial). Indeed, $\mathcal{O}$ is hereditary [Voi21, §23.3] so its idelic normalizer has [Voi21, Corollary 23.3.14]

$$N_{\widehat{B}^\times}(\widehat{\mathcal{O}})/(\widehat{F}^\times \widehat{\mathcal{O}}^\times) = \langle \varpi_2, \varpi_{17} \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

generated by elements ϖ_2 supported at $F_{\mathfrak{p}}$ and ϖ_{17} supported at F_{17} and whose reduced norms are uniformizers (so $\mathrm{nrd}(\varpi_2) = 1+\sqrt{3}$ and $\mathrm{nrd}(\varpi_{17}) = 17$). Then, as a consequence of strong approximation [Voi21, Corollary 28.5.10] we compute that the type set of $\mathcal{O}$ is the quotient of $\mathrm{Cl}^+ \mathbb{Z}_F$ by the ideals $\mathfrak{p}_2$ and (17), so is indeed trivial.

Now since B is split at the other real place, it yields an embedding $\iota_\infty \colon B \hookrightarrow \mathrm{M}_2(\mathbb{R})$ unique up to conjugation by $\mathrm{GL}_2(\mathbb{R})$. Let $\mathcal{O}^\times_{>0}$ be the group of units of $\mathcal{O}$ whose reduced norm is positive at both real places (they are automatically positive at the ramified real place). Then under ι_∞, the group $\mathrm{P}\mathcal{O}^\times_{>0} = \mathcal{O}^\times_{>0}/\mathbb{Z}_F^\times$ is a discrete group acting properly on the upper half-plane $\mathfrak{h}$, and the quotient $X^+(\mathfrak{p}_2; 17) := \mathrm{P}\iota_\infty(\mathcal{O}^\times_{>0})\backslash\mathfrak{h}$ is a Shimura curve of

genus 11 with signature $(11; 2, 2, 3, 3, 12, 12; 0)$ (compact with six elliptic points of the given orders) [Voi09, Ric22]. Finally, since (17) is narrowly principal there is an Atkin–Lehner involution $w_{17} \in N_{B^\times}(\mathcal{O})_{>0}$, and the further quotient $X^+(\mathfrak{p}_2; 17)/\langle w_{17} \rangle$ has genus 4 (more precisely, signature $(4; 2, 2, 2, 2, 2, 2, 2, 2, 2, 3, 12; 0)$).

Proposition 4.3.1. *There exists a smooth, projective, geometrically integral curve X' defined over $\mathbb{Q}$ with the property that $X'(\mathbb{C}) \simeq X^+(\mathfrak{p}_2; 17)/\langle w_{17} \rangle$ and $\operatorname{Jac} X'_F$ is isogenous to $A_{f'}$ where f' is the Hilbert modular form with label 2.2.12.1-578.1-d.*

Proof. The idelic Shimura curve [Voi21, §38.7] attached to $\widehat{\mathcal{O}}^\times$, namely

$$B^\times_{>0} \backslash (\widehat{B}^\times \times \mathfrak{h}) / \widehat{\mathcal{O}}^\times$$

has two components, indexed by $\mathrm{Cl}^+ \mathbb{Z}_F$ [Voi21, (38.7.14)]. Its canonical model (due to Shimura [Shi67] and Deligne [Del71]) is defined over the reflex field, which is F; and the components are defined over the narrow class field of F, namely $F(\sqrt{-1})$. The Atkin–Lehner involution w_{17} (preserving components) is defined over F.

This matches the associated calculation of Hilbert modular forms of parallel weight 2. The space of Hilbert modular forms of level $\mathfrak{N}$ which are new at $\mathfrak{p}_2$ are those of levels $\mathfrak{p}_2$ and $\mathfrak{N} = 17\mathfrak{p}_2$, but there are no newforms of level norm 2 so all are newforms of level norm 578. The total dimension of this space is $1 + 1 + 4 + 4 + 6 + 6 = 22 = 2 \cdot 11$. Moreover, the forms with Atkin–Lehner eigenvalue 1 for (17) form a space of dimension $4 + 4 = 8 = 2 \cdot 4$, so the Jacobian of the quotient of the above idelic Shimura curve by the Atkin–Lehner involution w_{17} is isogenous (over F) to the product of the abelian varieties attached to f', the quadratic twist of f (given by 2.2.12.1-578.1-c and computed in the previous section) by the nontrivial narrow class character.

