17T7 as a Galois group over $\mathbb{Q}$ through Hilbert modular forms

Raymond van Bommel

joint with Edgar Costa, Noam Elkies, Timo Keller, Sam Schiavone, and John Voight

Heilbronn Number Theory Seminars
2 October 2024

The inverse Galois problem

Given a polynomial $f \in \mathbb{Q}[x]$, we can create a splitting field $L/\mathbb{Q}$, a smallest field containing all roots of f. The group $\mathrm{Aut}(L)$ consisting of automorphisms of this splitting field, is called **the Galois group** of f. If f is irreducible of degree d, then its Galois group is a transitive subgroup of S_d

Problem

Does every transitive subgroup of S_d occur as the Galois group of some polynomial over $\mathbb{Q}$ of degree d?

There are variations of this problem where one asks for:

- a regular extension over $\mathbb{Q}(t)$ (i.e. the intersection of the extension with $\overline{\mathbb{Q}}$ is $\mathbb{Q}$),
- a Galois extension satisfying certain local properties (e.g. certain number of real roots, or certain splitting behaviour for certain primes).

In general, the problem is open, but it known for all solvable groups, and all transitive subgroups of S_d for $d \leq 22$. The "next" open case is $M_{23} \subset S_{23}$.

What is 17T7?

There is a systematic way to number transitive subgroups of S_d with labels of the shape $d\mathrm{T}n$ indicating the nth transitive subgroup of S_d. For example, the transitive subgroups of S_4 are $4\mathrm{T}1 = C_4$, $4\mathrm{T}2 = V_4$, $4\mathrm{T}3 = D_4$, $4\mathrm{T}4 = A_4$, and $4\mathrm{T}5 = S_4$.

Fun fact

Klüners and Malle maintain a database of number fields with certain Galois groups. The groups and number fields can also be found in the LMFDB.

It turns out that S_{17} has three non-solvable transitive subgroups:

$$17\mathrm{T}6 = \mathrm{SL}_2(\mathbb{F}_{16}), \qquad 17\mathrm{T}7 = \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_2, \qquad 17\mathrm{T}8 = \mathrm{SL}_2(\mathbb{F}_{16}) \rtimes C_4.$$

Here $\mathrm{SL}_2(\mathbb{F}_{16})$ naturally acts on the 17 elements of $\mathbb{P}^1(\mathbb{F}_{16})$ and C_2 (resp. C_4) act on $\mathbb{P}^1(\mathbb{F}_{16})$ through the Frobenius $x \mapsto x^4$ (resp. $x \mapsto x^2$).

The group 17T8 can be realised as a Galois group using Belyi maps. The group 17T6 can be realised using abelian fourfolds with real multiplication.

17T7 as a Galois group

Theorem

The polynomial

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

has Galois group 17T7.

Fun fact

The number field has discriminant $2^{44} \cdot 3^6 \cdot 17^8$.

You could verify this with your favourite computer algebra package and use it to write down a formal proof. But maybe the more interesting question is: how did we find this polynomial?

The answer is: Hilbert modular forms. Before I will introduce these, I will first talk about abelian varieties and real multiplication.

Abelian varieties

Abelian varieties are higher dimensional analogous of elliptic curves.

Definition

An abelian variety is a connected proper/projective algebraic group variety.

The typical example of an abelian variety is the Jacobian of a curve, but not all abelian varieties arise in this way.

Theorem

Over $\mathbb{C}$ an abelian variety is a complex torus, i.e. isomorphic to $\mathbb{C}^g/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}^g$ of full rank.

Let A be an abelian variety over $\mathbb{Q}$. Then, for any integer ℓ, the torsion subgroup $A[\ell](\overline{\mathbb{Q}}) \cong (\mathbb{Z}/\ell\mathbb{Z})^{2g}$ is a so-called Galois represention with the action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Endomorphisms of abelian varieties

Typically, the only endomorphisms of an abelian variety over $\mathbb{Q}$ are given by multiplication by n for some integer n. Sometimes there are more. For example, for elliptic curves, there is the case of complex multiplication (CM).

For general abelian varieties over $\mathbb{Q}$, there are a lot of different things that can happen. Depending on whether the abelian variety is simple or not, you could get matrix groups, orders in quaternion algebras, products of fields, et cetera.

We are interested in the case of real multiplication (RM), which for the purpose of this talk is defined as follows.

Definition

Let A/K be an abelian variety of dimension g over a number field K and let $\mathcal{O} \subset H$ be an order in a totally real number field of degree g. Then we say that A has **real multiplication** by $\mathcal{O}$, if there exists an injection $\mathcal{O} \hookrightarrow \mathrm{End}(A)$.

