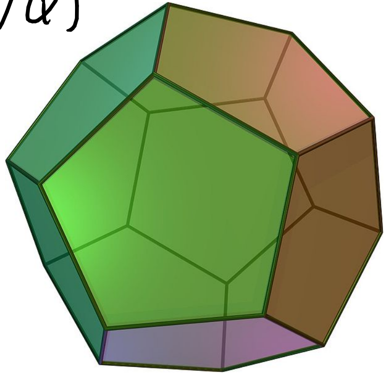
A Gentle Introduction to the Langlands Program

Jeremy Booher, University of Canterbury

Galois Representations

$$\begin{tikzcd} \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \arrow[rr] \arrow[dr] & & GL_n(\mathbb{C}) \\ & \mathrm{Gal}(K/\mathbb{Q}) \arrow[ur] & \end{tikzcd}$$



$A_5 \subset GL_2(\mathbb{R})$

Goals: - New perspective on $f(z) = q\prod(1-q^n)(1-q^{11n})$ $E: y^2+y=x^3-x$

- Langlands program expressed using Galois representations

- New concrete example

1) $g(z) = q\prod_{n=1}^{\infty}(1-q^n)(1-q^{23n}) = \eta(z)\eta(23z)$ mod form wt 1 for $\Gamma_0(23)$

$q = e^{2\pi i z}$ $= q - q^2 - q^3 + q^6 + q^8 - q^{13} - q^{16} + q^{23} + \dots + 2\cdot q^{59} + \dots$

2) Factorization of x^3-x-1 mod p

p	2	3	5	7	11	13	17	19		59
degree of factors	3	3	1+2	1+2	1+2	3	1+2	1+2	...	1+1+1

Observe:

factorization	coeff.
3	−1
1+2	0
1+1+1	2

Galois Theory and $x^3 - x - 1$

$$\begin{array}{l} L = K(\alpha) \quad \alpha^3 - \alpha - 1 = 0 \\ \quad \cup \\ K = \mathbb{Q}(\sqrt{-23}) \\ \quad \cup \\ \mathbb{Q} \end{array}$$

1) K is splitting field of $x^2 + 23$

$$\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$$

2) L is splitting field of $x^3 - x - 1$ ← discriminant -23

$$\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3 \quad \text{(permuting roots)}$$

Reminder: $\mathrm{Gal}(L/\mathbb{Q}) / \mathrm{Gal}(L/K) \simeq \mathrm{Gal}(K/\mathbb{Q})$

L is maximal unramified Abelian extension of K: Hilbert class field

Galois Theory and $x^3 - x - 1$

splitting of primes alg. # thry

$L = K(\alpha) \quad \alpha^3 - \alpha - 1 = 0$
$\cup$
$K = \mathbb{Q}(\sqrt{-23})$
$\cup$
$\mathbb{Q}$

Connection with splitting of $x^3 - x - 1 \bmod p$

What is splitting field of $x^3 - x - 1$ over $\mathbb{F}_p$?

$\mathbb{F}_{p^3}$: no roots in $\mathbb{F}_p$

$\mathbb{F}_{p^2}$: one root in $\mathbb{F}_p$

$\mathbb{F}_p$: all roots in $\mathbb{F}_p$

$x^2 + 23 \equiv 0 \bmod p$ has solutions

$p \equiv 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18 \bmod 23$

$x^2 + 23 \equiv 0 \bmod p$ has no solutions

$p \equiv 5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22 \bmod 23$

distinguish $\mathbb{F}_{p^3}$ vs $\mathbb{F}_p$ using modular form

Rephrasing Using Galois Theory

L splitting field of x^3-x-1 over $\mathbb{Q}$. Contains $K=\mathbb{Q}(\sqrt{-23})$

Key Idea: For each prime p, there is $\mathrm{Frob}_p \in \mathrm{Gal}(L/\mathbb{Q})$ such that

"Frob_p does same things to $\sqrt{-23}$ and roots of x^3-x-1 as

$x \mapsto x^p$

Frobenius does to roots of x^2+23 and x^3-x-1 in $\overline{\mathbb{F}_p}$"

