Galois representations and automorphic forms

Michael Harris

Columbia University,
Institut de Mathématiques de Jussieu

Yale, November 2013

Galois theory

Courses in Galois theory typically calculate a very short list of Galois groups of polynomials in $\mathbb{Q}[X]$.

Cyclotomic fields. The Galois group of the cyclotomic polynomial $P(X) = X^n - 1$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$.

$$(\mathbb{Z}/n\mathbb{Z})^\times \ni a \mapsto \sigma_a : \quad \sigma_a(\zeta) = \zeta^a, P(\zeta) = 0.$$

Solving by radicals. The Galois group of the polynomial $Q(X) = X^n - a$ is a subgroup of $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$.

All other examples are deep!

Kronecker's *Jugendtraum*

Kronecker's Jugendtraum (Hilbert's 12th problem): find explicit generators of abelian Galois extensions of number fields and expressions of Galois action (as for cyclotomic fields above).

Short list: complex multiplication (Kronecker, Weber, Shimura-Taniyama)

The Langlands program provides a systematic way to enlarge this list to *nonabelian* extensions.

Galois groups are attached, not to polynomials, but to the geometry of Shimura varieties.

(Langlands explicitly cited the Jugendtraum in this connection, but Wikipedia is not convinced:
"serious doubts remain concerning [the Langlands program's] *import for the question that Hilbert asked."*)

Number theory vs. analysis

The Langlands reciprocity conjectures – one part of the full Langlands program – unite two branches of mathematics that have little obvious in common.

Galois representations – linear representations of $\Gamma_{\mathbb{Q}} := Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ and its subgroups of finite index – are structures that organize the symmetries of roots of polynomials in $\mathbb{Q}[X]$.

Automorphic representations are structures that organize solutions to certain families of differential equations (invariant laplacians) and difference equations (Hecke operators) with a high degree of symmetry.

Goal: to unite the two structures by relating them both to *geometry*.

Classical modular forms

The group $SL(2,\mathbb{Z})$ acts on the upper half plane $\mathfrak{H} \subset \mathbb{C}$ by linear fractional transformations:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = \frac{az+b}{cz+d}.$$

The modular curve of level N is the Riemann surface

$$M(N) = \Gamma(N)\backslash\mathfrak{H}$$

where

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

Classical modular forms

Classical modular forms $f : \mathfrak{H} \to \mathbb{C}$ of level N are the most familiar automorphic forms.
They are solutions to the differential equations (eigenfunctions of hyperbolic laplacian) that satisfy this symmetry:

$$f(\frac{az+b}{cz+d}) = (cz+d)^k f(z), \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(N)$$

Because $\Gamma(N)$ is a congruence subgroup, there are also (highly symmetric) *difference equations* (Hecke operators).

Transcendental vs. algebraic

Guiding principle: transcendental structures that look algebraic come from algebra.
Example:

- Representations of Lie groups: Invariant differential equations on semisimple Lie groups with *integral* parameters have polynomial solutions.
- Hodge conjecture...
- Fontaine-Mazur conjectures: Irreducible representations of the Galois group of a number field F that look geometric come from algebraic varieties over F.

Galois representations

The Galois group $\Gamma_{\mathbb{Q}}$ is profinite and is compact for a totally disconnected topology.

One side of the correspondence consists in *continuous representations*

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

R an algebraically closed field (e.g. $\mathbb{C}$, or $\overline{\mathbb{F}}_p$, or $\bar{\mathbb{Q}}_p$).

In the latter case, (if the image is contained in $\mathbb{Q}_p$) for each $r \geq 0$, there is a representation

$$\rho_{X,r} : \Gamma_{\mathbb{Q}} \to GL(n, \mathbb{Z}/p^r\mathbb{Z})$$

which of course has finite image, and ρ_X is the unique representation whose reduction mod p^r is $\rho_{X,r}$ for all r.

One assumes ρ to be *semisimple* (completely reducible).
$\Rightarrow \rho$ is determined up to equivalence by the characteristic polynomials of a dense subset of its image. Even the *traces* of a dense set of elements suffice.

Galois representations

For $n = 1$, classification of $\rho : \Gamma_F = Gal(\overline{\mathbb{Q}}/F) \to GL(1, R) \Leftrightarrow$ classification of *abelian extensions* of F.
Automorphic classification is *class field theory*, a complete theory that focuses on the Galois group (not polynomials).
For general n, restrict the class of ρ.
Usually one assumes ρ is what is called *geometric*.

