GALOIS REPRESENTATIONS

ALGEBRAIC NUMBERS:

$\overline{\mathbf{Q}} = \{\alpha \in \mathbf{C} : \alpha$ **satisfies a polynomial equation with rational coefficients**$\}$

ABSOLUTE GALOIS GROUP OF Q:

$$\begin{aligned} G_{\mathbf{Q}} &= Aut(\overline{\mathbf{Q}}) \\ &= \{\text{bijections } \overline{\mathbf{Q}} \to \overline{\mathbf{Q}} \text{ preserving } +, \times\} \end{aligned}$$

with weakest topology for which the stabiliser of every algebraic number is open.

If $f \in \mathrm{Q}[X]$ then let G_f denote the Galois group of f, i.e. the group of permutations of the roots of f preserving algebraic relations with Q coefficients.

$f|g$ **implies** $G_g \twoheadrightarrow G_f$.

$$G_{\mathbf{Q}} = \lim_{\leftarrow f} G_f,$$

a profinite group.

The usual (archimedean) absolute value $|\ |_\infty = |\ |$ induces a metric on Q. Completing Q with this metric gives the field R of real numbers.

$$\begin{array}{rcl} \overline{\mathbf{Q}} & \hookrightarrow & \overline{\mathbf{R}} = \mathbf{C} \\ G_{\mathbf{Q}} & \hookleftarrow & G_{\mathbf{R}} = Aut^{cts}(\mathbf{C}) = \{1, c\} \end{array}$$

For a prime p we have the p-adic absolute value on $\mathbb{Q}$:

$$|\alpha|_p = p^{-r} \text{ if } \alpha = p^r a/b \text{ with } p \nmid ab$$

p-adic numbers $\mathbb{Q}_p$ = completion of $\mathbb{Q}$ for $|\ |_p$.

$$\begin{array}{rcl} \overline{\mathbf{Q}} & \hookrightarrow & \overline{\mathbf{Q}}_p \\ G_{\mathbf{Q}} & \hookleftarrow & G_{\mathbf{Q}_p} = Aut^{cts}(\overline{\mathbf{Q}}_p) \end{array}$$

p-adic integers $\mathbf{Z}_p$ **= elements** $\alpha \in \mathbf{Q}_p$ **with** $|\alpha_p|_p \leq 1$**.**

$$\mathbf{Z}_p/p\mathbf{Z}_p = \mathbf{Z}/p\mathbf{Z}$$

$$G_{\mathbf{Q}_p} \twoheadrightarrow G_{\mathbf{Z}/p\mathbf{Z}} = \langle Frob_p \rangle$$

kernel $= I_p =$ **inertia group at** p**.**

$Frob_p =$ **(geometric) Frobenius element:** $(Frob_p\ \alpha)^p = \alpha$**.**

If $f \in \mathbf{Q}[X]$ then for aa p the image of $I_p \subset G_{\mathbf{Q}}$ is trivial in G_f and so we have a well definied conjugacy class

$$[Frob_p] \subset G_f.$$

It is characterized by

$$(Frob_p \alpha)^p \equiv \alpha \bmod p$$

for α a root of f.

eg $f(X) = X^4 - 2$**.**

$f(X) \equiv (X-2)(X+2)(X^2+4) \bmod 7$

and so $Frob_7$ **fixed two roots of** f **and interchanges two. Thus**

$[Frob_7] = \{(i\sqrt[4]{2}, -i\sqrt[4]{2}),\ (\sqrt[4]{2}, -\sqrt[4]{2})\}.$

1

$$(\sqrt[4]{2},\, i\sqrt[4]{2},\, -\sqrt[4]{2},\, -i\sqrt[4]{2})$$

$$(\sqrt[4]{2},\, -\sqrt[4]{2})(i\sqrt[4]{2},\, -i\sqrt[4]{2})$$

$$(\sqrt[4]{2},\, -i\sqrt[4]{2},\, -\sqrt[4]{2},\, i\sqrt[4]{2})$$

$$c = (i\sqrt[4]{2},\, -i\sqrt[4]{2})$$

$$(\sqrt[4]{2},\, -i\sqrt[4]{2})(-\sqrt[4]{2},\, i\sqrt[4]{2})$$

$$(\sqrt[4]{2},\, -\sqrt[4]{2})$$

$$(\sqrt[4]{2},\, i\sqrt[4]{2})(-\sqrt[4]{2},\, -i\sqrt[4]{2})$$

$$[c] = [Frob_7] = \{(i\sqrt[4]{2}, -i\sqrt[4]{2}),\ (\sqrt[4]{2}, -\sqrt[4]{2})\}.$$