Reminder: $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p) \simeq \mathbb{Z}/2\mathbb{Z}$ $\quad$ $\mathrm{Gal}(\mathbb{F}_{p^3}/\mathbb{F}_p) \simeq \mathbb{Z}/3\mathbb{Z}$

generated by $F(x)=x^p$

if -23 is square in $\mathbb{F}_p$, Frob_p fixes $\sqrt{-23}$

if all roots of x^3-x-1 in $\mathbb{F}_p$, Frob_p = identity

1) $g(z) = q\prod_{n=1}^{\infty}(1-q^n)(1-q^{23n})$ modular weight 1 level 23

$q = e^{2\pi i z}$

$= q - q^2 - q^3 + q^6 + q^8 - q^{13} + q^{23} + \dots + 2\cdot q^{59} + \dots$

2) L splitting field of x^3-x-1 over $\mathbb{Q}$

Coefficients of g	factorization mod p	$\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$
-1	x^3-x-1 has 3 roots in $\mathbb{F}_p$	Frob_p is identity
2	x^3-x-1 has no roots in $\mathbb{F}_p$	Frob_p order 3
0 $x^2+23\equiv 0 \bmod p$ has no solutions	x^3-x-1 has one root in $\mathbb{F}_p$	Frob_p order 2

Note: Frob_p only defined up to conjugation. Not defined $p=23$

Pick prime $\mathfrak{p}$ of L over $p\in\mathbb{Z}$. $\{\sigma\in \mathrm{Gal}(L/\mathbb{Q}) : \sigma(\mathfrak{p})=\mathfrak{p}\} \cong \mathrm{Gal}(k(\mathfrak{p})/\mathbb{F}_p)$

Absolute Galois Groups

Definition: The absolute Galois group of a field K is $\mathrm{Gal}(\overline{K}/K)$. — actually use separable closure

Example: $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \varprojlim \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \varprojlim \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}$

Example: K Galois number field (finite ext'n of $\mathbb{Q}$ like $\mathbb{Q}(\sqrt{2})$)

$$\begin{array}{c} \overline{\mathbb{Q}} \\ \cup \\ K \\ \cup \\ \mathbb{Q} \end{array}$$

$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ has normal subgroup $\mathrm{Gal}(\overline{K}/K) = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$

with quotient $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})/\mathrm{Gal}(\overline{K}/K) \simeq \mathrm{Gal}(K/\mathbb{Q})$

This is mechanism to avoid fixing a particular extension of $\mathbb{Q}$ — and impose topology to make nicer

Big Goal in Number Theory: understand $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

Galois Representations

Definition: If G is a Galois group, a two dimensional Galois representation of G over a ring R is a homomorphism* $\rho: G \to GL_2(R)$

* Continuous, using natural topologies

$$GL_2(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \begin{array}{l} a,b,c,d \in R \\ ad-bc \in R^\times \end{array} \right\}$$

Example: L splitting field of x^3-x-1 over $\mathbb{Q}$. $Gal(L/\mathbb{Q}) \simeq S_3$.

$S_3 \hookrightarrow GL_2(\mathbb{C})$ via acting on $\underbrace{\{x_1+x_2+x_3=0\}}_{\text{two dim}} \subset \mathbb{C}^3$

Generalization: Any finite Galois ext'n of $\mathbb{Q}$ (any finite group?)

Any representation of that group

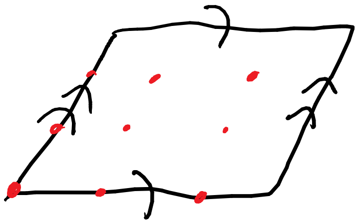
Galois Representations from Elliptic Curves

Let E be an elliptic curve over $\mathbb{Q}$: $y^2 = x^3 + Ax + B$ $\quad A, B \in \mathbb{Q}$

If $(x,y) \in E(\overline{\mathbb{Q}})$ and $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ then $(\sigma(x), \sigma(y)) \in E(\overline{\mathbb{Q}})$.

$$\sigma(y)^2 = \sigma(y^2) = \sigma(x^3 + Ax + B) = \sigma(x)^3 + A\sigma(x) + B.$$

Galois action compatible with group law.



