Galois representations and symplectic Galois groups over $\mathbb{Q}$

Valentijn Karemaker (UU)

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

Diamant Symposium, Arnhem

June 6, 2014

Inverse Galois Prolem (IGP)

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

Conjecture

Every finite group G occurs as a Galois group over $\mathbb{Q}$.

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

Absolute Galois group

Let $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group of $\mathbb{Q}$.
It is a profinite group, compact under the profinite topology.
Finite quotients of $G_{\mathbb{Q}}$ correspond to finite Galois extensions $L/\mathbb{Q}$.

IGP reformulated

What are the finite quotients of $G_{\mathbb{Q}}$?

Galois representations

A Galois representation is a continuous homomorphism

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}(n, R)$$

where R is a topological ring.

If R is discrete (e.g. $R = \mathbb{F}_q$), then $\rho(G_{\mathbb{Q}}) \cong \mathrm{Gal}(\bar{\mathbb{Q}}^{\ker(\rho)}/\mathbb{Q})$ is finite.

Hence, (surjective) Galois representations may answer IGP for finite linear groups.

Some known results

Consider the action of $G_{\mathbb{Q}}$ on algebro-geometric objects.

- Serre (1972): Elliptic curves $E/\mathbb{Q}$ (without CM) $\Rightarrow \mathrm{GL}(2, \mathbb{F}_\ell)$
- Ribet (1975): Modular forms (cuspidal Hecke eigenforms of even weight) $\Rightarrow \mathrm{PGL}(2, \mathbb{F}_{\ell^r})$ (r odd), $\mathrm{PSL}(2, \mathbb{F}_{\ell^r})$ (r even)
- Zywina (2013): Elliptic surface $\Rightarrow \mathrm{PSL}(2, \mathbb{F}_\ell)$ for all $\ell > 3$
- Dieulefait & Vila (2004): Smooth projective surfaces $\Rightarrow \mathrm{PSL}(3, \mathbb{F}_\ell)$, $\mathrm{PSU}(3, \mathbb{F}_\ell)$, $\mathrm{SL}(3, \mathbb{F}_\ell)$, $\mathrm{SU}(3, \mathbb{F}_\ell)$
- ...

We consider Galois representations attached to abelian varieties.

Abelian varieties

Let A be an abelian variety of dimension n, defined over $\mathbb{Q}$.

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

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

The Weil pairing e_ℓ is a perfect pairing

$$e_\ell : A[\ell] \times A^\vee[\ell] \to \mu_\ell(\bar{\mathbb{Q}}) \cong \mathbb{F}_\ell.$$

A is principally polarised when there exists an isogeny $\lambda : A \to A^\vee$ of degree 1. In this case,

$$e_\ell : A[\ell] \times A[\ell] \to \mathbb{F}_\ell : (P, Q) \mapsto e_\ell(P, \lambda(Q)).$$

General symplectic group

Let V be a $2n$-dimensional $\mathbb{F}_\ell$-vector space. A pairing $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{F}_\ell$ is called symplectic when it is skew-symmetric and non-degenerate.

We define the symplectic group

$$\mathrm{Sp}(V, \langle \cdot, \cdot \rangle) := \{M \in \mathrm{GL}(V) : \forall v_1, v_2 \in V, \langle Mv_1, Mv_2 \rangle = \langle v_1, v_2 \rangle\}$$

and the general symplectic group

$$\mathrm{GSp}(V, \langle \cdot, \cdot \rangle) := \{M \in \mathrm{GL}(V) : \exists m \in \mathbb{F}_\ell^\times \text{ s.t. } \forall v_1, v_2 \in V, \\ \langle Mv_1, Mv_2 \rangle = m \langle v_1, v_2 \rangle\}.$$

Symplectic image

The Weil pairing is a symplectic pairing.
Since $G_{\mathbb{Q}}$ acts on $\mu_\ell(\bar{\mathbb{Q}}) \cong \mathbb{F}_\ell$ through the mod ℓ cyclotomic character χ_ℓ, the action of $G_{\mathbb{Q}}$ on $A[\ell]$ is compatible with the Weil pairing:

$$\langle \rho(\sigma)(P), \rho(\sigma)(Q) \rangle = \chi_\ell(\sigma)\langle P, Q \rangle$$

for $\sigma \in G_{\mathbb{Q}}$, $P, Q \in A[\ell]$.
Hence, $\rho_{A,\ell}$ has a symplectic image:

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

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

Surjective $\rho_{A,\ell}$

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

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?

