In search of 17T7: explicit realizations of Galois groups

Sam Schiavone, MIT

Joint work with Raymond van Bommel, Edgar Costa, Noam Elkies, Timo Keller, and John Voight

VaNTAGe

October 31, 2023

Outline

(I) Background
(II) The group 17T7
(III) Previous work
(IV) In search of 17T7

The inverse Galois problem

Q: Does every finite group occur as a Galois group over $\mathbb{Q}$? I.e., given a finite group G, is there a finite Galois extension $K/\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) \cong G$?

If so, we say that *the IGP holds for G*.

The inverse Galois problem

Q: Does every finite group occur as a Galois group over $\mathbb{Q}$? I.e., given a finite group G, is there a finite Galois extension $K/\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) \cong G$?

If so, we say that *the IGP holds for G*.

Let α be a primitive element for K, so $K = \mathbb{Q}(\alpha)$. Let m be its minimal polynomial with roots $\alpha = \alpha_1, \ldots, \alpha_n$.

Then $\mathrm{Gal}(K/\mathbb{Q})$ acts faithfully and transitively on the α_i, realizing $\mathrm{Gal}(K/\mathbb{Q})$ as a transitive subgroup of S_n.

The Klüners-Malle database

In their database, for each transitive group of degree ≤ 23, Klüners and Malle give a polynomial realizing it as a Galois group over $\mathbb{Q}$. (http://galoisdb.math.uni-paderborn.de/)

With two notable exceptions: neither 17T7 nor 23T5 has a polynomial. 23T5 is the well-known Mathieu group M_{23}.

The group ~~17T7~~ 17T6 $\cong \mathrm{SL}_2(\mathbb{F}_{16})$

$\mathrm{SL}_2(\mathbb{F}_{16})$ acts on $\mathbb{P}^1(\mathbb{F}_{16})$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot (x : y) = (ax + by : cx + dy)$$

and this gives an embedding $\mathrm{SL}_2(\mathbb{F}_{16}) \hookrightarrow S_{17}$ whose image is 17T6.

The group ~~17T7~~ 17T6 $\cong \mathrm{SL}_2(\mathbb{F}_{16})$

$\mathrm{SL}_2(\mathbb{F}_{16})$ acts on $\mathbb{P}^1(\mathbb{F}_{16})$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot (x : y) = (ax + by : cx + dy)$$

and this gives an embedding $\mathrm{SL}_2(\mathbb{F}_{16}) \hookrightarrow S_{17}$ whose image is 17T6.

Lemma (Trace lemma)

Let $H \leq \mathrm{SL}_2(\mathbb{F}_{16})$ be a subgroup such that the trace map $\mathrm{tr} : H \to \mathbb{F}_{16}$ is surjective, i.e., every element of $\mathbb{F}_{16}$ occurs as the trace of an element of H. Then $H = \mathrm{SL}_2(\mathbb{F}_{16})$.

The group 17T7 $\cong \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2$

Throughout, let G be 17T7. As an abstract group

$$G \cong \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2 \,.$$

Here C_2 acts on $\mathrm{SL}_2(\mathbb{F}_{16})$ by the Frobenius map $\sigma : x \mapsto x^4$ of $\mathbb{F}_{16}/\mathbb{F}_4$, so

$$\sigma \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^4 & b^4 \\ c^4 & d^4 \end{pmatrix} \,.$$

The action $\mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2 \circlearrowright \mathbb{P}^1(\mathbb{F}_{16})$

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

embeds $\mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2 \hookrightarrow S_{17}$ as 17T7.

Realizing 17T6: an overview

In *Explicit computations with modular Galois representations*, Bosman uses the following strategy to show the IGP holds for 17T6.

- Find N and a modular form $f \in S_2(\Gamma_0(N))$ such that its mod 2 representation $\overline{\rho_f}$ has some desired properties.
- By modularity, this is isomorphic to the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the 2-torsion of an isogeny factor of $\mathrm{Jac}(X_0(N))$.
- Compute complex approximations of these 2-torsion points with sufficient precision to recover a polynomial realizing $\mathrm{SL}_2(\mathbb{F}_{16})$ over $\mathbb{Q}$.

Realizing 17T6

Let $f \in S_2(\Gamma_0(N))$ be a newform with q-expansion $f = \sum_{n=1}^{\infty} a_n q^n$, and let $H = \mathbb{Q}(\{a_n\}_n)$ be the Hecke eigenvalue field.

