Genus 3 curves and the inverse Galois problem

Samuele Anni
joint with Pedro Lemos and Samir Siksek

University of Warwick

Modular Forms and Curves of Low Genus: Computational Aspects
ICERM, Providence, 29th September 2015

The inverse Galois problem

Let G be a finite group. Does there exist a Galois extension $K/\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) \cong G$?

For example, let G be S_n, the symmetric group of n letters. Then G is a Galois group over $\mathbb{Q}$. Moreover, for all positive integer n we can realize G as the Galois group of the spliting field $x^n - x - 1$.

Galois representations may answer the inverse Galois problem for finite linear groups.

Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$ and let $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Let A be a principally polarized abelian variety over $\mathbb{Q}$ of dimension d.

Let ℓ be a prime and $A[\ell]$ the ℓ-torsion subgroup:

$$A[\ell] := \{P \in A(\overline{\mathbb{Q}}) \mid [\ell]P = 0\} \cong (\mathbb{Z}/\ell\mathbb{Z})^{2d}.$$

$A[\ell]$ is a $2d$-dimensional $\mathbb{F}_\ell$-vector space, as well as a $G_{\mathbb{Q}}$-module.

The polarization induces a symplectic pairing, the mod ℓ Weil pairing on $A[\ell]$, which is a bilinear, alternating, non-degenerate pairing:

$$\langle\ ,\ \rangle\ :\ A[\ell] \times A[\ell] \to \mu_\ell$$

that is Galois invariant: $\forall \sigma \in G_{\mathbb{Q}}\,,\ \forall v, w \in A[\ell]$

$$\langle \sigma v, \sigma w \rangle = \chi(\sigma) \langle v, w \rangle,$$

where $\chi : G_{\mathbb{Q}} \to \mathbb{F}_\ell^\times$ is the mod ℓ cyclotomic character.

$(A[\ell], \langle\ ,\ \rangle)$ is a symplectic $\mathbb{F}_\ell$-vector space of dimension $2d$. This gives a representation

$$\overline{\rho}_{A,\ell} : G_{\mathbb{Q}} \to \mathrm{GSp}(A[\ell], \langle\ ,\ \rangle) \cong \mathrm{GSp}_{2d}(\mathbb{F}_\ell).$$

Theorem (Serre)

Let A be a principally polarized abelian variety of dimension d, defined over $\mathbb{Q}$. Assume that $d = 2, 6$ or d is odd and, furthermore, assume that $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$. Then there exists a bound B_A such that for all primes $\ell > B_A$ the representation $\overline{\rho}_{A,\ell}$ is surjective.

The conclusion of the theorem is known to be false for general d (counterexample by Mumford for $d = 4$).

Open question

Given d as in the theorem, is there a uniform bound B_d depending only on d, such that for all principally polarized abelian varieties A over $\mathbb{Q}$ of dimension d with $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$, and all $\ell > B_d$, the representation $\overline{\rho}_{A,\ell}$ is surjective?

For elliptic curves an affirmative answer is expected, and this is known as Serre's Uniformity Question.

Much easier for semistable elliptic curves:

Theorem (Serre)

Let $E/\mathbb{Q}$ be a semistable elliptic curve, and $\ell \geq 11$ be a prime. Then $\overline{\rho}_{E,\ell}$ is surjective.

Back to the inverse Galois problem

The Galois representation attached to the ℓ-torsion of the elliptic curve $y^2 + y = x^3 - x$ is surjective for all prime ℓ. This gives a realization $\mathrm{GL}_2(\mathbb{F}_\ell)$ as Galois group for all ℓ.

Let C be the genus 2 hyperelliptic curve given by $y^2 = x^5 - x + 1$ and let J denotes its Jacobian. Dieulefait proved that $\overline{\rho}_{J,\ell}$ is surjective for all odd prime ℓ. This gives a realization $\mathrm{GSp}_4(\mathbb{F}_\ell)$ as Galois group for all odd ℓ.

$\mathrm{GSp}_6(\mathbb{F}_\ell)$

What about genus 3 curves?

Theorem (A., Lemos and Siksek)

Let A be a semistable principally polarized abelian variety of dimension $d \geq 1$ over $\mathbb{Q}$ and let $\ell \geq \max(5, d+2)$ be prime.
Suppose the image of $\overline{\rho}_{A,\ell} : G_{\mathbb{Q}} \to \mathrm{GSp}_{2d}(\mathbb{F}_\ell)$ contains a transvection.
Then $\overline{\rho}_{A,\ell}$ is either reducible or surjective.

