

Deformation theory of Galois representations

MA842 at BU Spring 2020

Robert Pollack

February 4, 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>.

1 Motivation

Lecture 1 21/1/2020

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

$$f \equiv E_2^{(N)} \pmod{p''}.$$

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

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

a profinite group.

$$\rho: G_{\mathbf{Q}} \rightarrow \text{GL}_2(\mathbf{Q}_p)$$

a continuous homomorphism. Then view $\text{GL}_2(\mathbf{Q}_p)$ as $\text{Aut}(V)$ 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

$$\bar{\rho}: G_{\mathbf{Q}} \rightarrow \text{GL}_2(\mathbf{F}_p)$$

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

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

We say ρ_1, ρ_2 are deformations of

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

(imagine this is reducible).

Start with

$$\bar{\rho}: G_{\mathbf{Q}} \rightarrow \text{GL}_2(\mathbf{F}_p)$$

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

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

$$\rho^{\text{univ}}: G_{\mathbf{Q}} \rightarrow \text{GL}_2(R^{\text{univ}})$$

such that if $\rho: G_{\mathbf{Q}} \rightarrow \text{GL}_2(R)$ is a deformation of $\bar{\rho}$ then there exists

$$R^{\text{univ}} \rightarrow R$$

such that

$$\begin{array}{ccc} G_{\mathbf{Q}} & \xrightarrow{\rho^{\text{univ}}} & \text{GL}_2(R^{\text{univ}}) \\ & \searrow \rho & \downarrow \\ & & \text{GL}_2(R) \end{array}$$

1.2 Modular forms

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

an eigenform leads to

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

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 $\bar{\rho}$.

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

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

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

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

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

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

$$T: G \rightarrow A$$

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

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

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 23/1/2020

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

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

G acts linearly on V . ◇

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

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

profinite compact and totally disconnected.

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

$$\rho: G_F \rightarrow \text{GL}_d(A)$$

a continuous homomorphism.

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

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

Exercise 2.4 Prove this.

Then we can write

$$\begin{array}{ccc} G_F & \xrightarrow{\rho} & \text{GL}_d(\mathbf{C}) \\ & \searrow & \nearrow \\ & \text{Gal}(L/F) & \end{array}$$

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

$$F = \mathbf{Q}$$

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

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

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

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

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

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

$$\rho_{E,p}: G_{\mathbf{Q}} \rightarrow \text{Aut}(E[p]) \simeq \text{GL}_2(\mathbf{F}_p)$$

$$\rho_{E,p^n}: G_{\mathbf{Q}} \rightarrow \text{Aut}(E[p^n]) \simeq \text{GL}_2(\mathbf{Z}/p^n)$$

$$\rho_{E,p^\infty}: G_{\mathbf{Q}} \rightarrow \text{Aut}(E[p^\infty]) \simeq \text{GL}_2(\mathbf{Z}_p).$$

□

Fact 2.8 ρ_{E,p^∞} has finite image.

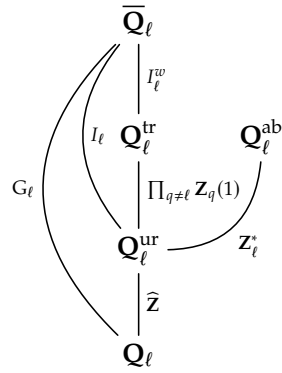
Exercise 2.9 Prove this.

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

$$\rho: G_{\mathbf{Q}_\ell} \rightarrow \text{GL}_d(\mathbf{Q}_p).$$

□

The Galois theory of local fields looks like



where

$$\mathbf{Q}_\ell^{\text{tr}} = \mathbf{Q}_\ell(\{\sqrt[n]{\ell}\}_{n \in \mathbf{N}})$$

the maximal tamely ramified extension

$$\mathbf{Q}_\ell^{\text{ur}} = \mathbf{Q}_\ell(\{\mu_n\}_{n \in \mathbf{N}})$$

the maximal unramified extension

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

the maximal abelian extension.