ℓ-adic cohomology

The only general methods to define representations of $\Gamma_{\mathbb{Q}}$ – to determine the structure of Galois groups – come from algebraic geometry.

Let X be an algebraic variety over $\mathbb{Q}$ (set of solutions of polynomials in several variables with $\mathbb{Q}$-coefficients).

For the next few slides the prime is called ℓ (we reserve p for other purposes). Then (Grothendieck)

$$H^*(X(\mathbb{C}), \mathbb{Q}_\ell) := \varprojlim H^*(X(\mathbb{C}), \mathbb{Z}/\ell^r\mathbb{Z}) \otimes \mathbb{Q}$$

is a finite-dimensional representation space for $\Gamma_{\mathbb{Q}}$.

A representation ρ of $\Gamma_{\mathbb{Q}}$ is *geometric* if it is an irreducible constituent of some $H^*(X(\mathbb{C}), \mathbb{Q}_\ell)$.

For example, if X is a non-singular cubic curve, $X(\mathbb{C})$ is a Riemann surface of genus 1, and $H^*(X(\mathbb{C}), \mathbb{Q}_\ell) \simeq \mathbb{Q}_\ell^2$.

So we have $\rho_X : \Gamma_\mathbb{Q} \to GL(2, \mathbb{Q}_\ell)$.

Galois representations and cubic curves

Write the equation:

$$X \quad y^2 = x^3 + ax + b, \;\; a, b \in \mathbb{Q}.$$

Tate conjecture (Theorem of Faltings): ρ_X (almost) completely determines X.

Birch-Swinnerton-Dyer conjecture: $\Rightarrow$ The structure of the group $X(\mathbb{Q})$ of rational solutions to the equation of X is completely determined by ρ_X (for varying ℓ).

(Wiles, Taylor, et al.) Any 2-dimensional representation that "looks like" a ρ_X is a ρ_X.

"Looks like": Fontaine and Mazur identify natural properties of geometric ρ and conjecture that any ρ with these properties is geometric:

Conjecture

(Fontaine-Mazur) ρ looks geometric $\Rightarrow$ ρ **is** *geometric.*

(Appearances notwithstanding, this is a precise conjecture.)

How to identify a (geometric) Galois representation

Each prime p provides a label for ρ; together they suffice to identify ρ.

If ρ is geometric then for almost all p, there is a well-defined conjugacy class $c_p = \rho(\{Frob_p\}) \subset Im(\rho)$.
To p and ρ we assign the characteristic polynomial $P_{p,\rho}(X)$ of (any) $\rho(Frob_p) \in c_p$.
The set of (monic, degree n, non-zero constant term) polynomials $P_{p,\rho}(X)$ (almost all p) determine ρ.

The remaining p also provide labels (by the *local Langlands correspondence*).

Geometric analogue

A longstanding analogy between Galois representations and homomorphisms

$$\tau : \pi_1(X, x_0) \to GL(n, \mathbb{C}),$$

X a Riemann surface with base point x_0.
Such τ parametrize *local systems* of rank n over X. So local systems on curves are the geometric analogue of Galois representations.
By the Riemann-Hilbert correspondence, τ also parametrize holomorphic linear differential equations on X with regular singularities.
(The "geometric" condition for Galois representations corresponds roughly to regularity of the singularities.)

Langlands transform

A (hypothetical) “Langlands transform” would be a (geometric or analytic) procedure to relate

$$\text{Galois representations} \leftrightarrow \text{automorphic representations}$$

Arinkin, Drinfel’d, and Gaitsgory have a precise (abstract) conjecture in the geometric setting and a proof in dimension 2.

In the original setting of Langlands, we are very far from such a procedure.

So we improvise with the best available structures:
Shimura varieties.

Why Shimura varieties?

The (ℓ-adic) cohomology $H^*(Sh)$ of a Shimura variety Sh has simultaneous actions of two groups:

The Galois group $\Gamma_F = Gal(\overline{\mathbb{Q}}/F)$ for some finite extension $F/\mathbb{Q}$;

and a group $G(\mathbf{A}_f)$ realizing symmetries of (automorphic) differential and difference equations;

these actions commute, making the cohomology a *kernel* for a (very partial) Langlands transform: if Π is a representation of $G(\mathbf{A}_f)$,

$$\mathcal{L}(\Pi) = Hom_{G(\mathbf{A}_f)}(\Pi, H^*(Sh))$$

is a representation of Γ_F.

These examples can be stretched to provide a complete solution, under important restrictions, to the reciprocity problem.

