The inverse Galois problem for symplectic groups

Valentijn Karemaker (University of Pennsylvania)

Joint with S. Arias-de-Reyna, C. Armana, M. Rebolledo, L. Thomas and N. Vila

Joint Mathematics Meetings, Atlanta

January 7, 2017

Inverse Galois Problem (IGP)

The IGP asks:

IGP

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

- Hilbert (1897): S_n, A_n for all n
- Shafarevich (1954): All finite solvable groups

Galois representations may answer IGP for finite linear groups.

Goal

Obtain realisations of $\mathrm{GSp}(6, \mathbb{F}_\ell)$ as a Galois group over $\mathbb{Q}$.

We consider Galois representations attached to abelian varieties.

Abelian varieties

Let $A/\mathbb{Q}$ be a principally polarised abelian variety of dimension g.

$A(\bar{\mathbb{Q}})$ is a group. Let ℓ be a prime.
Torsion points $A[\ell] := \{P \in A(\bar{\mathbb{Q}}) : [\ell]P = 0\} \cong (\mathbb{Z}/\ell\mathbb{Z})^{2g}$.
$G_{\mathbb{Q}}$ acts on $A[\ell]$, yielding a Galois representation

$$\rho_{A,\ell} : G_{\mathbb{Q}} \to GL(A[\ell]) \cong \mathrm{GL}(2g, \mathbb{F}_\ell).$$

The action is compatible with the (symplectic) Weil pairing, hence

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

Surjective $\rho_{A,\ell}$ solve IGP for general symplectic groups.

Surjective $\rho_{A,\ell}$

The image of $\rho_{A,\ell}$ in $\mathrm{GSp}(2g, \mathbb{F}_\ell)$ depends on A and ℓ.

Let $g = 3$. We ask the following questions:

1. Given a principally polarised abelian variety $A/\mathbb{Q}$, for which primes ℓ is $\rho_{A,\ell}$ surjective?
2. Given a prime ℓ, how do we construct an abelian variety $A/\mathbb{Q}$ such that $\rho_{A,\ell}$ is surjective?

We answer Question 1 in our WIN-E Proceedings paper:

Theorem 1 (AdR-A-K-R-T-V)

For a suitable principally polarised given $A/\mathbb{Q}$, there is a numerical algorithm which realises $\mathrm{GSp}(6, \mathbb{F}_\ell)$ as the image of $\rho_{A,\ell}$ for an explicit list of prime numbers ℓ.

In this talk, we explain our solution to Question 2.

Sufficient condition for surjectivity of $\rho_{A,\ell}$

Proposition

If $\mathrm{Im}(\rho_{A,\ell}) \supset \mathrm{Sp}(A[\ell], \langle \cdot, \cdot \rangle)$ then $\mathrm{Im}(\rho_{A,\ell}) = \mathrm{GSp}(A[\ell], \langle \cdot, \cdot \rangle)$.

PROOF: We have an exact sequence

$$1 \to \mathrm{Sp}(A[\ell], \langle \cdot, \cdot \rangle) \to \mathrm{GSp}(A[\ell], \langle \cdot, \cdot \rangle) \xrightarrow{m} \mathbb{F}_\ell^\times \to 1$$

where $m : A \mapsto a$ when $\langle Av_1, Av_2 \rangle = a\langle v_1, v_2 \rangle$ for all $v_1, v_2 \in A[\ell]$. $G_\mathbb{Q}$ acts such that $m|_{\mathrm{Im}(\rho_{A,\ell})} = \chi_\ell$, the **surjective** mod ℓ cyclotomic character. $\square$

Structure of *Sp*

Let V be a finite-dimensional vector space over $\mathbb{F}_\ell$, endowed with a symplectic pairing $\langle\cdot,\cdot\rangle : V \times V \to \mathbb{F}_\ell$.

A **transvection** is an element $T \in \mathrm{GSp}(V, \langle\cdot,\cdot\rangle)$ which fixes a hyperplane $H \subset V$.

Theorem (Arias-de-Reyna & Kappen, 2013)

Let $\ell \geq 5$ and let $G \subset \mathrm{GSp}(V, \langle\cdot,\cdot\rangle)$ be a subgroup containing both a non-trivial transvection and an element of non-zero trace whose characteristic polynomial is irreducible. Then $G \supset \mathrm{Sp}(V, \langle\cdot,\cdot\rangle)$.

Main result

Theorem 2 (AdR-A-K-R-T-V)

Let $\ell \geq 13$ be a prime number.
There is a family of projective genus 3 curves $C/\mathbb{Q}$ for which

$$\mathrm{Im}(\rho_{\mathrm{Jac}(C),\ell}) = \mathrm{GSp}(6, \mathbb{F}_\ell).$$

Namely, for any distinct odd primes $p, q \neq \ell$ with $q > 1.82\ell^2$, there exist $f_p \in \mathbb{F}_p[x, y]$ and $f_q \in \mathbb{F}_q[x, y]$ such that any $f \in \mathbb{Z}[x, y]$ satsifying

$$f \equiv f_q \pmod{q} \quad \text{and} \quad f \equiv f_p \pmod{p^3},$$

defines such a curve $C/\mathbb{Q}$: $f(x, y) = 0$.

