17T7 IS A GALOIS GROUP OVER THE RATIONALS

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

Abstract. 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. 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 fourfolds using Hilbert modular forms. Finally, building upon work of Dembélé, we show how to conjecturally reconstruct a period matrix for an abelian variety attached to a Hilbert modular form; we then use this to exhibit an explicit degree 17 polynomial with Galois group 17T7.

1. Introduction

1.1. **Motivation and first result.** The Inverse Galois Problem (IGP) [Ser08, MM99, JLY02], which asks if every finite group (up to isomorphism) occurs as a Galois group over $\mathbb{Q}$, remains of enduring fascination. 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 $f(x) \in \mathbb{Q}[x]$ 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].

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.

Our first main result is as follows.

Date: November 13, 2024.

2020 *Mathematics Subject Classification.* 12F12 (Primary) 11F80, 11F41, 14G10.

Key words and phrases. inverse Galois theory, Galois representations, Hilbert modular forms, Shimura curves.

Theorem 1.1.2. *The group* $G = \mathsf{17T7}$ *is a Galois group over* $\mathbb{Q}$. *More precisely, the polynomial*

$$\begin{aligned} x^{17} - 2x^{16} + 12x^{15} - 28x^{14} + 60x^{13} - 160x^{12} + 200x^{11} - 500x^{10} + 705x^9 - 886x^8 \\ + 2024x^7 - 604x^6 + 2146x^5 + 80x^4 - 1376x^3 - 496x^2 - 1013x - 490 \in \mathbb{Q}[x] \end{aligned} \tag{1.1.3}$$

has Galois group G.

Verification that the polynomial in (1.1.3) indeed has Galois group G is a quick calculation in Magma [BCP97] using the method of relative invariants due to Stauduhar [Sta73] as described and implemented by Fieker–Klüners [FK14]. What remains interesting, then, is the method by which such a polynomial can be exhibited.

1.2. **Further motivation and second result.** The (effective) IGP welcomes input from all branches of mathematics; our approach uses methods from arithmetic geometry, more specifically from abelian varieties and modular forms. For example, 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; and 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 $\mathbb{Q}$ 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]. However, in general the Galois groups over $\mathbb{Q}$ obtained from the normal closure yield wreath products.

We record an explicit criterion (Theorem 2.4.2) that 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 2.4.7. We then use this to solve the IGP for many groups G like $\mathsf{17T7}$ that are split extensions of finite cyclic groups by $\mathrm{PGL}_2(\mathbb{F}_q)$ by exhibiting certain Hilbert modular forms over abelian totally real fields F.

Our final, bold 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).

Our final contribution 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 (including those with varying signature).
2. Construct the moduli point $\tau \in (\mathbb{C} \smallsetminus \mathbb{R})^g$ corresponding to A 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. Several new features arise in this generalization, as is perhaps clear from this description. In this way, we solve the effective IGP for 17T7: the calculation is explained in detail in section 4.

Finally, when the period matrix lies in the Schottky locus, we could then also seek to reconstruct the abelian variety as a Jacobian of a curve, and use this to certify the construction. In fact, we are lucky in one of our examples, and succeed with this: see (4.3.3).

1.3. **Structure of the article.** In §2, we dive into our descent approach to the IGP. We then exhibit our general numerical 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 1.1.2.

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). 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 4.3.6. Finally, we thank Sachi Hashimoto, Adam Logan, and many other participants of the PCMI 2022 program who contributed to the early stages of the project.

Van Bommel, Costa, and Schiavone were supported by a Simons Collaboration grant (550033). Elkies was supported by a Simons Collaboration grant (550031). Keller was supported by the 2021 MSCA Postdoctoral Fellowship 01064790 – ExplicitRatPoints. Voight was supported by a Simons Collaboration grant (550029).

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 2.4.2.

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. The first equivalence follows by a direct calculation when $\#k \leq 3$, and for $\#k \geq 4$ since then $\mathrm{SL}_2(k)$ has no subgroup of index 2 (it is equal to its commutator subgroup). 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 $\mathrm{Gal}(k \,|\, \mathbb{F}_\ell)$ 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

$$\mathrm{SL}_2(\mathbb{F}_{16}) \rtimes \mathrm{Gal}(\mathbb{F}_{16} \,|\, \mathbb{F}_4) \leq \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes \mathrm{Gal}(\mathbb{F}_{16} \,|\, \mathbb{F}_2) =: \Sigma\mathrm{L}(F_{16})$$

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 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 $\#k \geq 4$. Then G contains $\mathrm{SL}_2(k)$ if and only if G contains:*

(i) *a split semisimple element (its characteristic polynomial splits into distinct linear factors in k);*
(ii) *a nonsplit semisimple element (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 $\mathrm{P}G \geq \mathrm{PSL}_2(k)$. 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. We rule out subgroups of affine and dihedral groups by (i) and (ii); we rule out exceptional groups by (iii) as there are no exceptional groups when $\#k = 4$ and only A_4 when $\#k = 5$. It follows that G is projective: up to conjugacy, we have $\mathrm{P}G = \mathrm{PSL}_2(k_0)$ or $\mathrm{P}G = \mathrm{PGL}_2(k_0)$ for some subfield $k_0 \subseteq k$. 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 $\mathrm{tr}\, G = k$.*