By a theorem of Doi–Naganuma [DN67, Corollary, p. 449], since the type number of $\mathcal{O}$ is 1 (their "narrow sense", see 1.4 in loc. cit.), the field of moduli of either component is $\mathbb{Q}$. Finally, the elliptic point of order 12 is unique, so the provided isomorphisms among the conjugates over $F(\sqrt{-1})$ must be pointed. We claim moreover that the Atkin–Lehner involution w_{17} also has field of moduli $\mathbb{Q}$: indeed, the subgroup of geometric automorphisms of a curve of genus ≥ 2 fixing a point is a finite cyclic group (in characteristic 0), so an involution is uniquely determined by its set of fixed points when nonempty. We confirm from the signature that the involution w_{17} has fixed (CM) points (or more simply, a fixed-point free involution of a curve of genus 11 has quotient of genus 6 by Riemann–Hurwitz). It follows then by pointed descent [SV16, Theorem A] that the curve, the point, and the quotient map descend canonically to $\mathbb{Q}$!

This applies to both components, so we obtain two curves of genus 4 over $\mathbb{Q}$. Upon extension to F, their Jacobians give the two abelian fourfolds under consideration, so one corresponds to A_f over F. We can isolate this component directly: there is still an Atkin–Lehner involution attached to $\mathfrak{p}_2$ defined over F defined on the idelic Shimura curve: it has degree 1 (since $\mathfrak{p}_2$ is ramified) and interchanges the two components. The quotient by this automorphism picks out a component according to its eigenvalue for this involution, opposite to that of the Hilbert modular form. □

Remark 4.3.2. A moduli-theoretic proof of the descent in Proposition 4.3.1 should also be possible: the data that defines the moduli problem is defined over F; in particular the Atkin–Lehner involutions are defined over F, and we find that there is an isomorphism to

the moduli problem which is conjugate under the nontrivial element of $\mathrm{Gal}(F \mid \mathbb{Q})$. This is another way to view the aforementioned result of Doi–Naganuma. This ensures that the field of moduli is $\mathbb{Q}$, and pointed descent then gives field of definition $\mathbb{Q}$.

In [Bou23], Bouchet presents a collection of invariants that classify genus 4 curves over an algebraically closed field; in [Bou24] he shows, given such a collection of invariants, how to produce a genus 4 curve with these invariants. Starting with the small period matrix Z (3.3.16), we first apply the methods of Hanselman–Pieper–Schiavone [HPS24] to produce approximate equations over $\mathbb{C}$ of a genus 4 curve corresponding to Z. We then compute numerical approximations of the Bouchet invariants of this curve, recognize them as rational numbers, and then reconstruct a genus 4 curve with these invariants using [Bou24]. We obtain the curve X_0 (the notation chosen to indicate descent to $\mathbb{Q}$) given by

$$\begin{aligned} 0 &= -8x^2 + 8xy + 17y^2 - 34xz - 2yz - 28z^2 - 10xw - 9yw - 18zw + 2w^2, \\ 0 &= 4x^3 - 6x^2y - 6xy^2 + 12x^2z + 6xyz + 24y^2z - 12xz^2 - 24z^3 + 2x^2w + 7xyw \\ &\quad + 4y^2w + 4xzw - 13yzw - 8z^2w - 20xw^2 - 3zw^2 - 12w^3 \end{aligned} \tag{4.3.3}$$

inside the projective space $\mathbb{P}^3$ with coordinates x, y, z, w.

Remark 4.3.4. If we had computed in the previous two sections with f' instead of f, since the associated abelian fourfolds being isomorphic over $\mathbb{C}$ we would have obtained the same invariants and hence the same reconstruction (4.3.3).

A computation with discriminants shows that this model has good reduction away from the primes 2, 3, 7, and 17. Projection from the point $(-12 : 2 : 4 : 3) \in X_0(\mathbb{Q})$ and a change of variables to minimize yields the singular affine plane model as in (1.1.6). Projection from the point $(-2 : -2 : 3 : 1)$ gives the model

$$\begin{aligned} &20x^5 + 34x^4y + 172x^4 - 6x^3y^2 + 60x^3y + 576x^3 - 61x^2y^3 - 606x^2y^2 + 204x^2y \\ &\quad + 776x^2 - 75xy^4 - 822xy^3 - 972xy^2 + 168xy + 384x - 34y^5 \\ &\quad - 338y^4 - 688y^3 - 448y^2 - 32y + 32 = 0 \end{aligned} \tag{4.3.5}$$

which reduces modulo 7 to a curve of genus 4, giving a model for X_0 with good reduction at 7.

Proposition 4.3.6. *Let $A_0 := \mathrm{Jac}(X_0)$ be the Jacobian of X_0. Then $A_{0,F}$ is isogenous to $A_{f'}$ over F.*

Our computations are performed in Magma.