Some known results

Theorem (Serre, 1985)

Let A be a principally polarised abelian variety of dimension n, defined over a number field K. Assume that $\mathrm{End}_{\bar{K}}(A) = \mathbb{Z}$ and that $n = 2, 6$ or odd. Then there exists a bound B_A such that $\rho_{A,\ell}$ is surjective for all $\ell > B_A$.

Theorem (Dieulefait, 2002)

Let A be a principally polarised abelian surface (so $n = 2$), defined over $\mathbb{Q}$. Assume that $\mathrm{End}_{\bar{\mathbb{Q}}}(A) = \mathbb{Z}$. Then there is an explicit algorithm to find a finite set of primes containing those for which $\rho_{A,\ell}$ is not surjective.

Theorem (Arias-de-Reyna & Vila, 2010)

Given a prime $\ell > 3$, one can construct an abelian surface $A/\mathbb{Q}$ such that $\rho_{A,\ell}$ is surjective, by choosing it to be the Jacobian of a suitable genus 2 curve.

Our main results

We have treated the case of $n = 3$, $\rho_{A,\ell} : G_{\mathbb{Q}} \to \mathrm{GSp}(6, \mathbb{F}_\ell)$.

Theorem (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.

Question 2: A theoretical construction of $A/\mathbb{Q}$ is in progress.

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

Recall that $\mathrm{GSp}(2n, \mathbb{F}_\ell) \cong \mathrm{GSp}(A[\ell], \langle \cdot, \cdot \rangle)$ and that $G_\mathbb{Q}$ acts through the mod ℓ cyclotomic character.

Proposition

When $\mathrm{Im}(\rho_{A,\ell}) \supset \mathrm{Sp}(A[\ell], \langle \cdot, \cdot \rangle)$ 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 $v_1, v_2 \in A[\ell]$. Restricting m to $\mathrm{Im}(\rho_{A,\ell})$ yields the cyclotomic mod ℓ character, which is surjective. $\square$

Structure of Sp, transvections

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 $G \supset \mathrm{Sp}(V, \langle\cdot,\cdot\rangle)$.

Finding transvections: Hall's condition

Proposition (Hall, 2011)

Let A be a principally polarised n-dimensional abelian variety, defined over a number field K.
Suppose that there exists a finite extension L/K so that the Néron model of A/L over $\mathcal{O}_L$ has a semistable fibre with toric dimension 1, at $\mathfrak{p}$ say.
Let ℓ be a prime such that $\ell \nmid (\tilde{A}_{\mathfrak{p}} : \tilde{A}^0_{\mathfrak{p}})$ and $\mathfrak{p} \nmid \ell$.
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 $K(A[\ell])$ lying over $\mathfrak{p}$.

Hall's condition

There exists a finite extension L/K so that the Néron model of A/L over $\mathcal{O}_L$ has a semistable fibre with toric dimension 1.

Irreducible characteristic polynomial

Consider $\rho_{A,\ell}(\mathrm{Frob}_q)$, for q a prime of good reduction for A.

For any $\tilde{\alpha} \in \mathrm{End}(A[\ell])$, induced by $\alpha \in \mathrm{End}(A)$, we have

$$\mathrm{CharPoly}(\tilde{\alpha}) = \mathrm{CharPoly}(\alpha) \mod \ell.$$

Now $\rho_{A,\ell}(\mathrm{Frob}_q) \in \mathrm{End}(A[\ell])$ is induced by the Frobenius endomorphism of the reduction $\phi_q \in \mathrm{End}(A/\mathbb{F}_q)$ (induced by $\phi_q \in G_{\mathbb{F}_q}$).
Hence,

$$\mathrm{CharPoly}(\rho_{A,\ell}(\mathrm{Frob}_q)) = \mathrm{CharPoly}(\phi_q) \mod \ell.$$

Note: For $A = \mathrm{Jac}(C)$, simply count $|C(\mathbb{F}_{q^r})|$ for $1 \leq r \leq n$.

Given A, find ℓ: Example

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

$$f(x) = x^2(x-1)(x+1)(x-2)(x+2)(x-3) + 7(x-28) \in \mathbb{Z}[x].$$

C is a hyperelliptic curve of genus 3. Let $A = \mathrm{Jac}(C)$.