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

(i) Let $\lambda \in k^\times \smallsetminus \{\pm 1\}$. Then by hypothesis there exists $g \in G$ such that $\mathrm{tr}(g) = \lambda + \lambda^{-1}$, 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 $a \in k$ such that $x^2 - ax + 1 \in k[x]$ is irreducible, since the map $k^\times \smallsetminus \{\pm 1\} \to k$ 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 $\mathrm{tr}(g) = a$ is therefore nonsplit semisimple.
(iii) An element g of projective order ≤ 5 has $\mathrm{tr}\, g = a \in \{\pm 2, \pm 1, 0\}$ 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 $\mathrm{tr}\, g = a$ will suffice, since then $u(g) = (\mathrm{tr}\, g)^2 = a^2$.

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

Remark 2.2.3. For completeness we consider the missing cases in the previous two propositions.

For Proposition 2.2.1, by a direct calculation we find that $G \le \mathrm{GL}_2(\mathbb{F}_\ell)$ contains $\mathrm{SL}_2(\mathbb{F}_\ell)$ for $\ell = 2, 3$ if and only if G has a nonsplit semisimple element and an element of (projective) order ℓ.

Proposition 2.2.2 is false for $\#k = 2, 3, 5$ by the counterexamples $C_3 \le \mathrm{SL}_2(\mathbb{F}_2)$, $Q_8 \le \mathrm{SL}_2(\mathbb{F}_3)$, 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 $\mathrm{Gal}_F := \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}} \,|\, F)$. Let k be a finite field and let

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

be a semisimple Galois representation. Then $\ker\rho$ cuts out a Galois extension $L := F(\rho) \supseteq F$ with Galois group $\mathrm{Gal}(L \,|\, F) = G := \operatorname{img}\rho \le \mathrm{GL}_n(k)$. 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.

Of course, 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 $\mathrm{Gal}(F \,|\, F_0)$, defined as follows. Let $\sigma \in \mathrm{Gal}(F \,|\, F_0)$. 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. Let $L^\sigma := \ker\rho^\sigma$.

Let N be the compositum of all L^σ for $\sigma \in \mathrm{Gal}(F \,|\, F_0)$. We define the wreath product

$$\mathrm{Gal}(L \,|\, F) \wr \mathrm{Gal}(F \,|\, F_0) := \left(\prod_{\sigma \in \mathrm{Gal}(F \,|\, F_0)} \mathrm{Gal}(L^\sigma \,|\, F) \right) \rtimes \mathrm{Gal}(F \,|\, F_0) \tag{2.3.5}$$

where $\mathrm{Gal}(F \,|\, F_0)$ acts on the product by permuting factors. By the Kaloujnine–Krasner universal embedding problem (see e.g. [BSCM23, Theorem 1.1]), we have an embedding

$$\mathrm{Gal}(N \,|\, F) \hookrightarrow \mathrm{Gal}(L \,|\, F) \wr \mathrm{Gal}(F \,|\, F_0). \tag{2.3.6}$$

Proposition 2.3.7 (Galois descent law)**.** *Suppose that there exists an injective group homomorphism*

$$\begin{aligned} \tau\colon \mathrm{Gal}(F \,|\, F_0) &\hookrightarrow \mathrm{Aut}(k) \\ \sigma &\mapsto \tau_\sigma \end{aligned} \tag{2.3.8}$$

such that there exists an isomorphism $\rho^\sigma \simeq \tau_\sigma(\rho)$ *of representations for all* $\sigma \in \mathrm{Gal}(F \,|\, F_0)$. *Then the extension* $L = F(\rho) \supseteq F_0$ *is Galois with* $\mathrm{Gal}(L \,|\, F_0) \simeq G \rtimes \mathrm{Gal}(F \,|\, F_0)$, *where* $\mathrm{Gal}(F \,|\, F_0)$ *acts on* $G \leq \mathrm{GL}_n(k)$ *entrywise via the map* τ.

Proof. For all $\sigma \in \mathrm{Gal}(F \,|\, F_0)$, 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. Thus in the embedding (2.3.6), the image maps to the subgroup of the wreath product isomorphic to $\mathrm{Gal}(L \,|\, F) \rtimes \mathrm{Gal}(F \,|\, F_0)$ via τ, which is therefore an isomorphism because τ is injective. ☐

Remark 2.3.9. The converse of Proposition 2.3.7 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.

Corollary 2.3.10. *The extension* $L \supseteq F_0$ *is Galois if*

$$\det(1 - \rho(\mathrm{Frob}_{\sigma(\mathfrak{p})})T) = \det(1 - \tau_\sigma(\rho)(\mathrm{Frob}_{\mathfrak{p}})T) \in k[T] \tag{2.3.11}$$

for all primes $\mathfrak{p} \notin S(\rho)$.