Proof. We certify using the methods of Costa–Mascot–Sijsling–Voight [CMSV19] that indeed $\mathrm{End}\, A_0 \simeq \mathbb{Z}[(1+\sqrt{5})/2]$ (over $\mathbb{Q}$) and $\mathrm{End}\, A_0^{\mathrm{al}}$ is isomorphic with the ring of integers $\mathbb{Z}_K$ of the quartic field K, and the endomorphisms are defined over $F = \mathbb{Q}(\sqrt{3})$ (i.e. $\mathrm{End}\, A_0^{\mathrm{al}} = \mathrm{End}(A_0)_{\mathbb{Q}(\sqrt{3})}$). The endomorphism ring is certified by exhibiting an explicit correspondence, i.e., by representing endomorphisms by their graphs in $\mathrm{Sym}^4 X_0 \times \mathrm{Sym}^4 X_0$, via the birational map $A_0 \to \mathrm{Sym}^4 X_0$. (In our case, this took about 8 CPU days to compute and takes over 32 MB to store.)

Next, the closure in the projective plane of the model (1.1.6) has points $(1 : 1 : 4)$ and $(1 : 0 : 0)$, and we verify that the difference $D := (1 : 1 : 4) - (1 : 0 : 0)$ gives $[D] \in A_0(\mathbb{Q})$

with order 29: using an algorithmic version of the Riemann–Roch theorem, there exists a rational function h whose divisor is $29D$. Moreover, A_0 has good ordinary reduction at $p = 29$—we have $L(X_{\mathbb{F}_{29}}, T) = 1 + 45T^2 + 2187T^4 + 45 \cdot 29^2T^6 + 29^4T^8$ and $2187 \equiv 12 \not\equiv 0 \pmod{29}$.

From now on, to ease notation in the proof we abbreviate $A = (A_0)_F$. The prime 29 factors as $29\mathbb{Z}_K = \mathfrak{p}^2\mathfrak{p}'$ where $\operatorname{Nm}\mathfrak{p} = 29$. Over F, since A has RM the natural 29-adic representation factors as

$$\rho_{A,\mathfrak{p}^\infty} \colon \operatorname{Gal}_F \to \operatorname{GL}_2(K_\mathfrak{p}).$$

Let $\rho_{A,\mathfrak{p}} \colon \operatorname{Gal}_F \to \operatorname{GL}_2(\mathbb{F}_\mathfrak{p})$ be the associated semisimple representation modulo $\mathfrak{p}$ as in (2.4.3). We just saw there is a torsion point of order 29 (in fact already defined over $\mathbb{Q}$), so the semisimplification is reducible: $\rho_{A,\mathfrak{p}} \simeq \chi_1 \oplus \chi_2$ where χ_2 is the trivial character and $\chi_1 = \varepsilon_{29,F} \colon \operatorname{Gal}_F \to \mathbb{F}_{29}^\times$ is the mod 29 cyclotomic character over F.

We use this to immediately conclude that A has semistable reduction at all primes $\mathfrak{q} \neq \mathfrak{p}$. Indeed, $\rho_{A,\mathfrak{p}}$ over $F(\zeta_{29})$ is unipotent, so Grothendieck's inertial semistable reduction criterion applies.

We now verify the hypotheses of Skinner–Wiles [SW98, Theorem A] in the residually reducible case. By Theorem 2.4.1, the representation $\rho_{A,\mathfrak{p}^\infty}$ is unramified away the primes above 29 and the primes of bad reduction. This representation is also irreducible, since $\det(1 - \rho_{A,\mathfrak{p}^\infty}(\operatorname{Frob}_\mathfrak{q})T)$ is irreducible over $K_\mathfrak{p}$ for any prime $\mathfrak{q}$ of norm 59. There is a unique place v of F above 29. Moreover,

$$F(\chi_1/\chi_2) = F(\zeta_{29}),$$

which is abelian over $\mathbb{Q}$. Since this field is totally imaginary, complex conjugation acts nontrivially on it; hence $\chi_1/\chi_2)(c) = -1$ for every complex conjugation c. The character χ_1/χ_2 is ramified at v, so in particular $(\chi_1/\chi_2)|_{D_v} \neq 1$.