$X^4 - 2 \equiv (X^2 + X - 1)(X^2 - X - 1)$ mod 3.

$$\begin{aligned}[Frob_3] = \{&(\sqrt[4]{2}, -i\sqrt[4]{2})(-\sqrt[4]{2}, i\sqrt[4]{2}),\\ &(\sqrt[4]{2}, i\sqrt[4]{2})(-\sqrt[4]{2}, -i\sqrt[4]{2})\}\end{aligned}$$

$X^4 - 2$ **irreducible** mod5.

$$\begin{aligned}[Frob_5] = \{&(\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}),\\ &(\sqrt[4]{2}, -i\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2})\}\end{aligned}$$

$X^4 - 2 \equiv (X^2 - 6)(X^2 + 6)$ mod 17.

$$[Frob_{17}] = \{(\sqrt[4]{2}, -\sqrt[4]{2})(i\sqrt[4]{2}, -i\sqrt[4]{2})\}.$$

$$G_{\mathbf{Q}_p} \subset G_{\mathbf{Q}} \supset \{1, c\}$$

MOTIVATING ALGEBRAIC PROBLEM:

Describe $G_{\mathbf{Q}}$ along with $G_{\mathbf{Q}_p}$, I_p, $Frob_p$ etc. inside it.

BETTER QUESTION:

Describe the representations of $G_{\mathbf{Q}}$ while keeping track of restrictions to each $G_{\mathbf{Q}_p}$.

e.g. $\varepsilon_n : \sigma \mapsto \sigma(\sqrt{n})/\sqrt{n} \in \{\pm 1\} \subset \mathbf{Q}^\times$.

$$Frob_p \mapsto 1$$

iff $X^2 - n$ **has** 2 **solutions in** $\mathbf{Z}/p\mathbf{Z}$.

e.g. GROTHENDIECK (1960's):

X/Q **smooth projective variety.**

$$H^i(X(\mathbf{C}), \overline{\mathbf{Q}}_l) = H^i(X(\mathbf{C}), \mathbf{Q}) \otimes_{\mathbf{Q}} \overline{\mathbf{Q}}_l$$

has a continuous action of $G_{\mathbf{Q}}$

1) For all but finitely many (aa) p the inertia group I_p acts trivially on $H^i(X(\mathrm{C}), \overline{\mathrm{Q}}_l)$ (i.e. is 'unramified' at p) so the conjugacy class $[Frob_p]$ in Aut$(H^i(X(\mathrm{C}), \overline{\mathrm{Q}}_l))$ **is defined.**

2) $H^i(X(\mathrm{C}), \overline{\mathrm{Q}}_l)$ is a de Rham representation of G_{Q_l} (and for aa l it is crystalline).

3) For aa p the characteristic polynomial of $Frob_p$ on $H^i(X(\mathrm{C}), \overline{\mathrm{Q}}_l)$ (for $l \neq p$) has coefficients in $\overline{\mathrm{Q}}$ and all its roots in C have absolute value $p^{i/2}$ (i.e. is 'pure' of weight i).

If $V/\overline{\mathbb{Q}}_l$ is a finite dimensional vector space and if

$$r : G_{\mathbf{Q}} \longrightarrow GL(V)$$

is a continuous representation satisfying these three properties define an L-function $L(V,s)$ as

$$\Pi_{p \neq l} \det(1_V - p^{-s} Frob_p)|_{V^{I_p}}^{-1}$$

$$\times(\textbf{similar factor at } l)$$

in $\mathrm{Re}\ s > 1 + i/2$**.**

(We fix once and for all

$$\mathbf{C} \supset \overline{\mathbf{Q}} \subset \overline{\mathbf{Q}}_l.)$$

Note

$$L(V_1 \oplus V_2, s) = L(V_1, s)L(V_2, s).$$

e.g. $L(\text{triv}, s) = \zeta(s) = \prod_p (1 - 1/p^s)^{-1} = \sum_{n=1}^{\infty} 1/n^s$.