Proof. Recalling that ρ is assumed to be semisimple, combine Proposition 2.3.7 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 (Proposition 2.3.7) 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 $i = 1, \ldots, n$ and Nebentypus character χ. Let $k_0 := \max(k_1, \ldots, k_n)$. 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 a semisimple Galois representation*

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

such that

$$\mathrm{tr}(\rho_{f,\mathfrak{l}}(\mathrm{Frob}_{\mathfrak{p}})) \equiv a_{\mathfrak{p}}(f) \pmod{\mathfrak{l}}$$
$$\det(\rho_{f,\mathfrak{l}}(\mathrm{Frob}_{\mathfrak{p}})) \equiv \chi(\mathfrak{p})\, \mathrm{Nm}(\mathfrak{p})^{k_0-1} \pmod{\mathfrak{l}}$$

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]. ☐

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 would be the decomposition and inertia groups).

Theorem 2.4.2. *Suppose there is an injective group homomorphism*

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

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

$$\begin{aligned} \tau_\sigma(a_{\mathfrak{p}}(f)) &\equiv a_{\sigma(\mathfrak{p})}(f) \pmod{\mathfrak{l}} \\ \tau_\sigma(\chi(\mathfrak{p})) &\equiv \chi(\sigma(\mathfrak{p})) \pmod{\mathfrak{l}}. \end{aligned} \tag{2.4.3}$$

Then the field $L = F(\rho_{f,\mathfrak{l}})$ *is Galois over* $\mathbb{Q}$*, and there is an injective group homomorphism*

$$\mathrm{Gal}(L\,|\,\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{F}_{\mathfrak{l}}) \rtimes \mathrm{Aut}(\mathbb{F}_{\mathfrak{l}}) \tag{2.4.4}$$

where $\mathrm{Aut}(\mathbb{F}_{\mathfrak{l}})$ *acts on* $\mathrm{GL}_2(\mathbb{F}_{\mathfrak{l}})$ *coefficientwise; the image is isomorphic to* $G \rtimes \mathrm{Gal}(F\,|\,\mathbb{Q})$*, where* $G = \operatorname{img}\rho_{f,\mathfrak{l}}$ *and* $\mathrm{Gal}(F\,|\,\mathbb{Q})$ *is considered as a subgroup of* $\mathrm{Gal}(\mathbb{F}_{\mathfrak{l}}\,|\,\mathbb{F}_\ell)$ *via* τ*.*

Proof. We apply the form of the Galois descent law (Proposition 2.3.7) given in Corollary 2.3.10. ☐

Remark 2.4.5. Since the group $D_{\mathfrak{l}}/I_{\mathfrak{l}} \hookrightarrow \mathrm{Gal}(\mathbb{F}_{\mathfrak{l}}\,|\,\mathbb{F}_\ell)$ is cyclic, Theorem 2.4.2 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 2.4.6. *Under the hypotheses of Theorem 2.4.2, 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* $\mathrm{P}G \rtimes \mathrm{Gal}(F\,|\,\mathbb{Q})$*.*

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

Remark 2.4.7. In work of Dembélé [Dem09] and Dembéle–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 together from the previous subsections 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) satisfying the descent condition (2.4.3).

We first focus on the proof of the (ineffective) version of Theorem 1.1.2, realizing 17T7, given as in Example 2.1.7. Looking at (2.4.4):

- We need a base field F such that $\mathrm{Gal}(F\,|\,\mathbb{Q}) = \langle\sigma\rangle \simeq C_2$, so we take F a real quadratic field.
- We need the image of the determinant to be trivial, so we take trivial Nebentypus character χ.
- The prime $\mathfrak{l}$ has 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 f would make it even harder to compute an explicit polynomial.)

- We must check that (2.4.3) holds; in our case this conidition reads

$$a_{\sigma(\mathfrak{p})}(f) \equiv a_{\mathfrak{p}}(f)^4 \pmod{2}.$$

- Finally, the eigenvalues $a_{\mathfrak{p}}(f)$ modulo 2 should hit every element of $\mathbb{F}_{16}$.

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 $\mathfrak{N}$.

To prove the congruence modulo 2, in principle this can be done with a finite computation using Hecke–Sturm bounds [GP17]; however, the relevant bound here will be quite large. When the congruence lifts to an equality $\tau(f) = f^\sigma$ of eigenforms, with $\tau \in \mathrm{Gal}(K_f \,|\, F)$ the nontrivial involution and $\sigma \in \mathrm{Gal}(F \,|\, \mathbb{Q})$ the nontrivial element, this can be done almost instantly from the list of eigenforms by using just the first few Hecke eigenvalues. In general, we can show this by 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]): if the Hilbert modular form f corresponds to the Jacquet–Langlands transfer $g \in S_2(\mathcal{O}, \mathbb{Z}_{K_f})$ (i.e., a map $\mathrm{Cls}\,\mathcal{O} \to \mathbb{Z}_{K_f}$ up to scalar, where $\mathrm{Cls}\,\mathcal{O}$ is the class set of the order $\mathcal{O}$ [Voi21, Chapter 17]), then we confirm that

$$\tau(g) \equiv g^\sigma \not\equiv 0 \pmod{2\mathbb{Z}_{K_f}}$$

whence $\tau(a_{\mathfrak{p}}(g)) - a_{\sigma(\mathfrak{p})}(g) \in 2\mathbb{Z}_{K_f}$ for all good primes $\mathfrak{p}$, as desired.