It remains to check the ordinary local condition at v. The variety A_0 has good ordinary reduction at 29: indeed

$$L(X_{0,\mathbb{F}_{29}}, T) = 1 + 45T^2 + 2187T^4 + 45 \cdot 29^2T^6 + 29^4T^8, \tag{4.3.7}$$

and the middle coefficient satisfies $2187 \equiv 12 \not\equiv 0 \pmod{29}$. Thus $\rho|_{D_v}$ is crystalline and ordinary. Let $\widetilde{\chi}_i$ denote the Teichmüller lift of χ_i. After choosing a basis compatible with the ordinary filtration, we have

$$\rho|_{D_v} \simeq \begin{pmatrix} \psi_1^{(v)}\widetilde{\chi}_1 & * \\ 0 & \psi_2^{(v)}\widetilde{\chi}_2 \end{pmatrix}. \tag{4.3.8}$$

Here $\psi_i^{(v)} \equiv 1 \pmod{\mathfrak{p}}$. Hence the image of $\psi_2^{(v)}$ lies in $1 + \mathfrak{p}\mathbb{Z}_{K_\mathfrak{p}}$, a pro-29 group. Also, the ordinary filtration identifies the upper-left character with the unit-root quotient, so $\psi_1^{(v)}|_{I_v}$ has finite image. (For further detail see Brinon–Conrad [BC09, §8.3, Proposition 8.3.4, Theorem 8.3.6].) This is precisely the local hypothesis in Skinner–Wiles, the conclusion of which is that $\rho_{A,\mathfrak{p}^\infty}$ is modular, hence $A = (A_0)_F$ is modular.

After noting that $\det\rho = \varepsilon_{29^\infty,F}$ is the 29-adic cyclotomic character restricted to F, we conclude that ρ is associated to a Hilbert modular form. This form must have parallel weight 2 (by the determinant), and its level is squarefree by semistability and must be supported within the primes of bad reduction of A_0.

This shows that the level of the form divides $\sqrt{3}\mathfrak{N}$. At level $\mathfrak{N}$ the dimension is 22 and either prime above 11 distinguishes the newforms and only f' is a match. At the remaining levels, using eigenvalues at small primes we find no match—the largest space considered is the space of newforms of level $\sqrt{3}\mathfrak{N}$, of dimension 142. □

Remark 4.3.9. It follows from Proposition 4.3.1 and Proposition 4.3.6 that the Shimura curve X' and the exhibited curve X_0 have isogenous Jacobians over F, but it unfortunately does not prove that they are isomorphic as curves.

Remark 4.3.10. The methods of Voight–Willis [VW14] give another technique for computing equations of Shimura curves (of arbitrary genus). Since we already had the period lattice, we found numerical reconstruction to be easier here; but we hope to use this technique in future work, as it would for example also provide us (numerically) the images of CM points.

In theory, it is now possible to separately compute the 2-isogeny representation of $\mathrm{Jac}(X)$ and see that it agrees with the one computed numerically from the Hilbert modular form f. With significant effort, we can also carry this out in practice.

Proposition 4.3.11. *The field $\mathbb{Q}(A_0[2])$ of 2-torsion of A_0 is the splitting field for (1.1.4).*

Proof. We consider the scheme of tritangent planes to X_0 in $\mathbb{P}^3$ (those planes that intersect the degree 6 curve X_0 in three points, each tangent, equivalently effective odd theta characteristics); it is a classical fact that the difference between two tritangent divisors yields all 2-torsion points of the Jacobian. In julia, we compute using homotopy continuation methods [BT18] numerical approximations to the nonsingular points of the tritangent scheme [Bre18]. We then refine these using Newton's method to high precision. We recover polynomials with real coefficients which vanish on these points and using continued fractions recognize their coefficients as rational numbers.

With further significant effort factoring these polynomials, we find an *exact* representation of the 120 tritangent planes over a field of degree 120. We then verify using exact methods (*a posteriori*) that these planes are indeed tritangents. We conclude that the 2-division field is equal to the splitting field of a degree 120 polynomial $g(x)$.

Finally, we show that the splitting fields of the polynomials $f(x)$ of degree 17 in (1.1.4) and $g(x)$ are isomorphic. Computing the splitting fields separately and checking for isomorphism would be far too expensive. We start with $K = \mathbb{Q}(\alpha)$ where $f(\alpha) = 0$. We compute using relative invariants for subgroups of permutaton groups (see [Els17, FK14]) the degree 3 extension $K' \supseteq K$ inside the splitting field of f; let $K' = \mathbb{Q}(\alpha')$ with $f'(x)$ the minimal polynomial of α'. We are then able to factor $g(x)$ over K' into 3 irreducible factors of degree 40; let $h(x) \in K'[x]$ be one of these factors. Then there exists $H(x, y) \in \mathbb{Q}[x, y]$ such that $H(\alpha', y) = h(y)$ with $\deg_x H(x, y) < 51$ and $\deg_y H(x, y) = 40$.

Now we make a bipartite graph Γ:

- the vertices are the roots $\{\alpha'_i\}_i$ of $f'(x)$ and $\{\beta_j\}_j$ of $g(x)$, respectively, in a splitting field; and
- there is an (undirected) edge between α'_i and β_j if and only if $H(\alpha'_i, \beta_j) = 0$.

