

HIGHER GENUS CURVES AND THE INVERSE GALOIS PROBLEM

Samuele Anni
joint work with Pedro Lemos and Samir Siksek

University of Warwick

Congreso de Jóvenes Investigadores de la Real Sociedad Matemática Española
Universidad de Murcia, 11th September 2015

- 1 THE INVERSE GALOIS PROBLEM
- 2 ABELIAN VARIETIES AND THE INVERSE GALOIS PROBLEM
- 3 THE MAIN RESULT
- 4 AN “ALGORITHM” FOR THE GENUS 3 CASE

THE INVERSE GALOIS PROBLEM

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

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 splitting field $x^n - x - 1$.

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

- 1 THE INVERSE GALOIS PROBLEM
- 2 ABELIAN VARIETIES AND THE INVERSE GALOIS PROBLEM
- 3 THE MAIN RESULT
- 4 AN “ALGORITHM” FOR THE GENUS 3 CASE

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}_ℓ -vector space, as well as a $G_{\mathbb{Q}}$ -module, where $G_{\mathbb{Q}} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

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

$$\langle \cdot, \cdot \rangle : A[\ell] \times A[\ell] \rightarrow \mathbb{F}_\ell(1)$$

that is Galois invariant. In particular, $(A[\ell], \langle \cdot, \cdot \rangle)$ is a symplectic \mathbb{F}_ℓ -vector space of dimension $2d$.

We obtain a representation

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

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 $\text{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$. Then there exists a bound B_A such that for all primes $\ell > B_A$ the representation $\bar{\rho}_{A,\ell}$ is surjective.

The conclusion of the theorem is known to be false for general d .

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 $\text{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$, 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 $y^2 = x^5 - x + 1$. Dieulefait proved that $\bar{\rho}_{J,\ell}$ is surjective for all odd prime ℓ , where J is the Jacobian of C . This provides 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?

One of the main obstructions to generalize Serre's result for semistable principally polarized abelian varieties is the absence of a satisfactory classification of maximal subgroups of $\mathrm{GSp}_{2d}(\mathbb{F}_\ell)$ for large d .

There is however a classification due to Arias-de-Reyna, Dieulefait and Wiese of subgroups of $\mathrm{GSp}_{2d}(\mathbb{F}_\ell)$ containing a **transvection**.

DEFINITION

Let $(V, \langle \ , \ \rangle)$ be a finite-dimensional symplectic vector space over \mathbb{F}_ℓ . 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 $\sigma - I$ has rank 1.

WHEN DOES $\bar{\rho}_{A,\ell}(G_{\mathbb{Q}})$ 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 $\bar{\rho}_{A,\ell}$ contains 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 for the Jacobian $J(C)$ at p has toric dimension 1.

CLASSIFICATION OF SUBGROUPS OF $\mathrm{GSp}_{2d}(\mathbb{F}_\ell)$ CONTAINING A TRANSVECTION

THEOREM (ARIAS-DE-REYNA, DIEULEFAIT AND WIESE)

Let $\ell \geq 5$ be a prime and let V a symplectic \mathbb{F}_ℓ -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 $\phi : G \rightarrow S_h$ such that $V = \bigoplus_{i=1}^h V_i$ 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) $\mathrm{Sp}(V) \subseteq G$.

- 1 THE INVERSE GALOIS PROBLEM
- 2 ABELIAN VARIETIES AND THE INVERSE GALOIS PROBLEM
- 3 THE MAIN RESULT
- 4 AN “ALGORITHM” FOR THE GENUS 3 CASE

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 $\bar{\rho}_{A,\ell} : G_{\mathbb{Q}} \rightarrow \mathrm{GSp}_{2d}(\mathbb{F}_{\ell})$ contains a transvection. Then $\bar{\rho}_{A,\ell}$ is either reducible or surjective.

In the proof of this theorem we rely on results of Raynaud about the description of the inertia subgroup, as well as the classification of Arias-de-Reyna, Dieulefait and Wiese.

- 1 THE INVERSE GALOIS PROBLEM
- 2 ABELIAN VARIETIES AND THE INVERSE GALOIS PROBLEM
- 3 THE MAIN RESULT
- 4 AN “ALGORITHM” FOR THE GENUS 3 CASE

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

ASSUMPTIONS

- (A) A is semistable;
- (B) there is a prime q such that the special fibre of the Néron model for A at q has toric dimension 1.
- (C) $\ell \geq 5$;
- (D) ℓ does not divide $\gcd(\{q \cdot \#\Phi_q : q \in S\})$, where S is the set of primes q satisfying (B) 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 $\bar{\rho}_{A,\ell}$ contains a transvection. Then, by the Main Theorem, $\bar{\rho}_{A,\ell}$ 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 $\bar{\rho}_{A,\ell}$ is irreducible and, hence, surjective.