Remark 2.5.1. Since τ is nontrivial, we cannot have f arising as a base change from $\mathbb{Q}$.

We cannot manufacture such forms from twisted base change. Suppose the form comes from twisted base change, say $f = f_0 \otimes \psi$ with f_0 from $\mathbb{Q}$ 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 a first run, 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; but we still implemented the more general check (using the definite method).

Field	Field label	Forms
$\mathbb{Q}(\sqrt{12})$	2.2.12.1	578.1-c, 578.1-d
$\mathbb{Q}(\sqrt{12})$	2.2.12.1	722.1-i, 722.1-j, 722.1-k, 722.1-l
$\mathbb{Q}(\sqrt{8})$	2.2.8.1	2601.1-j, 2601.1-k
$\mathbb{Q}(\sqrt{8})$	2.2.8.1	2738.1-e, 2738.1-f
$\mathbb{Q}(\sqrt{12})$	2.2.12.1	1587.1-i, 1587.1-l, 1587.1-m, 1587.1-n
$\mathbb{Q}(\sqrt{24})$	2.2.24.1	726.1-i, 726.1-j, 726.1-k, 726.1-l

Theorem 2.5.2. *The group* $G = \mathsf{17T7}$ *is a Galois group over* $\mathbb{Q}$.

Proof. Applying Proposition 2.2.2 and Theorem 2.4.2 to the Hilbert modular forms above, we find at least 6 different number fields. ☐

Remark 2.5.3. 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 $f^\sigma \neq \tau(f)$.

3. (Re)constructive approach

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, in particular those in Theorem 2.5.2 realizing $\mathsf{17T7}$. 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 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 reference, 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], and Bertolini–Darmon–Green [BDG04, §7], and others, which was made effective for elliptic curves over real quadratic fields by Dembélé [Dem08].

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 $\widehat{\mathbb{Z}}_F := \prod_{\mathfrak{p}} \mathbb{Z}_{F,\mathfrak{p}} \subset \widehat{F}$ 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 $\mathcal{H}^{\pm} := (\mathbb{C} \smallsetminus \mathbb{R})^n$, and let

$$Y(\widehat{\Gamma}) := \mathrm{GL}_2(F)\backslash \mathrm{GL}_2(\widehat{F}) \times \mathcal{H}^{\pm}/\widehat{\Gamma} \tag{3.3.2}$$

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

$$Y(\widehat{\Gamma}) = \bigsqcup_{[\mathfrak{b}]} \Gamma_{\mathfrak{b}}\backslash\mathcal{H} \tag{3.3.3}$$

where $\mathcal{H} \subseteq \mathcal{H}^{\pm}$ 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 $\mathcal{H}$ [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 ith 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 $z = (z_1, \dots, z_n) \in \mathcal{H}^{\pm}$, and extend to $s \in W_\infty$. Then the action of W_∞ descends to $Y(\widehat{\Gamma})$ and then to extends $X(\widehat{\Gamma})$ [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 be 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_f such that $\dim_{K_f} V_f = 2^n$, for example containing

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

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

Theorem 3.3.7. *The K_f-vector space V_f can be equipped with a polarized K_f-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 $0 \neq p \le n$,

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

where we take $s \in W_\infty$ 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 $j = 1,\ldots,g$. We map

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

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

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

where we abbreviate $+ = (+1,\ldots,+1)$. In similar fashion we define,

$$z_{f,s} := \left(\frac{\Omega_1^s}{\Omega_1^+},\ldots,\frac{\Omega_g^s}{\Omega_g^+}\right) \in \mathcal{H}. \tag{3.3.12}$$

Conjecture 3.3.13 ([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

$$\Lambda_s(\mathfrak{a},\mathfrak{b}) = \mathfrak{a}\begin{pmatrix} \Omega_1^s \\ \vdots \\ \Omega_g^s \end{pmatrix} \oplus \mathfrak{b}\begin{pmatrix} \Omega_1^+ \\ \vdots \\ \Omega_g^+ \end{pmatrix} \tag{3.3.14}$$

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

$$\begin{aligned} E_c \colon (\mathfrak{a} \oplus \mathfrak{b}) \times (\mathfrak{a} \oplus \mathfrak{b}) &\to \mathbb{Q} \\ (a_1, b_1), (a_2, b_2) &\mapsto \mathrm{Tr}_{H|\mathbb{Q}}(c(a_1 b_2 - a_2 b_1)). \end{aligned} \tag{3.3.15}$$

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 want

$$c\mathfrak{a}\mathfrak{b} = \mathbb{Z}_{K_f}^{\sharp}, \tag{3.3.16}$$

where $\mathbb{Z}_{K_f}^{\sharp} := \{a \in K_f : \mathrm{Tr}_{H|\mathbb{Q}}(a\mathbb{Z}_{K_f}) \subseteq \mathbb{Z}\}$ is the trace dual (the codifferent) of $\mathbb{Z}_{K_f}$. When $\mathrm{Cl}^+(\mathbb{Z}_{K_f})$ is trivial, we take just $\Lambda_s(\mathbb{Z}_{K_f}, \mathbb{Z}_{K_f})$ with c a totally positive generator of the codifferent.