It is immediate that $\mathrm{Gal}(f'(x)g(x))$ acts on Γ via its natural permutation action on the roots, giving an inclusion into $\mathrm{Aut}(\Gamma)$.

The graph Γ measures the relationship between the splitting fields that comes about from the factor $h(x)$. (Two extremes: if $h(x)$ were a linear factor, then the graph would be a simple

matching between the roots of $g(x)$ and a subset of roots of $f'(x)$; if at the other extreme $h(x) = g(x)$ and the factor were trivial, then the graph would be a complete bipartite graph giving no new information.)

The natural projection maps onto permutations of either subset of roots give (surjective) homomorphisms

$$p_{f'}\colon \operatorname{Aut}(\Gamma) \to \operatorname{Gal}(f'(x)) \quad \text{and} \quad p_g\colon \operatorname{Aut}(\Gamma) \to \operatorname{Gal}(g(x)). \tag{4.3.12}$$

We compute in this case, working with roots modulo a prime where both polynomials split completely, that in fact each projection $p_{f'}$ and p_g is *injective*! Therefore we have injective homomorphism $\operatorname{Gal}(f'(x)g(x)) \hookrightarrow \operatorname{Aut}(\Gamma) \xrightarrow{\sim} \operatorname{Gal}(f'(x))$ so that a splitting field of g is contained in that of f'; and vice versa, whence they are equal. □

Remark 4.3.13. There is an alternative p-adic approach to some of the above computations, as follows.

The division polynomial algorithm of Mascot [Mas20] takes as input a smooth, projective curve X of genus g with Jacobian $A := \operatorname{Jac}(X)$, a prime ℓ, and a prime $p \neq \ell$ of good reduction for X; it returns as output a rational function $\alpha \in \mathbb{Q}(A)$, a p-adic approximation of the corresponding division polynomial $F_\alpha(x) = \prod_{0 \neq P \in A[\ell]}(x - \alpha(P))$, and the matrix $[\mathrm{Frob}_p] \in \mathrm{GL}_{2g}(\mathbb{F}_\ell)$ of the Frobenius automorphism at p acting on $A[\ell]$. Running this algorithm in our case with $\ell = 2$ and $p = 5$ gives a polynomial of degree $2^8 - 1 = 255 = 17 \cdot 15$; with significant computational effort, we verify that it defines a number field that contains the field K defined in (1.1.4).

The method of Mascot can be adapted to carve out certain Galois submodules, and these ideas extend to get the degree 17 polynomial directly, as follows. We choose a prime p such that the factorization of $F_\alpha(x)$ modulo p consisting of 15 irreducible factors of degree 17. Then in some basis, $\rho(\mathrm{Frob}_p)$ has the form $\begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_{16}) \leq 17\mathrm{T}7$, where $\mathbb{F}_{16}^\times = \langle \epsilon \rangle \simeq C_{15}$. The smallest such prime is $p = 61$. Since the scalar matrix $\begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon \end{pmatrix}$ centralizes the semisimple element $\rho(\mathrm{Frob}_p)$ in $\mathrm{GL}_2(\mathbb{F}_{16})$, it can be computed explicitly as $E \in \mathbb{F}_2[\mathrm{Frob}_p]$, a polynomial in Frob_p, by linear algebra. Then from the matrix of Frob_p, we compute the orbits $\Omega_1, \ldots, \Omega_{17}$ of E on $A[2] \smallsetminus \{0\}$ and instead form

$$\prod_{i=1}^{17} \left(x - \sum_{P \in \Omega_i} \alpha(P) \right) \in \mathbb{Q}_p[x];$$

good rational approximations yield a polynomial of degree 17 in $\mathbb{Q}[x]$, which we quickly confirm yields our field K.

This does not give a rigorous result, but in principle it could be made rigorous (working with elements in $A(K)$ using their p-adic approximations, and certifying that they are ℓ-torsion).

We are grateful to Nicolas Mascot for sharing these calculations and ideas, which given the curve (!) takes only about a CPU hour!

References

[BSCM23] Adrian Barquero-Sanchez and Jimmy Calvo-Monge, *On the embedding of Galois groups into wreath products*, 2023, preprint, arXiv:2306.14386.

[BDG04] Massimo Bertolini, Henri Darmon, and Peter Green, *Periods and points attached to quadratic algebras*, Heegner points and Rankin L-series, Math. Sci. Res. Inst. Publ., **49**, Cambridge University Press, Cambridge, 2004, 323–367. 14, 17

[BR89] D. Blasius and J. Rogawski, *Galois representations for Hilbert modular forms*, Bull. Amer. Math. Soc. (N.S.) **21** (1989), vol. 1, 65–69. 9

[vB+24a] Raymond van Bommel, Edgar Costa, Noam D. Elkies, Timo Keller, Sam Schiavone, and John Voight, *17T7*, https://github.com/SamSchiavone/17T7. 18

[vB+24b] Raymond van Bommel, Edgar Costa, Noam D. Elkies, Timo Keller, Sam Schiavone, and John Voight, *EichlerShimuraHMF*, https://github.com/edgarcosta/EichlerShimuraHMF. 18

[BSSVY24] Andrew R. Booker, Jeroen Sijsling, Andrew V. Sutherland, John Voight, and Dan Yasaki, *Sato-Tate groups and automorphy for atypical abelian surfaces*, 2024, preprint. 11

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.