$E[3]$ over $\mathbb{C}$

Recall $E(\overline{\mathbb{Q}})[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

$\circlearrowright$ $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

Galois Representation:

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}/n\mathbb{Z})$$

E elliptic curve over $\mathbb{Q}$. $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}/n\mathbb{Z})$

Fix a prime ℓ.

$$\begin{tikzcd}
 & \cdots \arrow[d] \\
 & GL_2(\mathbb{Z}/(\ell^3)) \arrow[d] \\
\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \arrow[uur] \arrow[ur] \arrow[r] \arrow[dr] & GL_2(\mathbb{Z}/(\ell^2)) \arrow[d] \\
 & GL_2(\mathbb{Z}/(\ell))
\end{tikzcd}$$

Tate module

$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_\ell E) \simeq GL_2(\mathbb{Z}_\ell)$

Reminder: $\mathbb{Z}_\ell = \varprojlim_n \mathbb{Z}/\ell^n\mathbb{Z}$

$T_\ell E = \varprojlim_n E(\overline{\mathbb{Q}})[\ell^n]$

Example: $y^2+y=x^3-x$. We saw it had 5 points over $\mathbb{Q}$.

Obtain $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}/5\mathbb{Z})$ image in $\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$

Example Continued: $E: y^2+y=x^3-x$

$\rho_E : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}_5)$ 5-adic Galois rep

☆ $\rho_E(Frob_p) \equiv \begin{pmatrix} 1 & * \\ 0 & p \end{pmatrix} \bmod 5$

Use Weil pairing to see determinant is p

Use Tate module

☆ Proposition: $tr(\rho_E(Frob_p)) = a_p(E) = p+1-\#E(\mathbb{F}_p)$

Complementary Example: $y^2+y=x^3-x$ has no 7-torsion points over $\mathbb{Q}$

$\rho'_E : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}_7)$

$\rho'_E(Frob_p) \equiv$ nothing special mod 7

Choice of primes (5 vs. 7) influenced by torsion points defined over $\mathbb{Q}$

Galois Representations from Modular Forms

Hard Fact: There are ways to construct Galois representations from "nice" cusp forms.

Eichler-Shimura $k=2$
Deligne $k>2$
Deligne-Serre $k=1$

Example: $f(q) = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2$ cusp form weight 2 for $\Gamma_0(11)$

Fix a prime ℓ. There is Galois rep. $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}_\ell)$

such that $\rho_f(\mathrm{Frob}_p)$ satisfies $x^2 - a_p(f)x + p$ for all $p \nmid 11$.

i.e. $\mathrm{tr}\,\rho_f(\mathrm{Frob}_p) = a_p(f)$ and $\det(\rho_f(\mathrm{Frob}_p)) = p$

$$f(z) = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2 = \sum a_n(f)q^n \qquad E: y^2+y = x^3-x \qquad a_p(E) = p+1-\#E(\mathbb{F}_p)$$

Take $\ell = 5$: Galois rep for f and E the same. last time modularity of E.

$$a_p(f) = \operatorname{tr}\rho_f(\mathrm{Frob}_p) = \operatorname{tr}\rho_E(\mathrm{Frob}_p) = a_p(E) \qquad (p \neq 11)$$

$$a_p(f) \equiv p+1 \bmod 5 \longleftrightarrow \rho(\mathrm{Frob}_p) \equiv \begin{pmatrix} 1 & * \\ 0 & p \end{pmatrix} \bmod 5 \longleftrightarrow a_p(E) \equiv p+1 \bmod 5$$

congruence of modular forms

Congruence for Galois representation

rational points on modular elliptic curve

General Strategy: Explain congruences between modular forms using congruences between Galois representations. Swinnerton-Dyer

Example: $g(z) = q\prod_{n=1}^{\infty}(1-q^n)(1-q^{23n}) = \sum a_n(g)q^n$ weight 1 level 23

There is a Galois representation $\rho_g : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{C})$ s.t.

for $p \neq 23$ $\rho_g(\mathrm{Frob}_p)$ satisfies $x^2 - a_p(g)x \pm 1 = 0$

Sign depends on p

This is the same Galois representation constructed using L, the splitting field of $x^3 - x - 1$ over $\mathbb{Q}$

$$\rho_L : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(L/\mathbb{Q}) \simeq S_3 \hookrightarrow GL_2(\mathbb{C})$$

Thus $\mathrm{tr}\,\rho_g(\mathrm{Frob}_p) = a_p(g) = \mathrm{tr}\,\rho_L(\mathrm{Frob}_p)$