3.4. **Periods and L-values.** From now on, to simplify notation we abbreviate $K = K_f$. Recall that each embedding τ_j gives rise to an L-function

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

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 Dirichlet restriction

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

and sign

$$\chi_\infty \colon \{\pm 1\}^n \to \{\pm 1\}, \tag{3.4.3}$$

satisfying the compatibility

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

for all $a \in \mathbb{Z}_F$ coprime to $\mathfrak{c}$, where $\mathrm{sgn} \colon F^\times \to \{\pm 1\}^n$ are 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, Thm. 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 $j = 1, \ldots, g$*

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

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. **ℓ-isogeny polynomial.** From the lattice $\Lambda_s(\mathbb{Z}_K, \mathbb{Z}_K)$ with the pairing E_c (3.3.15), we construct a big period matrix $\Pi_s \in \mathrm{M}_{g,2g}(\mathbb{C})$ by choosing a symplectic $\mathbb{Z}$-basis of the lattice. We then make a small period matrix $Z \in \mathfrak{H}_g(\mathbb{C})$ (so $Z \in \mathrm{M}_g(\mathbb{C})_{\mathrm{sym}}$ is a $g \times g$ symmetric matrix with totally positive imaginary part) by writing $\Pi_s \sim (Z\ 1)$. We now compute a polynomial generating the ℓ-isogeny field of the corresponding abelian variety by forming suitable polynomials in the theta constants (with characteristic) evaluated at Π_s.

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

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

Given a principally polarized abelian varietry A of dimension g over $\mathbb{C}$ with small period matrix $Z \in \mathfrak{H}_g$, the theta constants of A are the $2^{g-1}(2^g+1)$ numbers $\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](0, Z)$ with a, b ranging over all even characteristics, i.e., pairs of representatives of $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ satisfying $4a^t b \equiv 0 \pmod 2$. One can express the Siegel Eisenstein series of weight 4 as the sum of the eighth powers of the theta constants Igusa [Igu64, p. 405]

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

Even though $E_4(Z)$ is likely to be transcendental, the ratio $\dfrac{E_4(Z')}{E_4(Z)}$ is algebraic if Z' is the period matrix of an abelian variety isogenous to A. (All we use about the Siegel E_4 is that its restriction to $\mathfrak{H}_g(\mathbb{C})$ is a Hilbert modular form that we can compute quickly to high precision.) We consider a set of such algebraic numbers forming a Galois orbit, as follows.

Let $\mathfrak{l} \subseteq \mathbb{Z}_K$ be a (nonzero) prime ideal; for simplicity suppose that $\mathfrak{l} = \ell\mathbb{Z}_K$ is narrowly principal, with $\ell \in \mathbb{Z}_K$ totally positive. We enumerate the $\mathrm{Nm}(\mathfrak{l}) + 1$ possible abelian varieties A' arising from an isogeny $A \to A'$ with kernel $\mathfrak{l}$—this is the Hecke orbit on the Hilbert modular variety. More precisely, we decompose the double coset

$$\mathrm{GL}_2(\mathbb{Z}_K) \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} \mathrm{GL}_2(\mathbb{Z}_K) = \bigsqcup_{i=1}^{\mathrm{Nm}(\mathfrak{l})+1} \mathrm{GL}_2(\mathbb{Z}_K)\alpha_i \tag{3.5.3}$$

into left cosets. With the identification above, we have $\iota_{\mathbb{Z}_K,\mathbb{Z}_K} = \iota\colon \mathrm{GL}_2(K) \hookrightarrow \mathrm{Sp}_{2g}(\mathbb{Q})$ and therefore take

$$(Z\ 1)\iota(\alpha_i)^T \sim (Z'_i\ 1). \tag{3.5.4}$$

The resulting set of $\mathrm{Nm}(\mathfrak{l})+1$ algebraic numbers

$$\left\{d(Z')\cdot\frac{E_4(Z')}{E_4(Z)}\right\}_{Z'} \tag{3.5.5}$$

is closed under Gal_F, where

$$d(Z') := \mathrm{Nm}(\mathfrak{l})^4\cdot j(\iota(\alpha_i),Z)^{-4} \tag{3.5.6}$$

(the Eisenstein series is weight 4) and $j(\alpha,Z)=\det(CZ+D)$ if $\alpha=\begin{pmatrix} * & * \\ C & D\end{pmatrix}$.