Theorem (A., Lemos and Siksek)

Let A be a semistable principally polarized abelian variety of dimension $d \geq 1$ over $\mathbb{Q}$ and let $\ell \geq \max(5, d+2)$ be prime.
Suppose the image of $\overline{\rho}_{A,\ell} : G_{\mathbb{Q}} \to \mathrm{GSp}_{2d}(\mathbb{F}_\ell)$ contains a transvection.
Then $\overline{\rho}_{A,\ell}$ is either reducible or surjective.

Transvection

Definition

Let $(V, \langle\ ,\ \rangle)$ be a finite-dimensional symplectic vector space over $\mathbb{F}_\ell$. A **transvection** *is an element $T \in \mathrm{GSp}(V, \langle\ ,\ \rangle)$ which fixes a hyperplane $H \subset V$.*

Therefore, a transvection is a unipotent element $\sigma \in \mathrm{GSp}(V, \langle\ ,\ \rangle)$ such that $\sigma - I$ has rank 1.

When does $\overline{\rho}_{A,\ell}(G_{\mathbb{Q}})$ contain a transvection?

Let $q \neq \ell$ be a prime and suppose that the following two conditions are satisfied:

- the special fibre of the Néron model for A at q has toric dimension 1;
- $\ell \nmid \#\Phi_q$, where Φ_q is the group of connected components of the special fibre of the Néron model at q.

Then the image of $\overline{\rho}_{A,\ell}$ contains a transvection (Hall).

When does $\overline{\rho}_{A,\ell}(G_{\mathbb{Q}})$ contain a transvection?

Let $C/\mathbb{Q}$ be a hyperelliptic curve of genus d:

$$C : y^2 = f(x)$$

where $f \in \mathbb{Z}[x]$ is a squarefree polynomial.

Let p be an odd prime not dividing the leading coefficient of f such that f modulo p has one root in $\overline{\mathbb{F}}_p$ having multiplicity precisely 2, with all other roots simple.
Then the Néron model of the Jacobian at p has toric dimension 1 (Hall).

Ingredients of the proof of the main theorem

In the proof of this theorem we rely on:

- the classification due to Arias-de-Reyna, Dieulefait and Wiese of subgroups of $\mathrm{GSp}_{2d}(\mathbb{F}_\ell)$ containing a transvection;
- results of Raynaud on the image of the inertia subgroup.

Classification of subgroups of $\mathrm{GSp}_{2d}(\mathbb{F}_\ell)$ with a transvection

Theorem (Arias-de-Reyna, Dieulefait and Wiese)

Let $\ell \geq 5$ be a prime and let V a symplectic $\mathbb{F}_\ell$-vector space of dimension $2d$. Any subgroup G of $\mathrm{GSp}(V)$ which contains a transvection satisfies one of the following:

(I) *There is a non-trivial proper G-stable subspace $W \subset V$.*

(II) *There are non-singular symplectic subspaces $V_i \subset V$ with $i = 1, \dots, h$, of dimension $2m < 2d$ and a homomorphism $\phi : G \to S_h$ such that $V = \oplus_{i=1}^h V_i$ and $\sigma(V_i) = V_{\phi(\sigma)(i)}$ for $\sigma \in G$ and $1 \leq i \leq h$. Moreover, $\phi(G)$ is a transitive subgroup of S_h.*

(III) $\mathrm{Sp}(V) \subseteq G$.

We apply this to $G = \overline{\rho}_{A,\ell}(G_{\mathbb{Q}})$ where A and ℓ are as in the main theorem. If $\mathrm{Sp}_{2d}(\mathbb{F}_\ell) \subseteq G$ then $G = \mathrm{GSp}_{2d}(\mathbb{F}_\ell)$, since the mod ℓ cyclotomic character is surjective.

Inertia and a theorem of Raynaud

Theorem (Raynaud)

Let A be an abelian variety over $\mathbb{Q}$. Let ℓ be a prime of semistable reduction for A. Regard $A[\ell]$ as an I_ℓ-module and let V be a Jordan-Hölder factor of dimension n over $\mathbb{F}_\ell$. Let $\psi_n : I_\ell \to \mathbb{F}_{\ell^n}^\times$ be a fundamental character of level n. Then V has the structure of a 1-dimensional $\mathbb{F}_{\ell^n}$-vector space and the action of I_ℓ on it is given by a character $\varpi : I_\ell \to \mathbb{F}_{\ell^n}^\times$, where $\varpi = \psi_n^{\sum_{i=0}^{n-1} a_i \ell^i}$ with $a_i = 0$ or 1.

Idea of the proof

Denote $\overline{\rho} = \overline{\rho}_{A,\ell}$. Let $G = \overline{\rho}(G_{\mathbb{Q}}) \subseteq \mathrm{GSp}_{2d}(\mathbb{F}_\ell)$.