Deligne-Lusztig varieties

Let now p be prime,

$$G = SL(2, \mathbb{F}_p) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{F}_p, \;\; ad - bc = 1 \},$$

which acts not only on $\mathbb{F}_p^2 \setminus 0$ but also on the affine variety

$$X = \{(x, y) \in k^2 \mid xy^p - x^p y = 1\}$$

where k is an algebraic closure of $\mathbb{F}_p$.

The torus $T = \{t \in \mathbb{F}_{p^2} \mid t^{p+1} = 1\}$ acts by $t(x, y) = (tx, ty)$ as before and this action fixes X and commutes with the action of G.

Deligne-Lusztig varieties

The torus $T = \{t \in \mathbb{F}_{p^2} \mid t^{p+1} = 1\}$ acts by $t(x,y) = (tx, ty)$ as before and this action fixes X and commutes with the action of G.

A special case of the theorem of Deligne-Lusztig is

Theorem

Let θ be a character of T. Then

$$\mathcal{DL}(\theta) = Hom_T(\theta, H^1_c(X, \overline{\mathbb{Q}}_\ell))$$

is (for most θ) an irreducible (cuspidal) representation of G.

Here and below, $H^i_c(*, \overline{\mathbb{Q}}_\ell)$ denotes ℓ-adic (étale) cohomology with compact support, which is the appropriate cohomology theory for varieties over finite fields.

Deligne-Lusztig varieties

More generally, if G is the group of $\mathbb{F}_p$-points of a reductive algebraic group (for example $G = GL(n, \mathbb{F}_q)$ $q = p^r$), then there is a family X_w of Deligne-Lusztig varieties, with an action of $G \times T_w$ for a finite abelian group T_w, such that the virtual representation

$$EP(X_w) = \sum_i (-1)^i H^i_c(X_w, \overline{\mathbb{Q}}_\ell)$$

decomposes as a direct sum of the form $\mathcal{DL}_w(\theta) \otimes \theta$ as above and every irreducible representation of G occurs in some $\mathcal{DL}_w(\theta)$.

Role of fixed point formulas

This theorem (of Deligne and Lusztig) is proved by applying the *Lefschetz fixed point formula*.
An irreducible representation $\rho : G \to Aut(V)$ (any finite group G) over a field K of char. 0 is determined by the K-valued function

$$\chi_\rho(g) = Tr(\rho(g)).$$

The trace of the action of $(g, t) \in G \times T_w$ on $EP(X_w)$ is calculated by the Grothendieck-Lefschetz formula if the fixed points are isolated:

$$Tr((g,t) \mid EP(X_w)) = \sum_{x \in Fix_{X_w}} Loc_x((g,t)),$$

$Loc_x((g,t)) \in \overline{\mathbb{Q}}_\ell$, or a more complicated formula in general.

Role of fixed point formulas

Cohomology forms a useful "kernel" for a representation-theoretic transform because the Lefschetz formula calculates traces.

In the automorphic situation – for example

- (Drinfel'd, Lafforgue) Langlands correspondence for curves over finite fields;
- (MH-Taylor) the local Langlands correspondence for p-adic fields

– one uses the Grothendieck-Lefschetz formula and the Arthur-Selberg trace formula.

Adèle groups

Let

$$\hat{\mathbb{Z}} = \varprojlim_N \mathbb{Z}/N\mathbb{Z} \simeq \prod_p \mathbb{Z}_p;$$

$$\mathbf{A}_f = \hat{\mathbb{Z}} \otimes \mathbb{Q}; \mathbf{A}_{f,F} = \mathbf{A}_f \otimes_{\mathbb{Q}} F$$

for any finite extension $F/\mathbb{Q}$.

An *automorphic representation of* $GL(n)_F$ is a (continuous) vector space representation of $GL(n, \mathbf{A}_{f,F})$, plus a representation of $GL(n, \mathbb{R} \otimes_{\mathbb{Q}} F)$, that satisfy a natural compatibility property.

Example: representations of $GL(n, \mathbf{A}_{f,F})$ in the cohomology of a *locally symmetric variety*; the existence of a compatible action of $GL(n, \mathbb{R} \otimes_{\mathbb{Q}} F)$ is concealed in the geometry.

How to identify an automorphic representation

Given an irreducible (admissible) representation Π of $GL(n, \mathbf{A}_f)$ is equivalent to giving an irreducible (smooth) representation Π_p of $GL(n, \mathbb{Q}_p)$ for each prime p such that for all but finitely many p, Π_p is *spherical* – i.e. has a non-zero vector fixed by $GL(n, \mathbb{Z}_p)$.