For each s, we form the polynomial associated to $\Lambda_s(\mathbb{Z}_K,\mathbb{Z}_K)$ (and $\mathfrak{l}$)

$$T_s(x)=\prod_{Z'}\left(x-d(Z')\frac{E_4(Z')}{E_4(Z)}\right)\in\mathbb{C}[x]. \tag{3.5.7}$$

According to Conjecture 3.3.13, there exists a polynomial $T(x)\in F[x]$ such that $T_{s_i}(x)=\sigma_i(T)(x)$ for all $i=1,\dots,n$.

Using the LLL lattice reduction algorithm, we can recognize the coefficients of these polynomials putatively as elements of F (or using all of the conjugates recognize their minimal polynomials with rational coefficients using continued fractions). In §4 below, we show how to do this in practice for our main example.

4. The inverse Galois problem for 17T7

In this section, we explain in detail the calculation that gives the 17T7 polynomial in Theorem 2.4.2. The code used to perform these computations is available at [vBCEKSV24a] and [vBCEKSV24b].

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 $H:=\mathbb{Q}(\nu)$ 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 2.2.12.1-578.1-d, which is the quadratic twist of 2.2.12.1-578.1-c by the nontrivial character of the narrow class group.

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 compute twisted periods as described in §3.4, using Hecke characters χ with conductors up to 25. 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

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

as in Equation (3.3.12). Note that z_{+-} and z_{-+} are, up to precision, related by the double transposition $(1\ 2)(3\ 4)$. This is because we actually have the equality $a_{\mathfrak{p}}(f^\sigma) = a_{\sigma(\mathfrak{p})}(f)$, rather than just a congruence mod 2. Thus the corresponding abelian varieties are isomorphic, whence it suffices to simply consider the first moduli point $z := z_{+-}$.

We compute that the different ideal $\mathfrak{D}_K$ of H 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 Equation (3.3.14) is principally polarisable, see §3.3. In practice, we can compute associated small period matrices as follows. We note that Λ is equipped with the pairing

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

as in Equation (3.3.15).

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. Thus we search over all $2^g + 1 = 17$ abelian varieties that are 2-isogenous to A/Λ and have RM by $\mathbb{Z}_K$, which amounts to considering

$$z' \in \left\{ \frac{z+b}{2} : b \in R \right\} \cup \{2z\}, \tag{4.1.2}$$

where $R \subseteq \mathbb{Z}_K$ is a set of representatives for $\mathbb{Z}_K/(2)$.

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. Rather than attempting to recognize the 2-isogeny polynomials of each of these abelian varieties, we can simply compute the value of the Schottky modular form evaluated at the small period matrix. We find a unique z' as in (4.1.2) such that the value of the Schottky modular form at the period matrix corresponding to z' 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

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

We note that number of correct digits appears to decrease as we consider later coefficients: the imaginary part of the coefficient of x^{16} is $< 10^{-58}$, while that of the constant term is only $< 10^{-3}$.

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 as follows. Consider the function

$$\begin{aligned}\varphi\colon \mathfrak{h}^4 &\to \mathbb{C}^4\\ w &\mapsto (b_1, b_2, b_3, b_4)\,,\end{aligned}$$

where $b_1, \ldots, b_4$ are the first four coefficients (not including the monic leading term) of the rescaled 2-isogeny polynomial T_D associated to w. Then Newton's method can numerically solve the equation $\varphi(w) = (a_1, \ldots, a_4)$ using $w = z'$ as our initial approximation. We compute numerical approximations to the Jacobian matrix $J(\varphi)$ of φ as

$$(J(\varphi)(w))_{ij} \approx \left(\frac{\varphi(w+\epsilon_i) - \varphi(w)}{\varepsilon}\right)_j\,,$$

where ϵ_i is the element of $\mathbb{C}^4$ with ε a small number in the i^{th} entry and zeroes elsewhere. It only takes four iterations of Newton's method to obtain an improved approximation of z whose corresponding 2-isogeny polynomial T has coefficients that are easily recognized as integers:

$$\begin{aligned}T(x) = x^{17} - 155176125916688x^{16} - 390377512345632733712637274 4x^{15} - \ldots\\ - \underbrace{153702846916677613155795943357742165422510948 26\ldots 14304}_{204 \text{ digits}} \qquad (4.2.1)\end{aligned}$$

Applying the PARI/GP [Pari] command `polredabs` [CDD91], we find the simplified polynomial

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

defining 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 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 2.4.2 can be found by taking the splitting field of T over F, and then taking its normal closure over $\mathbb{Q}$.