Main ideas for Theorem 2

p and q are auxiliary primes.

$C_p/\mathbb{F}_p\colon f_p(x,y)=0$ yields a transvection,

$C_q/\mathbb{F}_q\colon f_q(x,y)=0$ yields an element of irreducible characteristic polynomial and non-zero trace.

Simultaneously (Chinese remainder theorem) lift f_p and f_q to $f/\mathbb{Z}$.

$C/\mathbb{Q}\colon f(x,y)=0$ is such that $\mathrm{Jac}(C)$ has surjective $\rho_{\mathrm{Jac}(C),\ell}$.

Finding transvections: Hall's condition

Proposition (Hall, 2011)

Let $A/\mathbb{Q}$ be a principally polarised g-dimensional abelian variety. If the Néron model of $A/\mathbb{Z}$ has a semistable fibre at p with toric dimension 1, and if $p \nmid \ell$ and $\ell \nmid |\Phi_p|$, then $\mathrm{Im}(\rho_{A,\ell})$ contains a transvection T.

We may take T to be the image of a generator of the inertia subgroup of any prime in $\mathbb{Q}(A[\ell])$ lying above p.

Finding transvections: Explicit models

Let $f_p(x, y) \in \mathbb{Z}_p[x, y]$ be one of the following:

(H) $y^2 - x(x-p)m(x)$,
$m(x) \in \mathbb{Z}_p[x]$ of degree 5 or 6 with simple $\neq 0$ roots mod p;

(Q) $x^4 + y^4 + x^2 - y^2 + px$.

Then $C_p/\mathbb{Q}_p\colon f_p(x, y) = 0$ is a smooth projective geometrically connected genus 3 curve.

It has a semistable fibre at p with one ordinary node of thickness 2. Hence $|\Phi_p| = 2$.

Toric dimension $=$ rank of $H^1(\Gamma(C_{\overline{\mathbb{F}}_p}), \mathbb{Z}) = 1$.

Hall's result implies: For $2, p, \ell$ distinct primes, $\mathrm{Im}(\rho_{\mathrm{Jac}(C_p),\ell})$ contains a transvection.

Finding irr. characteristic polynomial of non-zero trace

Theorem 3 (AdR-A-K-R-T-V)

Let $\ell \geq 13$ be a prime number.
For each prime $q > 1.82\ell^2$, there exist a smooth geometrically connected curve $C_q/\mathbb{F}_q$ of genus 3,
whose Jacobian $\mathrm{Jac}(C_q)$ is a 3-dimensional ordinary absolutely simple abelian variety over $\mathbb{Q}$ such that the characteristic polynomial of its Frobenius endomorphism is irreducible moulo ℓ and has non-zero trace.

Weil q-polynomials

Fix a prime ℓ.

A Weil q-polynomial is a monic polynomial $P_q \in \mathbb{Z}[t]$ of even degree, whose complex roots all have absolute value $\sqrt{q}$.

Any degree 6 Weil q-polynomial will look like

$$P_q(t) = t^6 + at^5 + bt^4 + ct^3 + qbt^2 + q^2at + q^3.$$

Obtaining an abelian variety

$$\boxed{\text{Weil poly. } P_q} \xrightarrow{\text{(Honda-Tate)}} \boxed{A/\mathbb{Q}} \xrightarrow{\text{(Oort-Ueno, Serre)}} \boxed{\mathrm{Jac}(C_q)}$$

degree 6	dim. 3	genus 3
ordinary	ordinary	“good”
irr./$\mathbb{Z}$	abs. simple	geom. irr.
irr. $\mod \ell$,	Frob irr.,	idem
$a \not\equiv 0 \mod \ell$	$\neq 0$ trace	

End of proof: existence of suitable P_q

Proposition (AdR-A-K-R-T-V)

For any $\ell \geq 13$ and $q > 1.82\ell^2$, there exists such a Weil polynomial $P_q \in \mathbb{Z}[t]$, with $|a|, |b|, |c| < \frac{\ell-1}{2}$.

This proves Theorem 3, hence Theorem 2.

- Arias-de-Reyna, Armana, Karemaker, Rebolledo, Thomas, Vila (2014)
  Galois representations and symplectic Galois groups over $\mathbb{Q}$
  Proceedings of Women in Numbers Europe - Research Directions in Number Theory
- Arias-de-Reyna, Armana, Karemaker, Rebolledo, Thomas, Vila (2016)
  Large Galois images for Jacobian varieties of genus 3 curves
  Acta Arithmetica 174(4), 339 – 366.

Thank you for your attention!