During this talk, for simplicity, we will assume $\mathcal{O}$ the be the maximal order, i.e. the ring of integers.

17T6 as Galois group

The two-torsion of an abelian fourfold with RM can be used to realise 17T6 as a Galois group.

Idea (17T6)

Suppose $A/\mathbb{Q}$ is an abelian variety such that:

- A has dimension 4;
- A has RM by $\mathcal{O} \subset H$ for some totally real degree 4 number field H.
- the prime 2 is unramified and inert in $\mathcal{O}$, i.e. that $\mathcal{O}/2\mathcal{O} \cong \mathbb{F}_{16}$.

Then $A[2]$ becomes $\mathbb{F}_{16} \oplus \mathbb{F}_{16}$ as a $\mathbb{F}_{16}$-vector space, and the action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ respects this vector space structure, so it will act on the space $\mathbb{P}(A[2]) \cong \mathbb{P}^1(\mathbb{F}_{16})$ as a subgroup of $\mathrm{SL}_2(\mathbb{F}_{16})$.

By sampling some different primes $\ell > 2$ and making sure that every element of $\mathbb{F}_{16}$ occurs as the trace of some $\mathrm{Frob}_\ell \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we can guarantee that the Galois group is $\mathrm{SL}_2(\mathbb{F}_{16}) = 17\mathrm{T}6$.

17T7 as Galois group

By looking at an RM abelian fourfold over a quadratic field we can get 17T7.

Idea

This time take A/K as before but now over a quadratic number field K. We get a tower of fields

$$\mathbb{Q} \subset K \subset K(A[2])$$

and we take the normal/Galois closure of $K(A[2])$ over $\mathbb{Q}$. Generically, you would expect to get the wreath product $\mathrm{SL}_2(\mathbb{F}_{16}) \wr C_2$ as Galois group if you do this. However, we will impose

$$A[2] \xrightarrow{\sigma} A^\sigma[2] \xrightarrow{M} A^\sigma[2] \xrightarrow{\sigma} A[2] \ ,$$

is the map $\mathrm{Frob}_{\mathbb{F}_{16}/\mathbb{F}_4}(M)$ for any matrix $M \in \mathrm{SL}_2(\mathbb{F}_{16})$, where σ is the generator of $\mathrm{Gal}(K/\mathbb{Q})$.

Under these conditions, again assuming surjectivity on the traces, the Galois group of the normal closure of $K(A[2])$ will be 17T7.

Classical modular forms

Each elliptic curve is isomorphic to $\mathbb{C}/(\mathbb{Z}1 \oplus \mathbb{Z}\tau)$ for some $\tau \in \mathbb{H}$. There are different ways to represent the same lattice end $\mathrm{GL}_2^+(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})$ acts as

$$\tau \mapsto \frac{a\tau + b}{c\tau + d} \qquad \text{for} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Z}).$$

Definition

A **classical modular form** (of weight 2) is a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ such that[a]

$$f\left(\frac{az + b}{cz + d}\right) = (cz + d)^2 f(z) \qquad \text{for all} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma,$$

where $\Gamma \subset \mathrm{GL}_2^+(\mathbb{Z})$ is some congruence subgroup (e.g. $c \equiv 0 \mod n$).

[a] plus some other technical conditions.

Each modular form has a q-expansion $\sum_{n \geq 0} a_n q^n$ where $q = e^{2\pi i z}$.

Hilbert modular forms

Each RM abelian variety is isomorphic to $\mathbb{C}^g/(\mathcal{O}\vec{1} \oplus \mathcal{O}\vec{\tau})$ for some $\vec{\tau} \in \mathbb{H}^g$, where $\mathcal{O}$ acts on $\mathbb{C}^g$ through the g embeddings $\iota_1, \ldots, \iota_g : \mathcal{O} \hookrightarrow \mathbb{R}$. This time the group $\mathrm{GL}_2^+(\mathcal{O})$ acts on $\mathbb{H}^g$ as

$$(\tau_i)_i \mapsto \left(\frac{a_i\tau_i + b_i}{c_i\tau_i + d_i}\right)_i \quad \text{for} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathcal{O}), \quad \text{where } a_i = \iota_i(a), \ldots.$$

Definition

A **Hilbert modular form** (of parallel weight 2) is a holomorphic function $f : \mathbb{H}^g \to \mathbb{C}$ such that[a]

$$f\left(\frac{a\vec{z} + b}{c\vec{z} + d}\right) = \prod_{i=1}^{g} \frac{(c_i z_i + d_i)^2}{a_i d_i + b_i c_i} \cdot f(z) \qquad \text{for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma,$$

where $\Gamma \subset \mathrm{GL}_2^+(\mathcal{O})$ is some congruence subgroup (e.g. $c \equiv 0 \mod \mathfrak{n}$).