Given a prime $\ell \in \mathbb{Z}$ and a prime λ of H with $\lambda \mid \ell$, there is a Galois representation

$$\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\lambda)$$

such that for each prime $p \nmid N\ell$

$$\begin{aligned} \mathrm{tr}(\rho_f(\mathrm{Frob}_p)) &\equiv a_p \pmod{\lambda} \\ \det(\rho_f(\mathrm{Frob}_p)) &\equiv p \pmod{\lambda}. \end{aligned}$$

Realizing 17T6

Let $f \in S_2(\Gamma_0(N))$ be a newform with q-expansion $f = \sum_{n=1}^{\infty} a_n q^n$, and let $H = \mathbb{Q}(\{a_n\}_n)$ be the Hecke eigenvalue field.

Given a prime $\ell \in \mathbb{Z}$ and a prime λ of H with $\lambda \mid \ell$, there is a Galois representation

$$\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\lambda)$$

such that for each prime $p \nmid N\ell$

$$\begin{aligned} \mathrm{tr}(\rho_f(\mathrm{Frob}_p)) &\equiv a_p \pmod{\lambda} \\ \det(\rho_f(\mathrm{Frob}_p)) &\equiv p \pmod{\lambda}. \end{aligned}$$

The fixed field K of $\ker(\rho_f)$ is Galois over $\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{img}(\rho_f)$.

Realizing 17T6

$$\begin{aligned} \mathrm{tr}(\rho_f(\mathrm{Frob}_p)) &\equiv a_p \pmod{\lambda} \\ \det(\rho_f(\mathrm{Frob}_p)) &\equiv p \pmod{\lambda}. \end{aligned}$$

If $\ell = 2$, then $p \nmid N\ell$ is odd, so

$$\det(\rho_f(\mathrm{Frob}_p)) \equiv p \equiv 1 \pmod{\lambda}.$$

By Chebotarev, every element of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ occurs as a Frobenius, so this shows that $\mathrm{img}(\rho_f) \subseteq \mathrm{SL}_2(\mathbb{F}_\lambda)$.

Realizing 17T6

Using a computer, Bosman finds a suitable form $f \in S_2(\Gamma_0(137))$ such that H has defining polynomial $x^4 + 3x^3 - 4x - 1$ and 2 is inert in H.

Thus $\mathrm{img}(\rho_f) \subseteq \mathrm{SL}_2(\mathbb{F}_{16})$, and by showing that all traces occur, then $\mathrm{img}(\rho_f) = \mathrm{SL}_2(\mathbb{F}_{16})$ by the trace lemma.

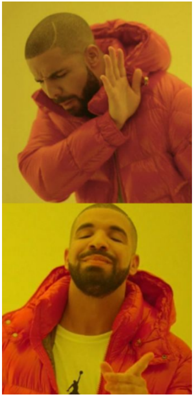
It turns out that the subspace of $S_2(\Gamma_0(137))$ spanned by the Galois conjugates of f is exactly the fixed space of the Atkin-Lehner operator w_{137}.

He computes numerical approximations of the 2-torsion points of $\mathrm{Jac}(X_0(137)/\langle w_{137}\rangle)$ and recognizes the polynomial

$$x^{17} - 5x^{16} + 12x^{15} - 28x^{14} + 72x^{13} - 132x^{12} + 116x^{11} - 74x^9 + 90x^8 - 28x^7 - 12x^6 + 24x^5 - 12x^4 - 4x^3 - 3x - 1\,.$$

Realizing 17T7?

How do we deal with the extra C_2 extension?



One possibility: try to find a suitable 8-fold occuring as an isogeny factor of $J_0(N)$ by searching for suitable classical modular forms. But these are high dimensional abelian varieties and necessitate computations with theta functions in 8 variables...

Our approach: try to find a suitable RM abelian 4-fold by searching a database of corresponding Hilbert modular forms.