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

the inertia group

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

the wild inertia group

We say

$$\rho: G_{\mathbf{Q}_\ell} \rightarrow \text{GL}_d(\mathbf{Q}_p)$$

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

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

The wild part: I_ℓ^w is pro- ℓ , $\text{GL}_d(\mathbf{Z}_p)$ 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

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

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

$$\begin{array}{ccc} \overline{\mathbf{Q}} & \longrightarrow & \overline{\mathbf{Q}}_\ell \\ \uparrow & & \uparrow \\ \mathbf{Q} & \longrightarrow & \mathbf{Q}_\ell \end{array}$$

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 .

$$\rho: G_{\mathbf{Q}} \rightarrow \text{GL}_d(A),$$

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

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

In which case

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

is well-defined.

Returning to

$$\rho_{E,p^\infty}: G_{\mathbf{Q}} \rightarrow \text{GL}_2(\mathbf{Q}_p)$$

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

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

so we get

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

taking the inverse limit we get

$$\begin{array}{ccc} G_{\mathbf{Q}} & \xrightarrow{\epsilon_p} & \mathbf{Z}_p^* \\ & \searrow & \nearrow \sim \\ & \text{Gal}(\mathbf{Q}(\mu_{p^\infty})/\mathbf{Q}) & \end{array}$$

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

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

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

$$\rho_f = \rho_{E,p^\infty}: G_{\mathbf{Q}} \rightarrow \text{GL}_2(\mathbf{Q}_p)$$

unramified outside Np

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

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

$$\rho_f: G_{\mathbf{Q}} \rightarrow \text{GL}_2(K)$$

K/\mathbf{Q}_p finite. □

2.2 Congruences and elliptic curves

Let

$$E_1: y^2 = x^3 + x - 10$$

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

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

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

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

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.

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

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

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

take $w = k_0$ to recover f .

Hida constructs

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

unramified outside Np .

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

2.4 More examples of Galois representations in families

Lecture 3 28/1/2020

A 1-dimensional family. let

$$\epsilon_p = \text{cyclotomic character}$$

$$\epsilon_p: G_{\mathbf{Q}} \rightarrow \mathrm{Gal}(\mathbf{Q}(\mu_{p^\infty})/\mathbf{Q}) \simeq \mathbf{Z}_p^* \simeq \mathbf{F}_p^* \times (1 + p\mathbf{Z}_p)$$

If we have $k \in \mathbf{Z}$ we can take

$$\epsilon_p^k$$

its power.

Note that when $k_1, k_2 \in \mathbf{Z}$ with

$$k_1 \equiv k_2 \pmod{p-1}$$

then

$$\epsilon_p^{k_1} \equiv \epsilon_p^{k_2} \pmod{p}$$

moreover if

$$k_1 \equiv k_2 \pmod{(p-1)p^N}$$

we have

$$\epsilon_p^{k_1} \equiv \epsilon_p^{k_2} \pmod{p^{N+1}}.$$

Set

$$\Lambda = \mathbf{Z}_p[[\mathbf{Z}_p^*]] = \varprojlim \mathbf{Z}_p[(\mathbf{Z}/p^N)^*]$$

$$\epsilon_p^{univ} : G_{\mathbf{Q}} \rightarrow \Lambda^* = \mathrm{GL}_1(\Lambda)$$

$$\sigma \mapsto [\epsilon_p(\sigma)]$$

$$\Lambda \xrightarrow{wt_k} \mathbf{Z}_p$$

$$wt_k \circ \epsilon_p^{univ}$$

where wt_k is defined by

$$\mathbf{Z}_p^* \rightarrow \mathbf{Z}_p^* \subseteq \mathbf{Z}_p$$

$$x \mapsto x^k$$

gives

$$\Lambda \xrightarrow{wt_k} \mathbf{Z}_p.$$

Take any

$$\phi \in \mathrm{Hom}_{cts}(\Lambda, \mathbf{C}_p) \simeq \mathrm{Hom}_{cts}(\mathbf{Z}_p^*, \mathbf{C}_p)$$