Since G contains a transvection, it is sufficient to show that the induced case does not arise.

Suppose otherwise. Write $V = \oplus_{i=1}^{h} V_i$ where V_i are non-singular symplectic subspaces of dimension $2m < 2d$. Then there is some $\phi : G \to S_h$ with transitive image such that $\sigma(V_i) = V_{\phi(\sigma)(i)}$. Let

$$\begin{tikzcd} G_{\mathbb{Q}} \arrow[r, "\overline{\rho}"'] \arrow[rr, bend left, "\pi"] & G \arrow[r, "\phi"'] & S_h \end{tikzcd}$$

Idea of the proof

$$\begin{tikzcd} G_{\mathbb{Q}} \arrow[r, "\overline{\rho}"'] \arrow[rr, bend left, "\pi"] & G \arrow[r, "\phi"'] & S_h \end{tikzcd}$$

Let $H = \ker(\pi)$. Then $H = G_K$ for some number field $K/\mathbb{Q}$. Moreover, $\overline{\rho}|_{G_K}$ is reducible as the V_i are stable under the action of G_K.

In the proof we show that for $\ell \geq \max(5, d+2)$ the extension $K/\mathbb{Q}$ is unramified at the finite places, and thus K has discriminant ± 1

$\Rightarrow K = \mathbb{Q} \quad \Rightarrow \quad \pi$ is trivial $\Rightarrow$ contradiction

The bound on ℓ is obtained considering the image of inertia subgroup and applying Raynaud's result.

We now let $A/\mathbb{Q}$ be a **principally polarized abelian threefold**.

Assumptions

(A) A is semistable;

(B) $\ell \geq 5$;

(C) there is a prime q such that the special fibre of the Néron model for A at q has toric dimension 1.

(D) ℓ does not divide $\gcd(\{q \cdot \#\Phi_q : q \in S\})$, where S is the set of primes q satisfying (C) and Φ_q is the group of connected components of the special fibre of the Néron model of A at q.

Under these assumptions the image of $\overline{\rho}_{A,\ell}$ contains a transvection. Then $\overline{\rho}_{A,\ell}$ is either reducible or surjective.

"Algorithm"

Practical method which should, in most cases, produce a small integer B (depending on A) such that for $\ell \nmid B$, the representation $\overline{\rho}_{A,\ell}$ is irreducible and, hence, surjective.

We will apply this procedure to the Jacobian of the hyperelliptic curve:

$$C \ : \ y^2 + (x^4 + x^3 + x + 1)y = x^6 + x^5$$

(look at the glassboard for the computations).

Determinants of Jordan–Hölder factors

Let $\chi : G_{\mathbb{Q}} \to \mathbb{F}_\ell^\times$ denote the mod ℓ cyclotomic character.

We will study the Jordan–Hölder factors W of the $G_{\mathbb{Q}}$-module $A[\ell]$. By the determinant of such a W we mean the determinant of the induced representation $G_{\mathbb{Q}} \to \mathrm{GL}(W)$.

Lemma

Any Jordan–Hölder factor W of the $G_{\mathbb{Q}}$-module $A[\ell]$ has determinant χ^r for some $0 \leq r \leq \dim(W)$.

Weil polynomials

From a prime $p \neq \ell$ of good reduction for A, we will denote by

$$P_p(x) = x^6 + \alpha_p x^5 + \beta_p x^4 + \gamma_p x^3 + p\beta_p x^2 + p^2\alpha_p + p^3 \in \mathbb{Z}[x]$$

the characteristic polynomial of Frobenius $\sigma_p \in G_{\mathbb{Q}}$ at p acting on the Tate module $T_\ell(A)$ (also known as the **Weil polynomial** of A mod p).
The polynomial P_p is independent of ℓ.
Its roots in $\overline{\mathbb{F}}_\ell$ have the form u, v, w, p/u, p/v, p/w.

1-dimensional Jordan–Hölder factors

Let T be a non-empty set of primes of good reduction for A. Let

$$B_1(T) = \gcd(\{p \cdot \#A(\mathbb{F}_p) \ : \ p \in T\}).$$

Lemma

Suppose $\ell \nmid B_1(T)$. The $G_{\mathbb{Q}}$-module $A[\ell]$ does not have any 1-dimensional or 5-dimensional Jordan–Hölder factors.

2-dimensional Jordan–Hölder factors

Lemma

Suppose the $G_{\mathbb{Q}}$-module $A[\ell]$ does not have any 1-dimensional Jordan–Hölder factors, but has either a 2-dimensional or 4-dimensional irreducible subspace U. Then $A[\ell]$ has a 2-dimensional Jordan–Hölder factor W with determinant χ.