Irreducible spherical representations of $GL(n, \mathbb{Q}_p)$ are in 1-1 correspondence with monic degree n-polynomials with non-zero constant term (Shimura, Satake).

So are characteristic polynomials of $Frob_p$.

Say (the Galois rep.) ρ is *attached to* (the automorphic rep.) Π if these polynomials match up for almost all primes p.

Designing a Langlands transform

By analogy with the geometric examples, we would like the kernel to be a space with four properties:

- A cohomology theory for which the Lefschetz formula is valid;
- Commuting actions of the two groups Γ_F and $GL(n, \mathbf{A}_{f,F})$ (not quite possible for $n > 2$);
- A good parametrization of fixed points;
- The action of at least one of the groups should be **large**: the shape of the fixed points shows that all desired representations occur in the cohomology. (For Shimura varieties, the action of $G(\mathbf{A}_f)$ is (tautologically) large, but not that of Γ_F – so the transform only goes in one direction. The reverse direction is the Taylor-Wiles method, based on very different principles.)

Locally symmetric varieties

Generalizing the case of classical modular forms, let G be a semisimple matrix group over $\mathbb{Q}$, $K \subset G(\mathbb{R})$ maximal compact such that $H_G = G/K$ is a hermitian symmetric domain.

For any discrete subgroup $\Gamma \subset G(\mathbb{Q})$ of cofinite invariant volume in $G(\mathbb{R})$,

$$M_G(\Gamma) := \Gamma \backslash H_G$$

is a complex analytic variety.

If $G(\mathbb{R}) = SU(n-1,1)$ or $U(n-1,1)$, $H_G = B^{n-1}$ is the unit ball in $\mathbb{C}^{n-1}$ (if $n = 2$, B^1 is isomorphic to $\mathfrak{H}$).

Locally symmetric varieties

If Γ is a congruence subgroup (like $\Gamma(N) \subset SL(2, \mathbb{Q})$) then $M_G(\Gamma)$ is an algebraic variety with a canonical model over a number field $E(\Gamma)$; for most classical groups the canonical model was constructed by Shimura.

For congruence Γ, natural *difference equations* (Hecke operators) for each prime p as well as invariant differential equations (Laplacians and higher order operators).

For nearly all prime numbers p, one also has a canonical model of $M_G(\Gamma)$ (for most G) over a finite field of characteristic p, hence the Grothendieck-Lefschetz formula can be applied to $M_G(\Gamma)$ as to the Deligne-Lusztig variety.

Adelic modular curves

Return to the case of modular curves. There is nothing special about N. If N divides N', there is a natural surjective map (change of level)

$$M(N') \to M(N)$$

$$M(N) = M(N')/[\Gamma(N)/\Gamma(N')]; \;\; M(1) = M(N)/SL(2, \mathbb{Z}/N\mathbb{Z}).$$

In this way one obtains a natural action of

$$SL(2, \hat{\mathbb{Z}}) = \varprojlim_N SL(2, \mathbb{Z}/N\mathbb{Z})$$

on the family of the $M(N)$, compatible with the change of level maps.

This extends to a continuous action of $SL(2, \mathbf{A}_f) = SL(2, \hat{\mathbb{Z}} \otimes \mathbb{Q})$ on the family $\{M(N), N \in \mathbb{N}\}$, and thus on $\varinjlim_N H^*(M(N))$ for any cohomology theory.

Adelic modular curves

One prefers to work with a variant family $\{Sh(N), N \in \mathbb{N}\}$ with an action of $GL(2, \mathbf{A}_f)$.

The p-adic [note the change!] étale cohomology $\varinjlim_N H^*(Sh(N), \mathbb{Q}_p)$ admits an action of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ that commutes with the $GL(2, \mathbf{A}_f)$-action.

Theorem

(Eichler-Shimura-Deligne-Langlands-Carayol) The action of $GL(2, \mathbf{A}_f)$ on $\varinjlim_N H^1_c(Sh(N), \overline{\mathbb{Q}}_p))$ establishes a correspondence from irreducible (cuspidal) representations of $GL(2, \mathbf{A}_f)$ to 2-dimensional representations of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$:

$$\Pi \mapsto \mathcal{L}(\Pi) = Hom_{GL(2,\mathbf{A}_f)}(\Pi, \varinjlim_N H^1_c(Sh(N), \overline{\mathbb{Q}}_p))).$$

The complete theorem considers non-trivial equivariant coefficient systems as well, and obtains more general Galois representations. It is now known in almost complete generality that this realizes the Langlands reciprocity correspondence for most 2-dimensional representations of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$.