induces

$$G_{\mathbf{Q}} \rightarrow \mathbf{C}_p^*$$

$$\phi \circ \epsilon_p^{univ}.$$

$$\mathrm{Hom}_{cts}(\mathbf{Z}_p^*, \mathbf{C}_p)$$

is a union of $p-1$ open disks as

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

the rightmost factor is topologically generated by $1+p$. So

$$\phi : \mathbf{Z}_p^* \rightarrow \mathbf{C}_p^*$$

is determined by

$$\phi|_{\mathbf{F}_p^*}$$

and

$$\phi(\gamma) \text{ for any } \gamma \text{ a top. gen..}$$

We need

$$|\phi(\gamma) - 1|_p < 1.$$

We have $p-1$ disks labelled by characters of \mathbf{F}_p^* . On each disk of $\phi \in \mathrm{Hom}(\mathbf{Z}_p^*, \mathbf{C}_p^*)$ the reduction of

$$\phi \circ \epsilon_p^{univ} : G_{\mathbf{Q}} \rightarrow \mathbf{C}_p^*$$

is the same.

A 2-d example. Let E/\mathbf{Q} be a CM elliptic curve.

$$\rho_{E,p^\infty}: G_{\mathbf{Q}} \rightarrow \mathrm{GL}_2(\mathbf{Z}_p)$$

then there exists K/\mathbf{Q} quadratic imaginary field and, if p is an ordinary prime

$$\psi: G_K \rightarrow \mathbf{Z}_p^*$$

s.t.

$$\rho_{E,p^\infty} \simeq \mathrm{Ind}_K^{\mathbf{Q}}(\psi).$$

So we get a “family”

$$\mathrm{Ind}_K^{\mathbf{Q}}(\psi^k),$$

more generally can make

$$\psi^{univ}: G_K \rightarrow \Lambda^*$$

$$\mathrm{Ind} \psi^{univ}: G_K \rightarrow \mathrm{GL}_2(\Lambda).$$

CM Hida family.

2.5 Deformation theory

G a profinite group, k a finite field of characteristic p (simpler $k = \mathbf{F}_p$).

$$\bar{\rho}: G \rightarrow \mathrm{GL}_d(k)$$

a continuous homomorphism.

To lift $\bar{\rho}$ to be A -valued, we need a homomorphism

$$A \twoheadrightarrow k$$

we may as well assume A is local so it lifts to $\mathrm{GL}_d(A)$. We then only have one residual representation. Localize it at

$$\ker(A \rightarrow k).$$

If A is a local ring then A has a natural topology. Letting \mathfrak{m}_A be the maximal ideal

$$\{\mathfrak{m}_A^j\}$$

is a neighborhood base at 0, this is the \mathfrak{m} -adic topology.

So we have A local, \mathfrak{m}_A maximal $A/\mathfrak{m}_A \simeq k$, we need to fix this identification to ensure we don't have automorphisms.

$$\begin{array}{ccc} G & \xrightarrow{\rho} & \mathrm{GL}_d(A) \\ & \searrow \bar{\rho} & \downarrow \\ & & \mathrm{GL}_d(k) \end{array}$$

Note 2.20 If we have $M \in \mathrm{GL}_d(A)$ s.t. $M \equiv 1 \pmod{\mathfrak{m}_A}$, then

$$M\rho M^{-1}$$

lifts $\bar{\rho}$ also.

Definition 2.21 Call ρ and $M\rho M^{-1}$ **strictly equivalent**.

◇

Definition 2.22 A deformation of $\bar{\rho}$ to A is a strict equivalence class of continuous homomorphisms

$$G \xrightarrow{\rho} \mathrm{GL}_d(A)$$

lifting $\bar{\rho}$. ◇

Want to rephrase this with less bases, instead of $\bar{\rho}$ use \bar{V} a d -dimensional continuous representation of G over k . V a free A -module of rank d with continuous action of G s.t.

$$V \otimes A/\mathfrak{m}_A \simeq \bar{V}.$$

Naive hope: two such V 's are equivalent if they are isomorphic as G -modules.