[a] plus some other technical conditions.

Hilbert modular forms have a q-expansion $a_0 + \sum_{\mu \in \mathrm{Diff}(\mathcal{O})_+^{-1}} a_\mu q^{\mathrm{Tr}(\mu\vec{z})}$.

Modularity

These Hecke eigenvalues a_n can be used to define an L-function of a modular form. This can be done similarly for abelian varieties, e.g. for an elliptic curve E over $\mathbb{Q}$, we define $a_p = p + 1 - |E_p(\mathbb{F}_p)|$ for any prime p of good reduction.

Conjecture (modularity, Eichler-Shimura)

There is a correspondence between Hilbert modular newforms (with $\mathcal{O} \subset K$) and RM abelian varieties defined over K having the same L-function.

Altough the conjecture is still open in many cases, it is possible to get the "torsion subgroup" directly from the modular form.

Theorem (Carayol, Taylor, Blasius–Rogawski)

For every Hilbert modular form, satisfying some mild conditions, and every prime $\mathfrak{l}$ there exists a Galois representation over $\mathbb{F}_\mathfrak{l}$, the "torsion subgroup of the abelian variety from the conjecture".

For most $\mathfrak{p} \nmid \mathrm{Norm}(\mathfrak{l})$, the trace of $\mathrm{Frob}_\mathfrak{p}$ of this representation is $a_\mathfrak{p} \mod \mathfrak{l}$. We can use this to find 17T7.

17T7 from a Hilbert modular form

The following idea is based on a strategy used by Bosman to realise 17T6 using classical modular forms.

Theorem

Suppose there exists a Hilbert modular form over a quadratic field K such that

- *its coefficient field H is of degree 4,*
- *2 is inert in H,*
- $a_{\sigma(\mathfrak{n})} = a_{\mathfrak{n}}^4 \mod 2$, *where* $\langle\sigma\rangle = \mathrm{Gal}(K/\mathbb{Q})$,
- $\{a_{\mathfrak{p}} \mod 2\} = \mathbb{F}_{16}$.

Then the Galois group of the associated representation over $\mathbb{F}_{16}$ will give rise to a Galois 17T7 extension of $\mathbb{Q}$.

We found the modular form $f =$ `2.2.12.1-578.1-c` satisfying these conditions on the L-functions and modular forms database, so we are done!

Question

How do we get an actual degree 17 polynomial now?

Periods from L-functions

The periods of A_f and A_{f^σ}, which can be defined using some integrals on a Hilbert modular surface, can also be computed using the following conjecture, which has similar vibes as BSD.

Conjecture (Oda)

Up to isogeny, the periods of A_f and A_{f^σ} as point in $\mathbb{H}^4$ are

$$\tau = \left(\frac{\Omega^{+-}}{\Omega^{++}}(f^\iota)\right)_{\iota\colon H\hookrightarrow\mathbb{C}} \quad \text{and} \quad \tau^\sigma = \left(\frac{\Omega^{-+}}{\Omega^{++}}(f^\iota)\right)_{\iota\colon H\hookrightarrow\mathbb{C}}.$$

For each character χ of K of sign $s, s' \in \{\pm 1\}$ there is an $\alpha_\chi \in \mathcal{O}_H$ such that

$$\alpha_\chi^\iota \Omega^{ss'}(f^\iota) = -4\pi^2\sqrt{\Delta(K)}G(\overline{\chi})L(f^\iota \otimes \chi, 1),$$

where G is the Gauß sum and $f^\iota \otimes \chi$ is a twisted L-function.

Idea (Cremona, Dembélé, Dembélé–Voight)

Compute all other terms and guess α_χ by taking multiple χs.

From periods to a degree 17 polynomial

Idea

From τ, we create a small period matrix. Note that we only had A_f up to isogeny, so we tried all 2-isogenies and found one period matrix Π in the Schottky locus of abelian varieties that are a Jacobian.[a]

Then we use a recent method by Kieffer to compute

$$\prod_{\mathbb{F}_{16}\text{-isog. } \Pi' \sim \Pi} \left(x - \frac{\sum_m \Theta_m^8(\Pi')}{\sum_m \Theta_m^8(\Pi)} \cdot 2^{e_{\Pi'}} \right).$$

We recognise some its coefficients as rational numbers and use Newton-Raphson's method to find the rest.

[a] This was expected as one can show independently that this abelian fourfold is a Jacobian through Shimura curves. Schiavone and collaborators exhibited an equation for this curve.

Fun fact

We computed $a_{\mathfrak{p}}$ for $\mathrm{Norm}(\mathfrak{p}) \leq 80\,000$, which took several CPU years, to do the computations with 80 digits of precision and finally recognise coefficients.