[Bos11] Johan Bosman, *Computations with modular forms and Galois representations*, Computational aspects of modular forms and Galois representations, Ann. of Math. Stud., vol. 176, Princeton University Press, Princeton, NJ, 2011, 129–157. 3, 10

[Bou23] Thomas Bouchet, *Invariants of genus 4 curves*, J. Algebra 660, 2024, 619–644. 22

[Bou24] Thomas Bouchet, *Covariant reconstruction of forms from their invariants*, preprint, 2024, arXiv:2403.17490. 22

[Bre18] Paul Breiding, *Tritangent planes to a genus 4 curve*, 26 November 2018, https://www.juliahomotopycontinuation.org/examples/tritangents/ (accessed 21 April 2025). 24

[BC09] Olivier Brinon and Brian Conrad, *CMI Summer School Notes on p-adic Hodge theory*, 2009, https://claymath.org/sites/default/files/brinon_conrad.pdf. 23

[BT18] Paul Breiding and Sascha Timme, *HomotopyContinuation.jl: a package for homotopy continuation in Julia*, Mathematical Software – ICMS 2018, eds. James H. Davenport, Manuel Kauers, George Labahn, and Josef Urban, 2018, Lect. Notes Comp. Sci., vol 10931, Springer, Cham, 458–465. 24

[Bro82] Kenneth S. Brown, *Cohomology of groups*, Grad. Texts in Math., vol. 87, Springer-Verlag, New York, 1982. 8

[Car86] Henri Carayol, *Sur les représentations l-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. École Norm. Sup. (4) **19** (1986), vol. 3, 409–468. 9

[CDD91] Henri Cohen and Francisco Diaz y Diaz, *A polynomial reduction algorithm*, Sém. Théor. Nombres Bordeaux (2) **3** (1991), no. 2, 351–360. 19

[CMSV19] Edgar Costa, Nicolas Mascot, Jeroen Sijsling, and John Voight, *Rigorous computation of the endomorphism ring of a Jacobian*, Math. Comp. **88** (2019), 1303–1339. 22

[Cre97] J.E. Cremona, *Algorithms for Modular Elliptic Curves*, 2nd. ed., Cambridge University Press, Cambridge, 1997. 17

[CD17] Clifton Cunningham and Lassina Dembélé, *Lifts of Hilbert modualr forms and application to modularity of abelian varieties*, preprint, 2017, arXiv:1705.03054. 11

[CR06] Charles W. Curtis and Irving Reiner, *Representation Theory of Finite Groups and Associative Algebras*, AMS Chelsea Publishing, Providence, RI, 2006. 9

[DL03] Henri Darmon and Adam Logan, *Periods of Hilbert modular forms and rational points on elliptic curves*, Int. Math. Res. Not. **2003**, no. 40, 2153–2180. 3, 14

[Dem08] Lassina Dembélé, *An algorithm for modular elliptic curves over real quadratic fields*, Experiment. Math. **17** (2008), no. 4, 427–438. 3, 14, 17

[Dem09] Lassina Dembélé, *A non-solvable Galois extension of ramified at 2 only*, Comptes Rendus. Math. **347** (2009), no. 3-4, 111–116. 3, 10

[DeV09] Lassina Dembélé and John Voight, *Explicit methods for Hilbert modular forms*, Elliptic curves, Hilbert modular forms and Galois deformations, Birkhäuser, Basel, 2013, 135–198. 3, 12, 13, 18

[DGV11] Lassina Dembélé, Matthew Greenberg, and John Voight, *Nonsolvable number fields ramified only at 3 and 5*, Compositio Math. **147** (2011), no. 3, 716–734. 3, 10, 11

[Del71] Pierre Deligne, *Travaux de Shimura*, Séminaire Bourbaki, 23ème année (1970/1971), exposé 389, Lecture Notes in Math., vol. 244, Springer, 1971, 123–165. 21

[DN67] Koji Doi and Hidehisa Naganuma, *On the algebraic curves uniformized by arithmetical automorphic functions*, Ann. Math. (2) **86** (1967), no. 3, 449–460. 21