The action of $\mathrm{GL}_2^+(F)$ on $\mathfrak{h}^2$

- $\mathfrak{h}$ = complex upper half-plane
- F = real quadratic field
- v_1, v_2 the embeddings $F \hookrightarrow \mathbb{R}$
- $\mathbb{Z}_F$ = ring of integers of F
- An element $\alpha \in F$ is *totally positive* (denoted $\alpha \gg 0$) if $v_j(\alpha) =: \alpha_j > 0$ for $j = 1, 2$.
- $\mathrm{GL}_2^+(F) = \{\gamma \in \mathrm{GL}_2(F) : \det(\gamma) \gg 0\}$

The action of $\mathrm{GL}_2^+(F)$ on $\mathfrak{h}^2$

- $\mathfrak{h}$ = complex upper half-plane
- F = real quadratic field
- v_1, v_2 the embeddings $F \hookrightarrow \mathbb{R}$
- $\mathbb{Z}_F$ = ring of integers of F
- An element $\alpha \in F$ is *totally positive* (denoted $\alpha \gg 0$) if $v_j(\alpha) =: \alpha_j > 0$ for $j = 1, 2$.
- $\mathrm{GL}_2^+(F) = \{\gamma \in \mathrm{GL}_2(F) : \det(\gamma) \gg 0\}$

We can embed $\mathrm{GL}_2^+(F) \hookrightarrow \mathrm{GL}_2^+(\mathbb{R}) \times \mathrm{GL}_2^+(\mathbb{R})$ via the embeddings v_1, v_2. This gives an action $\mathrm{GL}_2^+(F) \circlearrowright \mathfrak{h}^2$ coordinatewise by linear fractional transformations:

$$\gamma z = (\gamma_1 z_1, \gamma_2 z_2) = \left(\frac{a_1 z_1 + b_1}{c_1 z_1 + d_1}, \frac{a_2 z_2 + b_2}{c_2 z_2 + d_2} \right)$$

where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(F)$ and $z \in \mathfrak{h}^2$.

Standard congruence subgroups

Let

$$\Gamma_0(\mathfrak{N}) := \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Z}_F) : c \in \mathfrak{N} \right\} .$$

The quotient $\Gamma_0(\mathfrak{N})\backslash\mathfrak{h}^2 =: Y_0(\mathfrak{N})$ is a **Hilbert modular variety**. We denote its compactification by $X_0(\mathfrak{N})$. These are moduli spaces for polarized abelian varieties with RM by an order of F, together with level and torsion structure.

Hilbert modular forms

Let $k = (k_j)_j \in \mathbb{Z}^2_{\geq 0}$ with all k_j of the same parity. A **Hilbert modular form** (HMF) of weight k for $\Gamma_0(\mathfrak{N})$ is a holomorphic function $f\colon \mathfrak{h}^2 \to \mathbb{C}$ such that

$$f(\gamma z) = \left(\prod_{j=1}^{2} \frac{(c_j z_j + d_j)^{k_j}}{\det(\gamma_j)^{k_j/2}} \right) f(z)$$

for all $\gamma \in \Gamma_0(\mathfrak{N})$.

Hilbert modular forms

HMFs admit Fourier expansions! Assume F has narrow class number $h^+(F) = 1$. Then

$$f(z) = a_0 + \sum_{\nu \in \mathfrak{D}^{-1}_{>0}} a_\nu q_1^{\nu_1} \cdots q_n^{\nu_n} \,,$$

where $q_j = e^{2\pi i z_j}$ and $\mathfrak{D}$ is the different ideal of F.

HMFs admit Fourier expansions! Assume F has narrow class number $h^+(F) = 1$. Then

$$f(z) = a_0 + \sum_{\nu \in \mathfrak{D}^{-1}_{>0}} a_\nu q_1^{\nu_1} \cdots q_n^{\nu_n} \,,$$

where $q_j = e^{2\pi i z_j}$ and $\mathfrak{D}$ is the different ideal of F.

Given $0 \neq \mathfrak{n} \trianglelefteq \mathbb{Z}_F$, then $\mathfrak{n} = \nu\mathfrak{D}^{-1}$ for some $\nu \in \mathbb{Z}_{F,\geq 0}$. We then define

$$a_{\mathfrak{n}} := a_\nu$$

and call this the *Fourier coefficient of f at* $\mathfrak{n}$.

Hilbert modular forms

Write $\mathrm{Gal}(F/\mathbb{Q}) = \langle \sigma \rangle$. If $f \in S_2(\Gamma_0(\mathfrak{N}))$ has Fourier coefficients $a_{\mathfrak{n}}(f)$, define the HMF f^σ to have Fourier coefficients

$$a_{\mathfrak{n}}(f^\sigma) := a_{\sigma(\mathfrak{n})}(f)\,.$$

Conjecturally, to an HMF f, together with its Galois conjugate f^σ, one can associate a pair A, A' of abelian varieties.

