Deformation theory of Galois representations

MA842 at BU Spring 2020

Robert Pollack

January 23, 2020

These are notes for Robert Pollack's course MA842 at BU Spring 2020.

The course webpage is http://math.bu.edu/people/rpollack/Teach/842spring2020.html.

Lecture 1 21/1/2018

1 Motivation

Let E_k denote the Eisenstein series of weight k, $k > 2$.

$$E_k = \frac{-B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \in M_k(\mathrm{SL}_2(\mathbf{Z})).$$

Where B_k are the Bernoulli numbers and

$$\sigma_{k-1}(n) = \sum_{d|n,\, d>0} d^{k-1}.$$

E_2 however is not holomorphic, so not a modular form.

Fix N a prime, notation has stuck from Mazur's Eisenstein ideal paper.

Then there exists a unique Eisenstein series on $\Gamma_0(N)$ of weight 2.

$$E_2^{(N)} = \frac{N-1}{12} + \sum_{n=1}^{\infty} \sigma(n) q^n.$$

Funny observation: if $N \equiv 1 \pmod p$ for prime $p > 3$. Then $p|((N-1)/12)$, so $E_2^{(N)}$ "looks cuspidal".

Then we hope that there exists a cuspidal eigenform $f \in S_2(\Gamma_0(N))$ such that

$$f \equiv E_2^{(N)} \quad \text{“} \mod p\text{”}.$$

This is in fact true, due to Koike in the 70's, there exists $f \in S_2(\Gamma_0(N))$ such that

$$a_\ell(f) \equiv 1 + \ell \pmod p$$

for all $\ell \neq N, p$.

Question 1.1 How many such f are there? □

Merel '96:

$$f \text{ is unique } \iff \prod_{i=1}^{(N-1)/2} i^i \text{ is not a } p\text{-th power modulo } N.$$

Wake and Wang-Erickson describe the dimension of the space of such f using Massey products (higher cup products).

Method: Galois deformations!

1.1 Galois representations

We write

$$G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) = \varprojlim_{F/\mathbf{Q},\text{fin. galois}} \mathrm{Gal}(F/\mathbf{Q})$$

a profinite group.

$$\rho\colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Q}_p)$$

a continuous homomorphism. Then view $\mathrm{GL}_2(\mathbf{Q}_p)$ as $\mathrm{Aut}(V)$ for a 2-dimensional $\mathbf{Q}_p$ vector space and fix a 2-dimensional $\mathbf{Z}_p$-lattice

$$T \subseteq V$$

which is $G_{\mathbf{Q}}$ stable. Then we can take

$$\bar{\rho}\colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_p)$$

this is unique (w.r.t. the choice of T) only up to semisimplification.

So we say two Galois representations ρ_1, ρ_2 are congruent if

$$\bar{\rho}_1^{\mathrm{ss}} \simeq \bar{\rho}_2^{\mathrm{ss}}.$$

We say ρ_1, ρ_2 are deformations of

$$\bar{\rho}_1 = \bar{\rho}_2$$

(imagine this is reducible).

Start with

$$\bar{\rho}\colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_p)$$

consider "all" deformations of $\bar{\rho}$ in good cases there exists a "universal" deformation of $\bar{\rho}$.

R^{univ} a local ring with maximal ideal $\mathfrak{m}_R$ such that

$$R/\mathfrak{m}_R = \mathbf{F}_p.$$

$$\rho^{\mathrm{univ}}\colon G_{\mathbf{Q}} \to \mathrm{GL}_2(R^{\mathrm{univ}})$$

such that if $\rho\colon G_{\mathbf{Q}} \to GL_2(R)$ is a deformation of $\bar{\rho}$ then there exists

$$R^{\mathrm{univ}} \to R$$

such that

$$\begin{tikzcd} G_{\mathbf{Q}} \arrow[r, "\rho^{\mathrm{univ}}"] \arrow[dr, "\rho"'] & \mathrm{GL}_2(R^{\mathrm{univ}}) \arrow[d] \\ & GL_2(R) \end{tikzcd}.$$

1.2 Modular forms

$$f = \sum a_n q^n \in S_k(\Gamma_0(N))$$

an eigenform leads to

$$\rho_f \colon G_{\mathbf{Q}} \to \mathrm{GL}_2(K),\ K/\mathbf{Q}_p \text{ finite}$$

with the property that for all $\ell \nmid Np$ we have

$$\mathrm{Tr}(\rho_f(\mathrm{Frob}_\ell)) = a_\ell.$$

Modular forms can be congruent

$$a_\ell(f_1) \equiv a_\ell(f_2) \pmod{p} \text{ for all but finitely many } \ell$$

$$\Updownarrow$$

$$\bar\rho_{f_1}^{\mathrm{ss}} \simeq \bar\rho_{f_2}^{\mathrm{ss}}.$$

There exists a ring, the Hecke algebra $\mathbf{T}$ parametrizing all f's with the same $\bar\rho$.

$$f \rightsquigarrow \rho_f \implies R^{\mathrm{univ}} \to \mathbf{T}$$

so hope

$$R^{\mathrm{univ}} \simeq \mathbf{T}.$$

Wiles proof of FLT proved one of these.