e.g. if $M_p = \#$ **of solutions to** $X^2 + n \equiv 0 \bmod p$ **then** $L(\varepsilon_n, s)$ **equals**

$$\prod_{p:\ M_p=2} (1 - 1/p^s)^{-1} \prod_{p:\ M_p=0} (1 + 1/p^s)^{-1}.$$

e.g. $E/\mathbb{Q}$ **an elliptic curve and** $N_p = \#E(\mathbf{Z}/p\mathbf{Z})$**. Then** $Frob_p$ **on**

$$H^1(E(\mathbb{C}), \overline{\mathbf{Q}}_l) \cong \overline{\mathbf{Q}}_l^2$$

has trace $p - N_p$ **and determinant** p**. Thus**

$$L(\mathrm{Sym}^{n-1}E, s) = L(\mathrm{Sym}^{n-1}H^1(E(\mathbb{C}), \overline{\mathbf{Q}}_l), s)$$

in Re $s > (n+1)/2$**.**

e.g. If X/Q is smooth projective set

$$\zeta(X,s) = \prod_p \prod_{x \in X \times \mathbf{Z}/p\mathbf{Z}} (1 - p^{-s \deg x})^{-1}.$$

Then

$$\zeta(X,s) = \prod_i L(H^i(X(\mathbf{C}), \overline{\mathbf{Q}}_l), s)^{(-1)^i}$$

For instance

$$\zeta(\operatorname{Spec} \mathbf{Q}, s) = \zeta(s)$$

$$\zeta(\operatorname{Spec} \mathbf{Q}(\sqrt{n}), s) = \zeta(s) L(\varepsilon_n, s)$$

$$\zeta(E,s) = \zeta(s)\zeta(s-1)/L(\mathrm{Sym}^1 E, s)$$

FONTAINE-MAZUR CONJECTURE (1988): Suppose that

$$r : G_{\mathbf{Q}} \longrightarrow GL(V)$$

is a continuous irreducible representation satisfying properties 1. and 2. Then:

a) (Up to Tate twist) V **occurs in some** $H^i(X(\mathbf{C}), \overline{\mathbf{Q}}_l)$**.**

b) V **also satisfies property 3.**

1. **For aa p the inertia group I_p acts trivially on $H^i(X(\mathbb{C}), \overline{\mathbb{Q}}_l)$.**

2. **$H^i(X(\mathbb{C}), \overline{\mathbb{Q}}_l)$ is a de Rham representation of $G_{\mathbb{Q}_l}$.**

3. **For aa p the characteristic polynomial of $Frob_p$ on $H^i(X(\mathbb{C}), \overline{\mathbb{Q}}_l)$ (for $l \neq p$) has coefficients in $\overline{\mathbb{Q}}$ and all its roots in $\mathbb{C}$ have absolute value $p^{i/2}$ (i.e. is 'pure' of weight i).**

Topological ring of adeles:

$$\mathbf{A} = \mathbf{R} \times (\mathbf{Q} \otimes_{\mathbf{Z}} \prod_p \mathbf{Z}_p) \qquad (\subset \mathbf{R} \times \prod_p \mathbf{Q}_p)$$

$\mathbf{Q} \subset \mathbf{A}$ **- discrete and co-compact**

$$GL_n(\mathbf{Q})\backslash GL_n(\mathbf{A})/\textstyle\prod_p GL_n(\mathbf{Z}_p) = GL_n(\mathbf{Z})\backslash GL_n(\mathbf{R})$$

CLASS FIELD THEORY:

$Art_p : \mathbf{Q}_p^\times \longrightarrow G^{ab}_{\mathbf{Q}_p}$ **injective, dense image**

$$Art_\infty : \mathbf{R}^\times / \mathbf{R}^\times_{>0} \xrightarrow{\sim} G_{\mathbf{R}}$$

$$Art = \prod_x Art_x : \mathbf{Q}^\times \mathbf{R}^\times_{>0} \backslash \mathbf{A}^\times \xrightarrow{\sim} G^{ab}_{\mathbf{Q}}$$