Outline of our approach

1. Search for HMFs f, f^σ with desired properties.
2. Use an analogue of the Eichler-Shimura construction to compute the 2-torsion field of the corresponding abelian 4-folds A and A'.
   (i) Compute the periods of A and A' by twisting L-series by quadratic characters.
   (ii) Construct the moduli points $\tau, \tau' \in \mathfrak{h}^4$ corresponding to A, A' as ratios of the periods.
   (iii) Form the corresponding period matrices Π, Π'.
   (iv) Form suitable polynomials in the theta constants with characteristic evaluated at Π, Π'.

Recognizing the coefficients of these polynomials as rational numbers produces the desired degree 17 polynomial! (We hope!)

HMF search

Goal: Find HMFs f with the following properties. Let F be its base field (a real quadratic field) and $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ be the involution.

(i) f is not the base change of a classical modular form;

(ii) The Hecke eigenvalue field H of f is a totally real quartic field;

(iii) 2 is inert in H;

(iv) H has an involution $\iota : H \to H$ such that

$$\iota(a_{\mathfrak{p}}) \equiv a_{\sigma(\mathfrak{p})} \pmod 2$$

for all Hecke eigenvalues $a_{\mathfrak{p}}$ of f; and

(v) Every element of $\mathbb{F}_{16}$ occurs as an eigenvalue mod 2, i.e.,

$$\{a_{\mathfrak{p}} \bmod 2 : \mathfrak{p} \text{ a prime of } F\} = \mathbb{F}_{16}\,.$$

HMF search

Searching the LMFDB, we find 18 HMFs with these properties.

`2.2.12.1-578.1-c`	`2.2.12.1-578.1-d`	`2.2.12.1-722.1-i`
`2.2.12.1-722.1-j`	`2.2.12.1-722.1-k`	`2.2.12.1-722.1-l`
`2.2.8.1-2601.1-j`	`2.2.8.1-2601.1-k`	`2.2.8.1-2738.1-e`
`2.2.8.1-2738.1-f`	`2.2.12.1-1587.1-i`	`2.2.12.1-1587.1-l`
`2.2.12.1-1587.1-m`	`2.2.12.1-1587.1-n`	`2.2.24.1-726.1-i`
`2.2.24.1-726.1-j`	`2.2.24.1-726.1-k`	`2.2.24.1-726.1-l`

These have base fields $\mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{2})$, and $\mathbb{Q}(\sqrt{6})$, respectively.
Of these fields, only $\mathbb{Q}(\sqrt{2})$ has narrow class number 1.

Remark

The existence of such HMFs can be used to give a non-constructive proof that the IGP holds for 17T7.

The Eichler-Shimura construction

Let F be a real quadratic field and let $f \in S_2(\Gamma_0(\mathfrak{N}))$ be an eigenform with Fourier coefficients $a_{\mathfrak{n}}(f)$. Recall that f^σ is the HMF with Fourier coefficients $a_{\mathfrak{n}}(f^\sigma) = a_{\sigma(\mathfrak{n})}(f)$.

Conjecture (Eichler-Shimura)

Assume f has integral Fourier coefficients. Then there exist abelian varieties A, A' such that

$$L(A,s) = L(f,s) \qquad L(A',s) = L(f^\sigma,s)\,.$$

Decomposition of H_2

Assume $h^+(F) = 1$, and let $\epsilon \in \mathbb{Z}_F^\times$ be a unit with $\epsilon_1 > 0, \epsilon_2 < 0$.

Let $H := H_2(X_0(\mathfrak{N}), \mathbb{Q})$. Then there is a decomposition

$$H = H^{++} \oplus H^{+-} \oplus H^{-+} \oplus H^{--}$$

arising from the involutions

$$\begin{gathered} \mathfrak{h} \times \mathfrak{h} \to \mathfrak{h} \times \mathfrak{h} \\ (z_1, z_2) \mapsto (\epsilon_1 z_1, \epsilon_2 \overline{z_2}) \\ (z_1, z_2) \mapsto (\epsilon_2 \overline{z_1}, \epsilon_1 \overline{z_2}) \end{gathered}$$

that descend to $X_0(\mathfrak{N})$.