Many more such theorems in the past couple of decades.

Wake and Wang-Erickson show that the dimension of

$$\{f : f \equiv E_2^{(N)}\} \leftrightarrow \operatorname{rank} \mathbf{T} = \operatorname{rank} R^{\mathrm{univ}}.$$

$$a_\ell(f) \equiv 1 + \ell \pmod{p}$$

$$\implies \bar\rho^{\mathrm{ss}} = \mathbf{1} \oplus \mu_p$$

but there does not exist R^{univ} in this context.

The fix is to use pseudorepresentations instead of representations.

1.3 Pseudorepresentations

Let G be a group.

Then a pseudorepresentation T is a map

$$T \colon G \to A$$

for A a ring satisfying

1. $$T(xy) = T(yx)$$

2. $$T(x)T(y)T(z) - T(x)T(yz) - T(y)T(xz) - T(z)T(xy) + T(xyz) + T(xzy) = 0$$

and the analogous formulae for higher dimensions.

Fact 1.2 *If A is an algebraically closed field of characteristic $\neq 2$. Then for a given pseudorepresentation T there exists a true representation ρ such that*

$$T = \mathrm{Tr}(\rho).$$

But this does not hold in general.

Universal pseudodeformation rings always exist. Wake and Wang-Erickson use R^{univ} = universal pseudodeformation ring.

2 Definitions

2.1 Representations

Lecture 2 23/1/2018

Definition 2.1 Representations. Let G be a finite group and V a finite dimensional vector space over $\mathbf{C}$ of dimension d. A **representation** of G is a homomorphism

$$G \xrightarrow{\rho} \mathrm{Aut}(V) \simeq \mathrm{GL}_d(\mathbf{C}),$$

G acts linearly on V. ◊

Galois representations: Let G be a Galois group, possibly infinite. F be a field,

$$G_F = \mathrm{Gal}(\overline{F}/F) = \varprojlim_{L/F,\text{ fin. gal.}} \mathrm{Gal}(L/F)$$

profinite compact and totally disconnected.

Replace V with a finite free module over some topological ring A

$$\rho\colon G_F \to \mathrm{GL}_d(A)$$

a continuous homomorphism.

Example 2.2 $A = \mathbf{C}$ with the complex topology. □

Fact 2.3 *In this case* $\mathrm{im}(\rho)$ *is finite.*

Exercise 2.4 Prove this.

Then we can write

$$\begin{tikzcd} G_F \arrow[rr, "\rho"] \arrow[dr] & & \mathrm{GL}_d(\mathbf{C}) \\ & \mathrm{Gal}(L/F) \arrow[ur] & \end{tikzcd}$$

where L/F is finite. There are many such representations.

Conjecture 2.5 *Every finite group is a quotient of $G_{\mathbf{Q}}$.*

Example 2.6

$$F = \mathbf{Q}$$

$$L = \mathbf{Q}(\sqrt[4]{2}, i)$$

$$\mathrm{Gal}(L/\mathbf{Q}) \simeq D_4$$

$$G_{\mathbf{Q}} \to \mathrm{Gal}(L/\mathbf{Q}) \xrightarrow{\rho} \mathrm{GL}_2(\mathbf{C})$$

with ρ the unique irreducible 2-dimensional representation of D_4. □

Example 2.7 Let $E/\mathbf{Q}$ be an elliptic curve

$$G_{\mathbf{Q}} \circlearrowleft E[p] \simeq \mathbf{Z}/p \oplus \mathbf{Z}/p$$

$$\rho_{E,p} \colon G_{\mathbf{Q}} \longrightarrow \mathrm{Aut}(E[p]) \simeq \mathrm{GL}_2(\mathbf{F}_p)$$
$$\rho_{E,p^n} \colon G_{\mathbf{Q}} \longrightarrow \mathrm{Aut}(E[p^n]) \simeq \mathrm{GL}_2(\mathbf{Z}/p^n)$$
$$\rho_{E,p^\infty} \colon G_{\mathbf{Q}} \longrightarrow \mathrm{Aut}(E[p^\infty]) \simeq \mathrm{GL}_2(\mathbf{Z}_p).$$

□

Fact 2.8 *ρ_{E,p^∞} has finite image.*

Exercise 2.9 Prove this.