Problem: R^{univ} won't exist, too many automorphisms. Ideally if V_A is a deformation of \bar{V} to A then there exists a unique

$$R^{univ} \rightarrow A$$

inducing

$$V^{univ} \rightarrow V_A.$$

Take II, let V be a free A -module with a continuous action of G and a fixed isomorphism.

$$V \otimes_A A/\mathfrak{m}_A \simeq \bar{V}$$

as representations of G over $k \simeq A/\mathfrak{m}_A$.

Two V 's are equivalent if there exists a G -module isomorphism $V_1 \xrightarrow{\phi} V_2$ s.t.

$$\begin{array}{ccc} V_1 & \xrightarrow{\phi} & V_2 \\ \downarrow & & \downarrow \\ V_1 \otimes A/\mathfrak{m}_A & & V_2 \otimes A/\mathfrak{m}_A \\ \sim \downarrow & & \sim \downarrow \\ \bar{V} & \xrightarrow{=} & \bar{V} \end{array} .$$

Exercise 2.23 Check the two definitions are the same, GL_d definition vs. \bar{V} .

Another approach

$$\begin{array}{ccc} G & \xrightarrow{\rho} & \mathrm{GL}_d(A) \\ & \searrow \bar{\rho} & \downarrow \\ & & \mathrm{GL}_d(k) \end{array}$$

lift of $\bar{\rho}$ and say two ρ 's are the same if they are equal as maps, this is a **framed deformation**. We can write this more abstractly

$$\bar{V}$$

a continuous representation of G over k with fixed basis β .

$$V$$

a free A module with cont. action of G and a fixed isom.

$$V \otimes_A A/\mathfrak{m}_D \simeq \bar{V}$$

and a basis β_A lifting β .

Categories

$$C_k = C$$

the category of complete local Noetherian rings A with a fixed isomorphism $A/\mathfrak{m}_A \simeq k$. Where the maps are

$$A_1 \xrightarrow{\phi} A_2$$

a local ring homomorphism

$$\phi(\mathfrak{m}_{A_1}) \subseteq \mathfrak{m}_{A_2}$$

and the diagram

$$\begin{array}{ccc} A_1/\mathfrak{m}_{A_1} & \xrightarrow{\bar{\phi}} & A_2/\mathfrak{m}_{A_2} \\ & \searrow \sim & \swarrow \sim \\ & k & \end{array}$$

commutes.

Lecture 4 30/1/2020

Last time: multiplication by c on R^{univ} is not a ring map!

Exercise 2.24 Show that the “bad” definition of deformation (without fixing the isomorphism to \bar{V}) can’t be representable.

Exercise 2.25 If $\text{Aut}_G(\bar{\rho}) \supsetneq k^*$ show that the correct definition of deformation doesn’t lead to a representable functor.

k finite field of characteristic p . C_k category of complete local Noetherian rings with a fixed identification

$$A/\mathfrak{m}_A \simeq k$$

with (A, \mathfrak{m}_A) a local ring, maps are local homomorphisms preserving the fixed identification.

Witt vectors. $W(k)$ = Witt vectors of k and an object of C_k . The maximal ideal of $W(k)$ is $pW(k)$.

$$W(k)/pW(k) \simeq k$$

$$W(k)^\times \rightarrow k^\times$$

this map has a section which is multiplicative.

$$[x] \mapsto x.$$

Example 2.26 If $k \simeq \mathbb{F}_q$, $q = p^n$ then

$$W(k) = \mathcal{O}_{K_n}, K_n = \mathbb{Q}_p(\mu_{p^n-1})$$

unramified extension with

$$\mathfrak{m}_{W(k)} = (p)$$

take x^{q-1} and observe that its roots are distinct mod p . For $W(\mathbb{F}_p) \simeq \mathbb{Z}_p$. \square

$\bar{x} \in k$, lift to $x \in W(k)$

$$\lim_{m \rightarrow \infty} x^{q^m} = [x].$$

Exercise 2.27 Check this.

$A \in C_k$ there exists a unique ring hom

$$\begin{array}{ccc} W(k) & \longrightarrow & A \\ \downarrow & & \downarrow \\ k & \longrightarrow & A/\mathfrak{m}_A \end{array}$$

A is a $W(k)$ -module.