Irreducible representations

$$\pi = {\bigotimes_x}' \pi_x$$

are CUSPIDAL AUTOMORPHIC if they occur in

$$L^2_{\chi,0}(GL_n(\mathbf{Q})\backslash GL_n(\mathbf{A})),$$

where $(gf)(h) = f(hg)$**.**

$$L(\pi, s) = \prod_p L(\pi_p, s)$$

- **π_x: π_p (resp. π_∞) is a representation of $GL_n(\mathbf{Q}_p)$ (resp. $GL_n(\mathbf{R})$).**

- **χ: $f(zg) = \chi(z)f(g)$ for $z \in \mathbf{R}^\times_{>0}$.**

- **0: $\int_{N(\mathbf{Q})/N(\mathbf{A})} f(ng)dn = 0$ for N a subgroup**

$$\begin{pmatrix} I_m & * \\ 0 & I_{n-m} \end{pmatrix} \subset GL_n.$$

EXAMPLES:

GL_1: **Cuspidal automorphic representations $\sim$ Dirichlet characters**

$$(\mathbf{Z}/N\mathbf{Z})^\times \to \mathbf{C}^\times$$

GL_2: **Regular algebraic cuspidal automorphic forms $\sim$
cuspidal holomorphic modular forms which are newforms.**

LANGLANDS RECIPROCITY CONJECTURE: If

$$\rho : G_{\mathbf{Q}} \longrightarrow GL_n(\overline{Q}_l)$$

is a continuous, irreducible representation which is unramified at all but finitely many primes and for which $\rho|_{G_{\mathbf{Q}_l}}$ **is de Rham then there is a cuspidal automorphic representation** π **of** $GL_n(\mathrm{A})$ **with**

$$L(\pi, s) = L(\rho, s).$$

In fact this sets up a bijection between such ρ **and** π **with** π_∞ **algebraic.**

Suppose that

$$r : G_{\mathbf{Q}} \longrightarrow GL(V)$$

is a continuous irreducible representation satisfying the reciprocity conjecture then $L(V,s)$ **is has analytic continuation to** $\mathbb{C}$ **(except possibly for one simple pole if** $\dim V = 1$**) and satisfies an (explicit) functional equation relating** $L(V,s)$ **to** $L(V^*,1-s)$**.**

If moreover V **has weight** i **then** $L(V,s)$ **is non-zero in Re** $s \geq i/2+1$**.**

(Gelbart-Jacquet)

e.g. Gauss' law of quadratic reciprocity says

$$L(\varepsilon_n, s) = L(\chi, s)$$

for some $\chi : (\mathbf{Z}/4n\mathbf{Z})^\times \to \mathbf{C}^\times$**.**

e.g. The Shimura-Taniyama conjecture says that

$$L(\mathrm{Sym}^1 E, s) = L(f_E, s)$$

where

$f_E(z) = \sum_{n=1}^{\infty} a_n e^{2n\pi iz}$,

$L(f_E, s) = \sum_{n=1}^{\infty} a_n/n^s$,

$f((az+b)/(cz+d)) = (cz+d)^2 f(z)$ **for** $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$ **with** $N_E | c$ **(some** N_E**),**

$f(-1/(N_E z)) = \mp N_E z^2 f(z)$.

Then

$$
\begin{aligned}
& L(E,s) \\
= \; & (2\pi)^s/\Gamma(s) \textstyle\int_0^\infty f_E(iy) y^{s-1} dy \\
= \; & (2\pi)^s 11^{(1-s)/2}/\Gamma(s) \\
& \Big(N_E^{(s-1)/2} \textstyle\int_{1/\sqrt{N_E}}^\infty f(iy) y^{s-1} dy \\
& \pm N_E^{(1-s)/2} \textstyle\int_{1/\sqrt{N_E}}^\infty f(iy) y^{1-s} dy \Big).
\end{aligned}
$$

Thus $L(E,s)$ **extends to an entire function and**

$$
\begin{aligned}
& (2\pi)^{s-2}\Gamma(2-s)L(E,2-s) = \\
& \pm N_E^{s-1}(2\pi)^{-s}\Gamma(s)L(E,s).
\end{aligned}
$$

Conjecture (Birch-Swinnerton-Dyer, 1963): There are infinitely many pairs (x, y) of rational numbers satisfying

$$y^2 = x^3 + cx + d$$

if and only if $L(E, 1) = 0$.

Theorem (Gross-Zagier 1986, Kolyvagin 1989): True if order of vanishing ≤ 1.