Example 2.10 Let $F = \mathbf{Q}_\ell$, $A = \mathbf{Q}_p$

$$\rho \colon G_{\mathbf{Q}_\ell} \longrightarrow \mathrm{GL}_d(\mathbf{Q}_p).$$

□

The Galois theory of local fields looks like

$$\begin{tikzcd}
\overline{\mathbf{Q}}_\ell \arrow[d, dash, "I_\ell^w"] \arrow[dd, dash, bend right, "I_\ell"'] \arrow[ddd, dash, bend right=60, "\mathrm{G}_\ell"'] & \\
\mathbf{Q}_\ell^{\mathrm{tr}} \arrow[d, dash, "\prod_{q\neq\ell} \mathbf{Z}_q(1)"] & \mathbf{Q}_\ell^{\mathrm{ab}} \\
\mathbf{Q}_\ell^{\mathrm{ur}} \arrow[d, dash, "\widehat{\mathbf{Z}}"] \arrow[ur, dash, bend right, "\mathbf{Z}_\ell^*"'] & \\
\mathbf{Q}_\ell &
\end{tikzcd}$$

where

$$\mathbf{Q}_\ell^{\mathrm{tr}} = \mathbf{Q}_\ell(\{\sqrt[n]{\ell}\}_{\ell\nmid n})$$

the maximal tamely ramified extension

$$\mathbf{Q}_\ell^{\mathrm{ur}} = \mathbf{Q}_\ell(\{\mu_n\}_{\ell\nmid n})$$

the maximal unramified extension

$$\mathbf{Q}_\ell^{\mathrm{ab}} = \mathbf{Q}_\ell^{\mathrm{un}}(\mu_{\ell^\infty})$$

the maximal abelian extension.

$$I_\ell = \mathrm{Gal}(\overline{\mathbf{Q}}_\ell/\mathbf{Q}_\ell^{\mathrm{ur}})$$

the intertia group

$$I_\ell^w = \mathrm{Gal}(\overline{\mathbf{Q}}_\ell/\mathbf{Q}_\ell^{\mathrm{tr}})$$

the wild intertia group

We say

$$\rho \colon G_{\mathbf{Q}_\ell} \longrightarrow \mathrm{GL}_d(\mathbf{Q}_p)$$

is **unramified** if

$$\rho(I_\ell) = \{1\}$$

is **tamely ramified** if

$$\rho(I_\ell^w) = \{1\}.$$

In the first case ρ is completely determined by $\rho(\mathrm{Frob}_\ell)$. In the second case ρ is completely determined by $\rho(\mathrm{Frob}_\ell)$ and its value on a generator of

$$\mathrm{Gal}(\mathbf{Q}_\ell^{\mathrm{tr}}/\mathbf{Q}_\ell^{\mathrm{ur}}).$$

The wild part: I_ℓ^w is pro-ℓ, $\mathrm{GL}_d(\mathbf{Z}_p)$ is almost pro-p (it has a finite index pro-p subgroup).

Exercise 2.11 Prove this.

Example 2.12 For $d = 1$

$$\mathbf{Z}_p^* = \mathbf{F}_p^* \times (1 + p\mathbf{Z}_p).$$

□

Thus if $\ell \neq p$ then

$$\rho(I_\ell^w) \subseteq \mathrm{GL}_d(\mathbf{Q}_p)$$

is finite.

Exercise 2.13 Prove this.

If $\ell = p$ then this is handled by p-adic Hodge theory.

The connection to global representations is then that

$$\begin{tikzcd} \overline{\mathbf{Q}} \arrow[r] & \overline{\mathbf{Q}}_\ell \\ \mathbf{Q} \arrow[r] \arrow[u] & \mathbf{Q}_\ell \arrow[u] \end{tikzcd}$$

So

$$G_{\mathbf{Q}_\ell} \hookrightarrow G_{\mathbf{Q}}$$

via restriction to $\overline{\mathbf{Q}}$.

The image of this map is the **decomposition group** at ℓ.

$$\rho\colon G_{\mathbf{Q}} \to \mathrm{GL}_d(A),$$

we say that ρ is **unramified at** ℓ if

$$\rho(I_\ell) = \{1\}.$$

In which case

$$\mathrm{charpoly}(\rho(\mathrm{Frob}_\ell))$$

is well-defined.