DETERMINANTS OF JORDAN–HÖLDER FACTORS

Let $\chi : G_{\mathbb{Q}} \rightarrow \mathbb{F}_{\ell}^{\times}$ 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 $G_{\mathbb{Q}} \rightarrow \mathrm{GL}(W)$.

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

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

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 $A \bmod p$). 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

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

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**:

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

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

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

Let

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

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

$$B'_2(T) = \text{lcm}(R(M, T))$$

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

$$B_2(T) = \text{lcm}(B_1(T), B'_2(T))$$

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 is isogenous over \mathbb{Q} to $E \times A'$ where E is an elliptic curve and A' an abelian surface. If we take $M \mid N$ to 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 $P_p(x)$ in $\mathbb{Z}[x]$. Thus the resultant $R(M, p) = 0$ for all $p \nmid N$.
- Suppose the abelian threefold 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 $\mathcal{O}_f[x]$, and so the resultant $R(M, p) = 0$ for all $p \nmid N$.

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

We expect, but are unable to prove, that if $\text{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$ 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

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

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

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

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

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

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

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

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

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

If $\ell \nmid B(T)$ then $\bar{\rho}_{A,\ell}$ 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 $\bar{\rho}_{J,\ell}(G_{\mathbb{Q}}) = \mathrm{GSp}_6(\mathbb{F}_{\ell})$.

We will prove the theorem only for $\ell \geq 5$.

The model given above for C has good reduction at 2.

Let J be the Jacobian of C . This has conductor $N = 8907 = 3 \times 2969$.
As N is squarefree, the Jacobian J is semistable.

Completing the square, we see that the curve C has the following 'simplified' Weierstrass model.

$$y^2 = x^8 + 2x^7 + 5x^6 + 6x^5 + 4x^4 + 2x^3 + x^2 + 2x + 1 = f(x).$$

$$f \equiv (x + 1)(x + 2)^2(x^2 + x + 2)(x^3 + 2x^2 + 2x + 2) \pmod{3}$$

$$f \equiv (x + 1)(x + 340)(x + 983)^2(x^2 + x + 1)(x^2 + 663x + 1350) \pmod{2969}.$$

f has precisely one double root in $\overline{\mathbb{F}}_3$ and one double root in $\overline{\mathbb{F}}_{2969}$ with all other roots simple, we see that the Néron models for J at 3 and 2969 have special fibres with toric dimension 1.

$$\#\Phi_3 = \#\Phi_{2969} = 1.$$

Thus the image of $\bar{\rho}_{J,\ell}$ contains a transvection for all $\ell \geq 3$.

We now suppose $\ell \geq 5$.

By the Main Theorem we know that $\bar{\rho}_{J,\ell}$ is either reducible or surjective.

Take our chosen set of primes of good reduction to be $T = \{2, 5, 7\}$.

We note that

$$\#J(\mathbb{F}_2) = 2^5, \quad \#J(\mathbb{F}_5) = 2^7, \quad \#J(\mathbb{F}_7) = 2^6 \times 7.$$

It follows that $J[\ell]$ does not have 1- or 5-dimensional Jordan–Hölder factors.

Next we consider the existence of 2- or 4-dimensional irreducible subspaces. The possible values $M \mid N$ such that $S_2^{\text{new}}(M) \neq 0$ are $M = 2969$ and $M = 8907$, where the dimensions are 247 and 495 respectively. The resultants $R(M, p)$ are too large to reproduce here, for example, $R(8907, 7) \sim 1.63 \times 10^{2344}$.

However,

$$R(M, T) = \gcd(2 \cdot R(M, 2), 5 \cdot R(M, 5), 7 \cdot R(M, 7)) = \begin{cases} 2^4 & M = 2969, \\ 2^{22} & M = 8907. \end{cases}$$

It follows that $J[\ell]$ does not have 2- or 4-dimensional irreducible subspaces.

It remains to eliminate the possibility of a Jordan–Hölder filtration $0 \subset U \subset J[\ell]$ where both U and $J[\ell]/U$ are 3-dimensional. In the notation of the previous Lemmas

$$K_2 = 14, \quad K_5 = 6900, \quad K_7 = 83202.$$

Then $\gcd(K_2, K_5, K_7) = 2$, so we eliminate the case where $\det(U) = \chi$ or χ^2 . Moreover,

$$K'_2 = 154490, \quad K'_5 = 15531373270380, \quad K'_7 = 10908656905042386.$$

Then $\gcd(K'_2, K'_3, K'_7) = 2$, so we exclude the case where $\det(U) = 1$ or χ^3 . It follows that $\bar{\rho}_{J,\ell}$ is irreducible and hence surjective for all $\ell \geq 5$.

HIGHER GENUS CURVES AND THE INVERSE GALOIS PROBLEM

Samuele Anni

joint work with Pedro Lemos and Samir Siksek

University of Warwick

Congreso de Jóvenes Investigadores de la Real Sociedad Matemática Española
Universidad de Murcia, 11th September 2015

Thanks!