Adelic Shimura varieties

Let $H_n = GL(n,\mathbb{R})/O(n,\mathbb{R}) \cdot \mathbb{R}^\times$; get an adelic locally symmetric space:

$$S_n(N) = \{GL(n,\mathbb{Q})\backslash H_n \times GL(n,\mathbf{A}_f)/(I + N \cdot M(n,\hat{\mathbb{Z}})), N \in \mathbb{N}\}.$$

However, for $n > 2$, H_n has no complex structure and $S_n(N)$ is not an algebraic variety.

Functorial transfer (cf. Arthur's new book) identifies part of the cohomology of $S_n(N)$ with cohomology of (adelic) Shimura varieties attached to a unitary group G (not $GL(n)$).

$\Rightarrow$ construction of Galois representations ρ_Π attached to automorphic representation Π if $\Pi \simeq \Pi^\vee$.

Adelic Shimura varieties

Concretely, if G is a reductive algebraic group over $\mathbb{Q}$ with hermitian symmetric space, we can construct a Shimura variety:

$$S_G(N) = \{G(\mathbb{Q})\backslash H_G \times G(\mathbf{A}_f)/K_N, N \in \mathbb{N}\}.$$

Here K_N is a congruence subgroup and $S_G(N)$ is a finite union of $M_G(\Gamma)$.
The case of $G = U(n-1,1)$ (Kottwitz, Clozel, MH-Taylor, Labesse, Shin, Morel).

Self-dual cohomological representations

$G = U(n-1,1)$: use the cohomology of the corresponding Shimura varieties as "kernel" for a Langlands transform $\mathcal{L}(\Pi)$,
$\Rightarrow$ most of:

Theorem

(Preceding list, plus MH-Chenevier) Suppose Π is a representation of $GL(n, \mathbf{A}_f)$ in the (cuspidal) cohomology of $\{S_n(N)\}$, and suppose $\Pi \simeq \Pi^\vee$. Then

- *For all p there is a $\rho_{\Pi,p} : \Gamma_{\mathbb{Q}} \to GL(n, \overline{\mathbb{Q}}_p)$ attached to Π.*
- *For most Π (Blasius-Rogawski, "Shin regular") $\rho_{\Pi,p}$ is geometric.*
- *For all Π, $\rho_{\Pi,p}$* **looks** *geometric in the sense of Fontaine-Mazur.*

General cohomological representations

More recently, the duality condition has been relaxed.

Theorem

(MH, Lan, Taylor, Thorne) Suppose Π *is a representation of* $GL(n, \mathbf{A}_f)$ *in the (cuspidal) cohomology of* $\{S_n(N)\}$*. Then for each prime p there is a continuous* $\rho_{\Pi,p} : \Gamma_{\mathbb{Q}} \to GL(n, \overline{\mathbb{Q}}_p)$ *attached to* Π.

We can replace $\mathbb{Q}$ by any totally real or CM field, but Scholze has proved much stronger results, for example

Theorem

(Scholze) Let Π *be a representation of* $GL(n, \mathbf{A}_f)$ *on the mod p cohomology of* $\{S_n(N)\}$*. Then there is a continuous* $\rho_{\Pi,p} : \Gamma_{\mathbb{Q}} \to GL(n, \overline{\mathbb{F}}_p)$ *attached to* Π.

p-adic approximation

The Galois representations in the last theorems *cannot* be obtained by a Langlands transform.
Instead, one constructs the representations by successive (p-adic) approximation – gluing together $2n$-dimensional mod p^r representations attached to varying self-dual Π_r on $GL(2n, \mathbf{A}_f)$ – and then cuts the result into two pieces, one of which is $\rho_{\Pi,p}$.

Scholze's method recovers the representations in [HLTT], as well as the mod p representations. He uses a completely new kind of p-adic geometry (perfectoid spaces) to do this. The Π in his theorem is purely topological and has no obvious connection to automorphic forms. This is the first result of this time, and no one can tell how far he will be able to go with his methods.

What next?

(1) It's impossible to prove the $\rho_{\Pi,p}$ *are* geometric using Shimura varieties. For the mod p representations, it's not even clear what sense to give the question.

(2) Do the (characteristic zero) representations look geometric? (Ila Varma, work in progress)

(3) Ramanujan conjecture (purity)? Completely open.

(4) For Π not cohomological, a serious barrier; practically no ideas.