Returning to

$$\rho_{E,p^\infty}\colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Q}_p)$$

now.

Fact 2.14 *ρ_{E,p^∞} is unramified outside of $N_E \cdot p$ (N_E is the conductor of E). i.e.*

$$\rho_{E,p^\infty}$$

is unramified at ℓ if and only if $\ell \neq p$ and ℓ is a prime of good reduction for E.

So ρ_{E,p^∞} sees bad reduction.

From ρ_{E,p^∞} you can recover E up to isogeny (Faltings).

Example 2.15

$$G_{\mathbf{Q}} \circlearrowright \mu_{p^n}$$

so we get

$$G_{\mathbf{Q}} \to \mathrm{Aut}(\mu_{p^n}) \simeq (\mathbf{Z}/p^n\mathbf{Z})^* \simeq \mathrm{GL}_1(\mathbf{Z}/p^n)$$

taking the inverse limit we get

$$\begin{tikzcd} G_{\mathbf{Q}} \arrow[rr, "\epsilon_p"] \arrow[dr] & & \mathbf{Z}_p^* \\ & \mathrm{Gal}(\mathbf{Q}(\mu_{p^\infty})/\mathbf{Q}) \arrow[ur, "\sim"'] & \end{tikzcd}$$

this ϵ_p is known as the p-adic cyclotomic character. This is unramified outside p and

$$\epsilon_p(\mathrm{Frob}_\ell) = \ell$$

for $\ell \neq p$. □

Remark 2.16

$$\det(\rho_{E,p^\infty}) = \epsilon_p.$$

Example 2.17

$$f = \sum a_n q^n \in S_2(\Gamma_0(N), \mathbf{Q})$$

a weight 2 eigenform on $\Gamma_0(N)$, with rational fourier coefficients. Eichler-Shimura gives $E_f/\mathbf{Q}$ an elliptic curve. Define

$$\rho_f = \rho_{E,p^\infty} \colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Q}_p)$$

unramified outside Np

$$\mathrm{Tr}(\rho(\mathrm{Frob}_\ell)) = a_\ell$$

for $\ell \nmid Np$. More generally

$$f \in S_2(\Gamma_0(N))$$

an eigenform, Eichler-Shimura gives

$$A_f/\mathbf{Q}$$

an abelian variety which leads to

$$\rho_f \colon G_{\mathbf{Q}} \to \mathrm{GL}_2(K)$$

$K/\mathbf{Q}_p$ finite. □

2.2 Congruences and elliptic curves

Let

$$E_1 \colon y^2 = x^3 + x - 10$$

conductor $2^2 \cdot 13$, https://www.lmfdb.org/EllipticCurve/Q/52a1/

$$E_2 \colon y^2 = x^3 - 584x + 5444$$

conductor $2^2 \cdot 7 \cdot 13$, https://www.lmfdb.org/EllipticCurve/Q/364a1/.

Table 2.18 a_p**'s for** E_1, E_2

p	2	3	5	7	11	13	17	19	23	29
$a_p(E_1)$	0	0	2	-2	-2	-1	6	-6	8	2
$a_p(E_2)$	0	0	-3	1	-2	-1	-4	-1	-7	7

Note that

$$a_\ell(E_1) \equiv a_\ell(E_2) \pmod 5,\ \forall \ell \neq 7$$
$$\implies \rho_{E_1,5} \simeq \rho_{E_2,5} (= \bar{\rho})$$

as Galois representations.

Exercise 2.19 Prove this.

How common is this? We have 2 lifts of $\bar{\rho}$

$$\rho_{E_1,5^\infty} \simeq \rho_{E_2,5^\infty}$$

how many other such?

2.3 Hida theory

$$\sum a_n(f)q^n = f \in S_{k_0}(\Gamma_0(N))$$

an eigenform.

$$a_p(f)$$

a p-adic unit.

$$\mathscr{F} = \sum_{n=1}^{\infty} a_n(k)q^n$$

with a_n a p-adic analytic function in k. The whole family gives Galois representations that reduce to the same $\bar{\rho}$.

Specialise k to some integer w

$$\mathscr{F} = \sum a_n(w)q^n \in S_w(\Gamma_0(N))$$

take $w = k_0$ to recover f.

Hida constructs

$$\rho^{Hida} \colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}_p[[x]])$$

unramified outside Np.

$$\ell \nmid Np \implies \mathrm{tr}(\rho^{Hida}(\mathrm{Frob}_\ell)) = a_\ell(x).$$