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

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 $\mathfrak{p}$ 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 $F_{\mathfrak{p}_2}$ and ϖ_{17} supported at F_{17} and whose reduced norms are uniformizers (so $\operatorname{nrd}(\varpi_2) = 1+\sqrt{3}$ and $\operatorname{nrd}(\varpi_{17}) = 17$). 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 $\operatorname{Cl}^+ \mathbb{Z}_F$ 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 $\mathcal{O}_{>0}^\times$ 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 $\mathrm{P}\mathcal{O}_{>0}^\times = \mathcal{O}_{>0}^\times/\mathbb{Z}_F^\times$ is a discrete group acting properly on the upper half-plane $\mathcal{H}$, and the quotient $X^+(\mathfrak{p};17) := \mathrm{P}\iota_\infty(\mathcal{O}_{>0}^\times)\backslash\mathcal{H}$ 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 $X^+(\mathfrak{p};17)/\langle w_{17}\rangle$ has genus 4 (signature $(4;2^9,3,12;0)$,where "2^9" means 9 elliptic points of order 2).

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

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

$$B_{>0}^\times \,\backslash\, (\widehat{B}^\times \times \mathcal{H}) \,/\, \widehat{\mathcal{O}}^\times$$

has two components, indexed by $\operatorname{Cl}^+ \mathbb{Z}_F$ [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 full set of Hilbert modular forms of level $\mathfrak{N}$ which are new at $\mathfrak{p}$ consists precisely of those newforms of level norm 578 (as there are no forms at level $\mathfrak{p}$) and has total dimension $1+1+4+4+6+6 = 22 = 2\cdot 11$. 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 and its quadratic twist 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 $\mathrm{Gal}(F \,|\, \mathbb{Q})$. 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 $\mathbb{Q}$.

Applying the methods of Hanselman–Pieper–Schiavone [HPS24] and Bouchet [Bou23, Bou24], we were able to numerically reconstruct a genus 4 curve X from its invariants, defined by

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

inside the projective space $\mathbb{P}^3$ with coordinates x, y, z, w, from the period matrix associated to z' as in (4.1.2). A computation with discriminants shows that this model has good reduction away from the primes 2, 3, 7, and 17. Projection from the point $(-12 : 2 : 4 : 3) \in X(\mathbb{Q})$ and a change of variables to minimize yields the singular affine plane model

$$\begin{aligned} &8x^4y + 8x^3y^2 + 10x^2y^3 + 4xy^4 + 2y^5 - 8x^4 + 24x^3y + 6x^2y^2 + 12xy^3 \\ &\qquad - 2y^4 - 2x^3 - 3x^2y + 6xy^2 - 11y^3 + 14x^2 - 6xy - 4y^2 - 7x + 2y + 1 = 0. \end{aligned} \tag{4.3.4}$$

Let $A := \mathrm{Jac}(X)$ be the Jacobian of X. We have substantial reason to believe that $A_{\mathbb{Q}(\sqrt{3})}$ is isogenous to A_f. First, we confirm that the good L-polynomials over F match by point counts in a large range. Second, using [CMSV19], we compute that the numerical endomorphism algebra of the Jacobian is isomorphic to $\mathbb{Q}(\sqrt{5})$ (over $\mathbb{Q}$) and the numerical geometric endomorphism algebra is indeed isomorphic with the ring of integers of the quartic field 4.4.725.1 and defined over $\mathbb{Q}(\sqrt{3})$. Moreover, it numerically appears that the period matrix of X is isogenous to the one associated to z'. (These are computations done to 100 decimal digits of precision, which are not rigorous.)

Remark 4.3.5. If we knew that A is modular, a computation with finitely many spaces of Hilbert modular forms would allow us to find enough Hecke eigenvalues to show that the only form that could possibly match would be f. Unfortunately we do not know modularity, and this computation would be quite difficult. The method of Faltings–Serre would in principle also allow us to prove the isogeny, but that would require us first to exhaustively list and match the possible mod $\mathfrak{p}$ representations, and the smallest prime norm in the Hecke field is 11, presenting a significant computational challenge.

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. It turns out to be quite computationally expensive to do this in a direct way, say by computing the action of $\mathrm{Gal}(\overline{\mathbb{Q}}\,|\,\mathbb{Q})$ on the tritangent planes of the canonically embedded curve X given in (4.3.3). However, p-adic methods apply, as in the following remark.

Remark 4.3.6. The division polynomial algorithm of Mascot [Mas20] takes as input a smooth, projective curve X of genus g with Jacobian $A := \mathrm{Jac}(X)$, 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 can verify that it defines a number field that contains the field K defined in (1.1.3).

His algorithm 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!

Remark 4.3.7. 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.

References

[BSCM23] Adrian Barquero-Sanchez and Jimmy Calvo-Monge, *On the embedding of Galois groups into wreath products*, 2023, preprint, arXiv:2306.14386. 6

[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. 11, 14

[BR89] D. Blasius and J. Rogawski, *Galois representations for Hilbert modular forms*, Bull. Amer. Math. Soc. (N.S.) **21** (1989), vol. 1, 65–69. 7

[vBCEKSV24a] Raymond van Bommel, Edgar Costa, Noam D. Elkies, Timo Keller, Sam Schiavone, and John Voight, *17T7*, https://github.com/SamSchiavone/17T7. 15