[Dok04] Tim Dokchitser, *Computing special values of motivic L-functions*, Experiment. Math. **13** (2004), no. 2, 137–149. 18

[Dok21] Tim Dokchitser, *Inverse Galois problem: PCMI 2021 Graduate Summer School Program "Number Theory Informed by Computation"*, 2021, https://people.maths.bris.ac.uk/~matyd/InvGal/. 1

[DoV21] Steve Donnelly and John Voight, *A database of Hilbert modular forms*, Arithmetic geometry, number Theory, and computation, eds. Jennifer S. Balakrishnan, Noam Elkies, Brendan Hassett, Bjorn Poonen, Andrew V. Sutherland, and John Voight, Simons Symp., Springer, Cham, 2021, 365–373. 11

[Edi11] Bas Edixhoven, *Computing the residual Galois representations*, Computational aspects of modular forms and Galois representations, Ann. of Math. Stud., vol. 176, Princeton Univ. Press, Princeton, NJ, 2011, 371–382. 3

[EK] Noam D. Elkies and Jean Kieffer, *A uniform quasi-linear time algorithm for evaluating theta functions in any dimension*, preprint, arXiv:2505.22382. 19

[Els17] Andreas-Stephan Elsenhans, *Improved methods for the construction of relative invariants for permutation groups*, J. Symbolic Comput. **79** (2017), 211–231. 24

[FK14] Claus Fieker and Jürgen Klüners, *Computation of Galois groups of rational polynomials*, LMS J. Comput. Math. **17** (2014), no. 1, 141–158. 20, 24

[Flint] The FLINT team, *FLINT: Fast Library for Number Theory*, 2024, Version 3.1.3, https://flintlib.org. 19

[G88] Gerard van der Geer, *Hilbert Modular Surfaces*, Ergeb. Math. Grenzgeb. (3), vol. 16, Springer-Verlag, Berlin, 1988. 17

[GP17] Jose Ignacio Burgos Gil and Ariel Pacetti, *Hecke and Sturm bounds for Hilbert modular forms over real quadratic fields*, Math. Comp. **86** (2017), no. 306, 1949–1978. 11

[Gor02] Eyal Z. Goren, *Lectures on Hilbert Modular Varieties and Modular Forms*, CRM Monogr. Ser., vol. 14, Amer. Math. Soc., Providence, RI, 2002. 16

[Gra96] Louis Granboulan, *Construction d'une extension régulière de* $\mathbf{Q}(T)$ *de groupe de Galois* M_{24}, Experiment. Math. **5** (1996), no. 1, 3–14. 1

[GV11] Matthew Greenberg and John Voight, *Computing systems of Hecke eigenvalues associated to Hilbert modular forms*, Math. Comp. **80** (2011), no. 274, 1071–1092. 13

[HPS24] Jeroen Hanselman, Andreas Pieper, and Sam Schiavone, *Equations of genus 4 curves from their theta constants*, preprint, 2024, arXiv:2402.03160. 22

[Igu64] Jun-ichi Igusa, *On Siegel modular forms of genus two. II*, Amer. J. Math. **86** (1964), 392–412. 18

[JLY02] Christian U. Jensen, Arne Ledet, and Noriko Yui, *Generic polynomials: Constructive aspects of the inverse Galois problem*, Math. Sci. Res. Inst. Publ., vol. 45, Cambridge University Press, Cambridge, 2002. 1

[JR07] John W. Jones and David P. Roberts. *Galois number fields with small root discriminant*, Journal of Number Theory **122** (2007), no. 2, 379-407. 10

[Kin05] Oliver H. King, *The subgroup structure of finite classical groups in terms of geometric configurations*, Surveys in combinatorics 2005, London Math. Soc. Lecture Note Ser., vol. 327, Cambridge Univ. Press, Cambridge, 2005, 29–56. 6

[KM01] Jürgen Klüners and Gunter Malle, *A database for field extensions of the rationals*, LMS J. Comput. Math. **4** (2001), 182–196. 1

[KM24] Jürgen Klüners and Gunter Malle, *Missing polynomials (group)*, 2024, http://galoisdb.math.upb.de/statistics/missing_polynomials/group. 1

[LMFDB] The LMFDB Collaboration, *The L-functions and modular forms database*, https://www.lmfdb.org, accessed 2 April 2024. 11

[MM99] Gunter Malle and B. Heinrich Matzat, *Inverse Galois Theory*, Springer Monogr. Math., Springer-Verlag, Berlin, 1999. 1

[Mas18] Nicolas Mascot, *Certification of modular Galois representations*, Math. Comp. **87** (2018), no. 309, 381–423. 3

[Mas20] Nicolas Mascot, *Hensel-lifting torsion points on Jacobians and Galois representations*, Math. Comp. **89** (2020), no. 323, 1417–1455. 25