$g(z) = q\prod(1-q^n)(1-q^{23n})$ cusp form of weight 1 level 23

L splitting field of x^3-x-1 $\qquad \rho_g = \rho_L$

Coef. of q^p in $g(z)$	$\operatorname{tr}\rho_L(\mathrm{Frob}_p)$	$\mathrm{Gal}(L/\mathbb{Q})$	factorization mod p
2	2	Frob_p identity	x^3-x-1 has 3 roots in $\mathbb{F}_p$
-1	-1	Frob_p has order 3	x^3-x-1 has no roots in $\mathbb{F}_p$
0	0	Frob_p has order 2	x^3-x-1 has one root in $\mathbb{F}_p$

Calculation for traces: if Frob_p swaps 2^{nd} + 3^{rd} roots:
$$e_1-e_2 \longmapsto e_1-e_3$$
$$e_2-e_3 \longmapsto -e_2+e_3$$

$$\rho_L(\mathrm{Frob}_p) = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$$

What is the Langlands Program?

Partial picture

"nice" Galois representations $\xleftrightarrow{\text{trace of } \mathrm{Frob}_p \;\longleftrightarrow\; \text{Coeff of } q^p}$ "nice" modular forms

finding Galois rep geometrically
(cohomology of variety over number field)

We talked about examples:

Galois rep from modular form: look in cohomology of modular curve.

Galois rep from elliptic curve: Use Tate module

Modular form from elliptic curve: Modularity theorems.
[Use Galois rep]

What is the Langlands Program?

Partial picture

"nice" Galois representations $\longleftrightarrow$ "nice" modular forms

$\searrow$ Finding Galois rep geometrically $\swarrow$

(cohomology of variety over number field)

This is part of Langlands program for GL_2:

Galois Rep: $GL_2(\mathbb{R})$

Geometrically: $\mathrm{Aut}(T_\ell E) \simeq GL_2(\mathbb{Z}_\ell)$

(or two dim piece of cohomology)

Modular Forms: $GL_2(\mathbb{R})^+$ acts on $\mathcal{H}$

$$\mathcal{H} \simeq GL_2(\mathbb{R})^+ / \mathbb{R}^\times SO_2(\mathbb{R})$$

What is the Langlands Program?

It's for reductive groups GL_n SO_n ← preserve inner product

Sp_{2n} U_n E_8 ...

"Nice" Galois Representations ⟷ "Nice" automorphic forms/representations

$\rho: Gal(\overline{K}/K) \to G(\overline{\mathbb{Q}}_\ell)$

G reductive

K local or global field

$\mathcal{E}$ for reductive group

via

(piece of) cohomology of a geometric object ← Shimura Varieties, perfectoid spaces...

How to match them: generalize

coeff of q^p ⟷ trace of $Frob_p$

Warning: the reductive group on Galois/automorphic sides may be different

Galois Reps from Modular Forms: Cartoon Version (if time)

f cusp form weight 2 for $\Gamma_0(11)$.

1) $\mathcal{H}/\Gamma_0(11)$ is a genus 1 Riemann surface modular curve $X_0(11)$

2) $f(z)dz$ defines a differential form on $X_0(11)$. $f(z)dz$ and $\overline{f(z)dz}$ give basis for $H^1(X_0(11), \mathbb{C}) \simeq H^{1,0}(X_0(11)) \oplus H^{0,1}(X_0(11))$

3) Coefficient of q^p in q-series for f: eigenvalue of p^{th} Hecke operator on space of mod forms, eigenvector f.

4) Interpret Hecke operators as correspondences on $X_0(11)$

Complications: $X_0(N)$ may have higher genus — need to break cohomology into chunks

weight >2: not differential form — use more complicated coefficients

Galois Reps from Modular Forms: Cartoon Version

5) Realize that $X_0(11)$ is algebraic: scheme over $\mathrm{Spec}(\mathbb{Z}[\frac{1}{11}])$

6) Get a Galois Representation from $H^1_{ét}(X_0(11)_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)$.

7) (Eichler-Shimura) Relate Galois action of Frob_p with map on cohomology induced by p^{th} Hecke operator.
Study modular curve modulo p.

8) Have Galois rep with $\mathrm{tr}\,\rho(\mathrm{Frob}_p) = a_p(f)$. Yay!

A1) Find equations for $X_0(11)$, or find it in database based on invariant: it's $y^2+y = x^3 - x$

A2) Galois rep of this elliptic curve uses Tate module: dual to $H^1_{ét}$

Special as genus one