Let N be the conductor of A. Let W be a 2-dimensional Jordan–Hölder factor of $A[\ell]$ with determinant χ. The representation

$$\tau : G_{\mathbb{Q}} \to \mathrm{GL}(W) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$$

is odd (as the determinant is χ), irreducible (as W is a Jordan–Hölder factor) and 2-dimensional. By Serre's modularity conjecture (Khare, Wintenberger, Dieulefait, Kisin Theorem), this representation is **modular**:

$$\tau \cong \overline{\rho}_{f,\ell}$$

it is equivalent to the mod ℓ representation attached to a newform f of level $M \mid N$ and weight 2.

Let $\mathcal{O}_f$ be the ring of integers of the number field generated by the Hecke eigenvalues of f. Then there is a prime $\lambda \mid \ell$ of $\mathcal{O}_f$ such that for all primes $p \nmid \ell N$,

$$\mathrm{Tr}(\tau(\sigma_p)) \equiv c_p(f) \pmod{\lambda}$$

where $\sigma_p \in G_{\mathbb{Q}}$ is a Frobenius element at p and $c_p(f)$ is the p-th Hecke eigenvalue of f.

As W is a Jordan–Hölder factor of $A[\ell]$ we see that $x^2 - c_p(f)x + p$ is a factor modulo λ of P_p.

Now let $H_{M,p}$ be the p-th Hecke polynomial for the new subspace $S_2^{\mathrm{new}}(M)$ of cusp forms of weight 2 and level M. This has the form

$$H_{M,p} = \prod (x - c_p(g)),$$

where g runs through the newforms of weight 2 and level M. Write

$$H'_{M,p}(x) = x^d H_{M,p}(x + p/x) \in \mathbb{Z}[x],$$

where $d = \deg(H_{M,p}) = \dim(S_2^{\mathrm{new}}(M))$.

It follows that $x^2 - c_p(f)x + p$ divides $H'_{M,p}$.

Let

$$R(M, p) = \mathrm{Res}(P_p, H'_{M,p}) \in \mathbb{Z}\,,$$

where Res denotes resultant. If $R(M, p) \neq 0$ then we have a bound on ℓ.

The integers $R(M, p)$ can be very large. Given a non-empty set T of rational primes p of good reduction for A, let

$$R(M, T) = \gcd(\{p \cdot R(M, p) \ : \ p \in T\}).$$

In practice, we have found that for a suitable choice of T, the value $R(M, T)$ is fairly small.

Let

$$B_2'(T) = \mathrm{lcm}(R(M, T))$$

where M runs through the divisors of N such that $\dim(S_2^{\mathrm{new}}(M)) \neq 0$, and let

$$B_2(T) = \mathrm{lcm}(B_1(T), B_2'(T))$$

where $B_1(T)$ is given as before.

Lemma

Let T be a non-empty set of rational primes of good reduction for A, and suppose $\ell \nmid B_2(T)$. Then $A[\ell]$ does not have 1-dimensional Jordan–Hölder factors, and does not have irreducible 2- or 4-dimensional subspaces.

We fail to bound ℓ in the above lemma if $R(M, p) = 0$ for all primes p of good reduction.

Here are two situations where this can happen:

- Suppose $A \cong_{\mathbb{Q}} E \times A'$ where E is an elliptic curve and A' an abelian surface. Let $M \mid N$ be the conductor of the elliptic curve, and f to be the newform associated to E by modularity, then $x^2 - c_p(f)x + p$ is a factor of $P_p(x) \Rightarrow R(M, p) = 0$ for all $p \nmid N$.
- Suppose A is of GL_2-type. Let f be the corresponding eigenform, then again $x^2 - c_p(f)x + p$ is a factor of $P_p(x)$ in $\mathcal{O}_f[x]$ $\Rightarrow R(M, p) = 0$ for all $p \nmid N$.

Note that in both these situations $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \neq \mathbb{Z}$.

We expect, but are unable to prove, that if $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$ then there will be primes p such that $R(M, p) \neq 0$.