By construction, A satisfies Hall's condition at $p = 7$.
We compute $(\tilde{A}_7 : \tilde{A}_7^0) = 2$.

So for $\ell \geq 11$, we have transvections.
Now for $\ell \neq q$, check whether $\rho_{A,\ell}(\mathrm{Frob}_q)$ has irreducible characteristic polynomial over $\mathbb{F}_\ell$ and non-zero trace.

Given A, find ℓ: Example

Computations in SAGE give a list of primes ℓ for a fixed q ($q = 53$ say).

We use that $\mathrm{CharPoly}(\rho_{A,\ell}(\mathrm{Frob}_q)) = \mathrm{CharPoly}(\phi_q) \mod \ell$, where ϕ_q is the Frobenius endomorphism of the reduction of C at q.

These primes form a subset with a Dirichlet density of $\frac{1}{6}$.
The Galois group G of $\mathrm{CharPoly}(\mathrm{Frob}_{53})$ is $C_2 \wr S_3$, $|G| = 48$.

To find all $11 \leq \ell \leq B$, we vary q. Our computations have checked up to $B = 100.000$.

Conclusion

For this $A/\mathbb{Q}$, our algorithm realises $\mathrm{GSp}(6, \mathbb{F}_\ell)$ as the image of $\rho_{A,\ell}$ for all $11 \leq \ell \leq 100.000$. $\square$

Weil polynomials - *work in progress*

Fix a prime ℓ.

A Weil polynomial is a monic polynomial with integer coefficients, whose roots come in complex conjugate pairs and all have absolute value $\sqrt{q}$ for some q.

$\mathrm{CharPoly}(\phi_q)$, for $A/\mathbb{F}_q$, is a Weil polynomial. When $n = 3$, it has degree 6.

Conversely, we may start with such a polynomial:

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

and find q, a, b, c for which it is an irreducible Weil polynomial which stays irreducible after reducing modulo ℓ.

Obtaining an abelian variety - *work in progress*

Suppose we have found a suitable $P_q(t)$.

Theorem (Honda & Tate, 1968)

There is a bijection between the set of $\mathbb{F}_q$-isogeny classes of simple abelian varieties over $\mathbb{F}_q$ and Weil polynomials for q.

Hence, we obtain a three-dimensional abelian variety $A/\mathbb{F}_q$ such that $\mathrm{CharPoly}(\mathrm{Frob}_q) = P_q(t)$.

Theorem (Howe, 1995)

When $q \nmid c$, then $P_q(t)$ is an ordinary Weil polynomial, corresponding to a simple ordinary abelian variety over $\mathbb{F}_q$. When the abelian variety is odd-dimensional, it is isogenous to a principally polarised abelian variety.

So we may assume that $A/\mathbb{F}_q$ is principally polarised.

Jacobians of genus 3 curves - *work in progress*

Theorem (Oort & Ueno, 1973)

Any principally polarised abelian variety of dimension 3 over $\mathbb{F}_q$ is isogenous to the Jacobian of a curve C of genus 3, defined over a finite extension $L/\mathbb{F}_q$.

When A is absolutely simple, C is defined over $\mathbb{F}_q$.

Because C is a genus 3 curve, it is either a hyperelliptic curve or a smooth plane quartic curve.

We now lift C, so that C and $A = \mathrm{Jac}(C)$ are defined over $\mathbb{Q}$, in fact over $\mathbb{Z}$.

Imposing Hall's condition - *work in progress*

For surjective $\rho_{A,\ell}$ it remains to find a transvection in the image. Recall:

Hall's condition

There exists a finite extension L/K so that the Néron model of A/L over $\mathcal{O}_L$ has a semistable fibre with toric dimension 1.

Suppose that C has semi-stable reduction. (Always true over some $K/\mathbb{Q}$.)

Let $\mathcal{C}/\mathbb{Z}$ be the minimal regular model of C. Then $\mathrm{Pic}^0_{\mathcal{C}/\mathbb{Z}}$ is (the identity component of) a Néron model for $\mathrm{Jac}(C) = A$. Its fibres are semi-stable curves over finite fields.

A fibre has toric dimension 1 exactly when it has a single node.
So we can construct $C/\mathbb{Z}$ in such a way that it has a reduction with one node, using the Chinese Remainder Theorem.

Then $\mathrm{Im}(\rho_{A,\ell}) = \mathrm{GSp}(6, \mathbb{F}_\ell)$, answering Question 2.