[Oda82] Takayuki Oda, *Periods of Hilbert modular surfaces*, Progr. Math., vol. 19 Birkhäuser, Boston, MA, 1982. 3, 14, 15, 16, 18

[Oda90] Takayuki Oda, *The Riemann-Hodge period relation for Hilbert modular forms of weight 2*. Cohomology of arithmetic groups and automorphic forms (Luminy-Marseille, 1989), Lecture Notes in Math., vol. 1447, Springer-Verlag, Berlin, 1990, 261–286. 14, 15

[Pari] The PARI Group, PARI/GP version `2.15.4`, Univ. Bordeaux, 2023, `http://pari.math.u-bordeaux.fr/`. 19

[Ric22] James Rickards, *Improved computation of fundamental domains for arithmetic Fuchsian groups*, Math. Comp. **91** (2022), no. 338, 2929–2954. 21

[Rot95] Joseph J. Rotman, *An introduction to the theory of groups*, 4th ed., Grad. Texts in Math., vol. 148, Springer-Verlag, New York, 1995. 8

[Ser08] Jean-Pierre Serre, *Topics in Galois theory*, 2nd. ed., with notes by Henri Darmon, Res. Notes Math., vol. 1, A K Peters, Ltd., Wellesley, MA, 2008. 1

[Shi67] Goro Shimura, *Construction of class fields and zeta functions of algebraic curves*, Ann. Math. (2), **85** (1967), no. 1, 58–159. 21

[SV16] Jeroen Sijsling and John Voight, *On explicit descent of marked curves and maps*, Res. Number Theory **2**:27 (2016), 35 pages. 21

[SW98] C.M. Skinner and Andrew J. Wiles, *Residually reducible representations and modular forms*, Inst. Hautes Études Sci. Publ. Math., no. 89, 1999, 5–126. 23

[Sta73] Richard P. Stauduhar, *The determination of Galois groups*, Math. Comput. **27** (1973), 981–996. 20

[Tay89] Richard Taylor, *On Galois representations associated to Hilbert modular forms*, Invent. Math. **98** (1989), vol. 2, 265–280. 9

[Voi09] John Voight, *Computing fundamental domains for Fuchsian groups*, J. Théorie Nombres Bordeaux **21** (2009), no. 2, 467–489. 21

[Voi21] John Voight, *Quaternion algebras*, Grad. Texts in Math., vol. 288, Springer, Cham, 2021. 12, 14, 20, 21

[VW14] John Voight and John Willis, *Computing power series expansions of modular forms*, Computations with modular forms, Contrib. Math. Comput. Sci., vol. 6, Springer, Cham, 2014, 331–361. 13, 24

[Z01] Shouwu Zhang, *Heights of Heegner points on Shimura curves*, Ann. of Math. (2) **153** (2001), no. 1, 27–147. 13

[Zyw23] David Zywina, *Modular forms and some cases of the inverse Galois problem*, Canad. Math. Bull. **66** (2023), no. 2, 568–586. 3

Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Ave., Bldg. 2-336 Cambridge, MA 02139, USA; School of Mathematics, University of Bristol, Fry Building, Woodland Road, Bristol, BS8 1UG, United Kingdom
Email address: r.vanbommel@bristol.ac.uk
URL: https://raymondvanbommel.nl/

Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Ave., Bldg. 2-336 Cambridge, MA 02139, USA
Email address: edgarc@mit.edu
URL: https://edgarcosta.org

Department of Mathematics, Harvard University, Cambridge, MA 02138, USA
Email address: elkies@math.harvard.edu
URL: https://people.math.harvard.edu/~elkies/

Institut für Mathematik, Universität Würzburg, Emil-Fischer-Strasse 30, 97074, Würzburg, Germany; Rijksuniveriteit Groningen, Bernoulli Institute, Bernoulliborg, Nijenborgh 9, 9747 AG Groningen, The Netherlands; Leibniz Universität Hannover, Institut für Algebra, Zahlentheorie und Diskrete Mathematik, Welfengarten 1, 30167 Hannover, Germany
Email address: math@kellertimo.de
URL: https://www.timo-keller.de

Massachusetts Institute of Technology, Department of Mathematics, 77 Massachusetts Ave., Bldg. 2-336 Cambridge, MA 02139, USA
Email address: sam.schiavone@gmail.com
URL: https://math.mit.edu/~sschiavo/

Dartmouth College, Department of Mathematics, 6188 Kemeny Hall, Hanover, NH 03755-3551, USA; Department of Mathematics and Statistics, Carslaw Building (F07), University of Sydney, NSW 2006, Australia
Email address: jvoight@gmail.com
URL: https://jvoight.github.io