[vBCEKSV24b] Raymond van Bommel, Edgar Costa, Noam D. Elkies, Timo Keller, Sam Schiavone, and John Voight, *EichlerShimuraHMF*, https://github.com/edgarcosta/EichlerShimuraHMF. 15

[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. 8

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265. 2

[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. 2

[Bou23] Thomas Bouchet, *Invariants of genus 4 curves*, preprint, 2023, arXiv:2310.01158. 19

[Bou24] Thomas Bouchet, *Covariant reconstruction of forms from their invariants*, preprint, 2024, arXiv:2403.17490. 19

[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. 7

[CDD91] Henri Cohen and Francisco Diaz y Diaz, *A polynomial reduction algorithm*, Sém. Théor. Nombres Bordeaux (2) **3** (1991), no. 2, 351–360. 17

[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. 19

[Cre97] J.E. Cremona, *Algorithms for Modular Elliptic Curves*, 2nd. ed., Cambridge University Press, Cambridge, 1997. 14

[CD17] Clifton Cunningham and Lassina Dembélé, *Lifts of Hilbert modualr forms and application to modularity of abelian varieties*, preprint, 2017, arXiv:1705.03054. 8

[CR06] Charles W. Curtis and Irving Reiner, *Representation Theory of Finite Groups and Associative Algebras*, AMS Chelsea Publishing, Providence, RI, 2006. 7

[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. 2, 11

[Dem08] Lassina Dembélé, *An algorithm for modular elliptic curves over real quadratic fields*, Experiment. Math. **17** (2008), no. 4, 427–438. 2, 11, 14

[Dem09] Lassina Dembélé, *A non-solvable Galois extension of ramified at* 2 *only*, Comptes Rendus. Math. **347** (2009), no. 3-4, 111–116. 2, 8

[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. 2, 9, 10, 15

[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. 2, 8

[Del71] Pierre Deligne, *Travaux de Shimura*, Séminaire Bourbaki, 23ème année (1970/1971), exposé 389, Lecture Notes in Math., vol. 244, Springer, 1971, 123–165. 18

[DN67] Koji Doi and Hidehisa Naganuma, *On the algebraic curves uniformized by arithmetical automorphic functions*, Ann. Math. (2) **86** (1967), no. 3, 449–460. 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. 9

[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. 2

[EK] Noam D. Elkies and Jean Kieffer, *A uniform quasi-linear time algorithm for evaluating theta functions in any dimension*, in preparation. 16

[FK14] Claus Fieker and Jürgen Klüners, *Computation of Galois groups of rational polynomials*, LMS J. Comput. Math. **17** (2014), no. 1, 141–158. 2, 17

[Flint] The FLINT team, *FLINT: Fast Library for Number Theory*, 2024, Version 3.1.3, https://flintlib.org. 16

[G88] Gerard van der Geer, *Hilbert Modular Surfaces*, Ergeb. Math. Grenzgeb. (3), vol. 16, Springer-Verlag, Berlin, 1988. 13

[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. 9

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

[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. 11

[HPS24] Jeroen Hanselman, Andreas Pieper, and Sam Schiavone, *Equations of genus 4 curves from their theta constants*, preprint, 2024, arXiv:2402.03160. 19

[Igu64] Jun-ichi Igusa, *On Siegel modular forms of genus two. II*, Amer. J. Math. **86** (1964), 392–412. 14

[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

[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. 5

[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. 9

[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. 2

[Mas20] Nicolas Mascot, *Hensel-lifting torsion points on Jacobians and Galois representations*, Math. Comp. **89** (2020), no. 323, 1417–1455. 20

[Oda82] Takayuki Oda, *Periods of Hilbert modular surfaces*, Progr. Math., vol. 19 Birkhäuser, Boston, MA, 1982. 2, 11, 12, 13, 15

[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. 11, 12

[Pari] The PARI Group, PARI/GP version 2.15.4, Univ. Bordeaux, 2023, http://pari.math.u-bordeaux.fr/. 17

[Ric22] James Rickards, *Improved computation of fundamental domains for arithmetic Fuchsian groups*, Math. Comp. **91** (2022), no. 338, 2929–2954. 18

[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. 18

[SV16] Jeroen Sijsling and John Voight, *On explicit descent of marked curves and maps*, Res. Number Theory **2**:27 (2016), 35 pages. 19

[Sta73] Richard P. Stauduhar, *The determination of Galois groups*, Math. Comput. **27** (1973), 981–996. 2, 17

[Tay89] Richard Taylor, *On Galois representations associated to Hilbert modular forms*, Invent. Math. **98** (1989), vol. 2, 265–280. 7

[Voi09] John Voight, *Computing fundamental domains for Fuchsian groups*, J. Théorie Nombres Bordeaux **21** (2009), no. 2, 467–489. 18

[Voi21] John Voight, *Quaternion algebras*, Grad. Texts in Math., vol. 288, Springer, Cham, 2021. 9, 11, 18

[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. 11, 20

[Z01] Shouwu Zhang, *Heights of Heegner points on Shimura curves*, Ann. of Math. (2) **153** (2001), no. 1, 27–147. 10

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

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