3-dimensional Jordan–Hölder factors

Lemma

Suppose $A[\ell]$ has Jordan–Hölder filtration $0 \subset U \subset A[\ell]$ where both U and $A[\ell]/U$ are irreducible and 3-dimensional. Moreover, let u_1, u_2, u_3 be a basis for U, and let

$$G_{\mathbb{Q}} \to \mathrm{GL}_3(\mathbb{F}_\ell), \qquad \sigma \mapsto M(\sigma)$$

give the action of $G_{\mathbb{Q}}$ on U with respect to this basis. Then we can extend u_1, u_2, u_3 to a symplectic basis u_1, u_2, u_3, w_1, w_2, w_3 for $A[\ell]$ so that the action of $G_{\mathbb{Q}}$ on $A[\ell]$ with respect to this basis is given by

$$G_{\mathbb{Q}} \to \mathrm{GSp}_6(\mathbb{F}_\ell), \qquad \sigma \mapsto \left(\begin{array}{c|c} M(\sigma) & * \\ \hline \mathbf{0} & \chi(\sigma)(M(\sigma)^t)^{-1} \end{array}\right).$$

$\det(U) = \chi^r$ and $\det(A[\ell]/U) = \chi^s$ where $0 \le r, s \le 3$ with $r + s = 3$.

Lemma

Let p be a prime of good reduction for A. For ease write α, β and γ for the coefficients α_p, β_p, γ_p in the equation of the Weil polynomial. Suppose $p+1 \neq \alpha$. Let

$$\delta = \frac{-p^2\alpha + p^2 + p\alpha^2 - p\alpha - p\beta + p - \beta + \gamma}{(p-1)(p+1-\alpha)} \in \mathbb{Q}, \qquad \epsilon = \delta + \alpha \in \mathbb{Q}.$$

Let $g(x) = (x^3 + \epsilon x^2 + \delta x - p)(x^3 - \delta x^2 - p\epsilon x - p^2) \in \mathbb{Q}[x]$. Write k for the greatest common divisor of the numerators of the coefficients in $P_p - g$. Let

$$K_p = p(p-1)(p+1-\alpha)k.$$

Then $K_p \neq 0$. Moreover, if $\ell \nmid K_p$ then $A[\ell]$ does not have a Jordan–Hölder filtration as in the previous Lemma with $\det(U) = \chi$ or χ^2.

Lemma

Let p be a prime of good reduction for A. Write α, β and γ for the coefficients α_p, β_p, γ_p in the equation of the Weil polynomial. Suppose $p^3+1 \neq p\alpha$. Let $\epsilon' = p\delta' + \alpha \in \mathbb{Q}$ where

$$\delta' = \frac{-p^5\alpha + p^4 + p^3\alpha^2 - p^3\beta - p^2\alpha + p\gamma + p - \beta}{(p^3-1)(p^3+1-p\alpha)} \in \mathbb{Q}\,.$$

Let $g'(x) = (x^3 + \epsilon' x^2 + \delta' x - 1)(x^3 - p\delta' x^2 - p^2\epsilon' x - p^3) \in \mathbb{Q}[x]$. Write k' for the greatest common divisor of the numerators of the coefficients in $P_p - g'$. Let

$$K_p' = p(p^3-1)(p^3+1-p\alpha)k'.$$

Then $K_p' \neq 0$. Moreover, if $\ell \nmid K_p'$ then $A[\ell]$ does not have a Jordan–Hölder filtration as in the above Lemma with $\det(U) = 1$ or χ^3.

Summary

The following theorem summarizes all the lemmas:

Theorem (A., Lemos and Siksek)

Let A and ℓ satisfy conditions (A)–(D). Let T be a non-empty set of primes of good reduction for A. Let

$$B_3(T) = \gcd(\{K_p \; : \; p \in T\}), \qquad B_4(T) = \gcd(\{K'_p \; : \; p \in T\}),$$

where K_p and K'_p are defined in the last two Lemmas. Let

$$B(T) = \operatorname{lcm}(B_2(T), B_3(T), B_4(T)).$$

If $\ell \nmid B(T)$ then $\overline{\rho}_{A,\ell}$ is surjective.

Example

Theorem (A., Lemos and Siksek)

Let $C/\mathbb{Q}$ be the following genus 3 hyperelliptic curve,

$$C \ : \ y^2 + (x^4 + x^3 + x + 1)y = x^6 + x^5.$$

and write J for its Jacobian. Let $\ell \geq 3$ be a prime. Then $\overline{\rho}_{J,\ell}(G_{\mathbb{Q}}) = \mathrm{GSp}_6(\mathbb{F}_\ell)$.

Proof.

For $\ell \geq 5$ we apply the algorithm, look at the glassboard for the computations. For $\ell = 3$, we prove the result by direct computations. $\square$

Genus 3 curves and the inverse Galois problem

Samuele Anni
joint with Pedro Lemos and Samir Siksek

University of Warwick

Modular Forms and Curves of Low Genus: Computational Aspects
ICERM, Providence, 29th September 2015

Thanks!