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 \( \text{Gal}(L/\mathbb{Q}) \cong G \)?

- 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 \( \text{GSp}(6, \mathbb{F}_\ell) \) 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 $g$.

$A(\overline{\mathbb{Q}})$ is a group. Let $\ell$ be a prime.

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

$G_{\mathbb{Q}}$ acts on $A[\ell]$, yielding a Galois representation

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

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

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

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

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

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

1. Given a principally polarised abelian variety $A/\mathbb{Q}$, for which primes $\ell$ is $\rho_{A,\ell}$ surjective?
2. Given a prime $\ell$, 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 $\text{GSp}(6, \mathbb{F}_\ell)$ as the image of $\rho_{A,\ell}$ for an explicit list of prime numbers $\ell$.

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

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

PROOF: We have an exact sequence

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

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 \( m|_{\text{Im}(\rho_{A,\ell})} = \chi_\ell \), the \textbf{surjective} mod \( \ell \) cyclotomic character. \( \square \)
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 $T \in \text{GSp}(V, \langle \cdot , \cdot \rangle)$ which fixes a hyperplane $H \subset V$.

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

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

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

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 $f \in \mathbb{Z}[x, y]$ satisfying

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

defines such a curve $C/\mathbb{Q}$: $f(x, y) = 0$. 
Main ideas for Theorem 2

$p$ and $q$ are auxiliary primes.

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

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

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

$C/\mathbb{Q} : f(x, y) = 0$ is such that $\text{Jac}(C)$ has surjective $\rho_{\text{Jac}(C),\ell}$. 
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 $\text{Im}(\rho_{A,\ell})$ 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 $C_p/\mathbb{Q}_p : f_p(x, y) = 0$ 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 $H^1(\Gamma(C_{\overline{F}_p}), \mathbb{Z}) = 1.$

Hall’s result implies: For 2, $p, \ell$ distinct primes, $\text{Im}(\rho_{\text{Jac}(C_p), \ell})$ 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 \( C_q/F_q \) of genus 3, whose Jacobian \( \text{Jac}(C_q) \) is a 3-dimensional ordinary absolutely simple abelian variety over \( \mathbb{Q} \) such that the characteristic polynomial of its Frobenius endomorphism is irreducible modulo \( \ell \) and has non-zero trace.
Weil $q$-polynomials

Fix a prime $\ell$.

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

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

\[
\begin{align*}
\text{Weil poly. } P_q & \overset{\text{(Honda-Tate)}}{\longrightarrow} A/\mathbb{Q} & \overset{\text{(Oort-Ueno, Serre)}}{\longrightarrow} \text{Jac}(C_q) \\
dergree 6 & \quad \text{dim. 3} & \text{genus 3} \\
\text{ordinary} & \quad \text{ordinary} & \text{“good”} \\
\text{irr.}/\mathbb{Z} & \quad \text{abs. simple} & \text{geom. irr.} \\
\text{irr. mod } \ell, & \quad \text{Frob irr.}, & \text{idem} \\
a \not\equiv 0 \mod \ell & \quad \not= 0 \text{ trace}
\end{align*}
\]
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

Thank you for your attention!