Riemann-Hodge period relation

Theorem

Let $\{\gamma_{ss'} : s, s' \in \{\pm\}\}$ *be a normalized basis respecting the above decomposition. Let*

$$\Omega_j^{ss'} := (2\pi i)^2 \int_{\gamma_{ss'}} f_j(z_1, z_2)\, dz_1 \wedge dz_2$$

where f_j *is the* j^{th} *embedding of* f*. Then*

$$\Omega_j^{++}\Omega_j^{--} + \Omega_j^{+-}\Omega_j^{-+} = 0$$

for all j*.*

Moduli point of an RM abelian variety

Theorem

Let $f \in S_2(\mathrm{SL}_2(\mathbb{Z}_F))$ be a primitive form, and let A, A' be the corresponding RM abelian varieties. With notation as before, then

$$\tau := \left(\frac{\Omega_1^{+-}}{\Omega_1^{++}}, \ldots, \frac{\Omega_g^{+-}}{\Omega_g^{++}}\right) \in \mathfrak{h}^g$$

$$\tau' := \left(\frac{\Omega_1^{-+}}{\Omega_1^{++}}, \ldots, \frac{\Omega_g^{-+}}{\Omega_g^{++}}\right) \in \mathfrak{h}^g$$

represent the moduli points in $\mathrm{GL}_2^+(F)\backslash\mathfrak{h}^g$ of the isogeny classes of A and A'. (For us, $g = 4$.)

Computing periods $\Omega_j^{ss'}$ via twisting

The following conjecture is inspired by BSD.

Conjecture

Assume $h^+(F) = 1$ *and let* ε *be a fundamental unit with* $\varepsilon_1 > 0, \varepsilon_2 < 0$. *Let* $\chi : (\mathbb{Z}_F/\mathfrak{c})^\times \to \mathbb{C}^\times$ *be a primitive quadratic character of conductor* $\mathfrak{c} = (\nu)$ *that is coprime to* $\mathfrak{N}$, *where* $\nu \gg 0$. *Then*

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

for some $\alpha_\chi \in \mathbb{Z}_H$, *where* $G(\chi)$ *is the Gauss sum of* χ, *and*

$$\chi(\sigma(\varepsilon)) = s \qquad \chi(\varepsilon) = s'.$$

By computing for multiple χ, we can get an educated guess for the period $\Omega_j^{ss'}$.

Forming period matrices

Choose an integral basis $\beta_1, \ldots, \beta_g$ of $\mathbb{Z}_H$, and let $\eta_1, \ldots, \eta_g$ be the embeddings $H \hookrightarrow \mathbb{R}$.

The small period matrix corresponding to the lattice $\mathbb{Z}_H \oplus \mathbb{Z}_H \tau$ is

$$\Pi := M^{-1} D_\tau (M^t)^{-1}$$

where M is the $g \times g$ matrix whose i, j entry is $\eta_i(\beta_j)$ and $D_\tau = \text{diag}(\tau_1, \ldots, \tau_g)$.

Remark

Π has positive definite imaginary part iff each τ_j has positive imaginary part, which can be arranged if H also has narrow class number 1.

Theta constants

The tuple of theta constants $(\theta_m)_m$ with characteristic give embeddings of $A, A' \hookrightarrow \mathbb{P}^N$ into projective space.

We consider the images of the 2-torsion points under this embedding and form a suitable polynomial. This polynomial will hopefully realize 17T7 as a Galois group!

Progress

- Using our implementation, reproduced examples from Dembélé's *An Algorithm for Modular Elliptic Curves over Real Quadratic Fields*. In this case, we were able to recover the curves themselves, rather than just their 2-torsion fields.
- Reproduced 2-dimensional examples from Dembélé–Voight's *Explicit methods for Hilbert modular forms*. However, determining the correct isogeny proved difficult.

Outline of our approach

1. Search for HMFs f, f^σ with desired properties. ✓
2. Use an analogue of the Eichler-Shimura construction to compute the 2-torsion field of the corresponding abelian 4-folds A and A'.
   (i) Compute the periods of A and A' by twisting L-series by quadratic characters. ✓
   (ii) Construct the moduli points $\tau, \tau' \in \mathfrak{h}^4$ corresponding to A, A' as ratios of the periods. ✓
   (iii) Form the corresponding period matrices Π, Π'. ✓
   (iv) Form suitable polynomials in the theta constants with characteristic evaluated at Π, Π'.

Recognizing the coefficients of these polynomials as rational numbers produces the desired degree 17 polynomial! (We hope!)

TODO

- The Eichler-Shimura construction only produces abelian varieties up to isogeny. How do we find the right isomorphism class within this isogeny class? (In the elliptic curve case, the number of real components affects this.)
- What degree isogeny must we apply to get from the abelian variety we produce to the one that we want?

Thank you!