Moreover, A is a quotient of $W(k)[[x_1, \dots]]$. For $A, A' \in C_k$

$$A \xrightarrow{\phi} A'$$

in C_k then ϕ is automatically $W(k)$ -linear.

Deformation functor.

$$\bar{\rho}: G \rightarrow \mathrm{GL}_d(k)$$

$$D_{\bar{\rho}}: C_k \rightarrow \mathrm{Set}$$

$$A \mapsto \{\text{deformations of } \bar{\rho} \text{ to } A\} = \{\rho: G \rightarrow \mathrm{GL}_d(A) \text{ lifting } \bar{\rho}\} / \text{strict equiv.}$$

Given

$$R \in C_k$$

we have

$$F_R: C_k \rightarrow \mathrm{Set}$$

$$A \mapsto \mathrm{Hom}(R, A).$$

Exercise 2.28 If $A \xrightarrow{\phi} A'$ is a local ring Hom which is $W(k)$ -linear then ϕ is a map in C_k .

Definition 2.29 Representable functors. Any functor

$$F: C_k \rightarrow \mathrm{Set}$$

is said to be representable if there exists $R \in C_k$ such that

$$F \simeq F_R.$$

◇

To say $D_{\bar{\rho}}$ is representable says that

$$\exists R_{\bar{\rho}}^{univ} \in C_k$$

such that

$$D_{\bar{\rho}}(A) \simeq \mathrm{Hom}(R_{\bar{\rho}}^{univ}, A)$$

which is functorial in A .

In this set-up take $A = R_{\bar{\rho}}^{univ}$. Then

$$D_{\bar{\rho}}(R_{\bar{\rho}}^{univ}) \simeq \mathrm{Hom}(R_{\bar{\rho}}^{univ}, R_{\bar{\rho}}^{univ}) \ni 1$$

so this corresponds to some V^{univ}

Now given

$$\rho_A: G \rightarrow \mathrm{GL}_d(A) \simeq \mathrm{Aut}(V_A)$$

we have $\rho_A \in D_{\bar{\rho}}(A) \simeq \text{Hom}(R_{\bar{\rho}}^{univ}, A)$, so we get some $\phi: R_{\bar{\rho}}^{univ} \rightarrow A$. Giving a diagram

$$\begin{array}{ccc} D_{\bar{\rho}}(R_{\bar{\rho}}^{univ}) & \longrightarrow & \tilde{\text{Hom}}(R_{\bar{\rho}}^{univ}, R_{\bar{\rho}}^{univ}) \ni 1 \\ \phi \downarrow & & \downarrow \\ D_{\bar{\rho}}(A) & \longrightarrow & \tilde{\text{Hom}}(R_{\bar{\rho}}^{univ}, A) \ni \phi \end{array}$$

Framed deformations.

$$D_{\bar{\rho}}^{\square}(A) = \{\rho: G \rightarrow \text{GL}_d(A) \text{ lifting } \bar{\rho}\}$$

we will prove that

$$D_{\bar{\rho}}^{\square}$$

is in fact representable.

$$\bar{\rho}: G \rightarrow \text{GL}_d(k)$$

we build

$$R_{\bar{\rho}}^{\square, univ}$$

and

$$\rho_{\bar{\rho}}^{\square, univ}: G \rightarrow \text{GL}_d(R_{\bar{\rho}}^{\square, univ}).$$

Let $\{g_{\alpha}\}_{\alpha}$ be a generating set of G . Make formal variables X_{ij}^{α} for all α , $1 \leq i, j \leq d$.

$$R = W(k)[[\{X_{ij}^{\alpha}\}]]$$

try sending

$$g_{\alpha} \mapsto (X_{ij}^{\alpha}) \in M_d(R)$$

doesn't land in GL_d .

So "add on $\bar{\rho}$ ".

$$k \rightarrow W(k)$$

$$x \mapsto [x]$$

so we get

$$\text{GL}_d(k) \xrightarrow{[\cdot]} \text{GL}_d(W(k))$$

$$[(a_{ij})_{ij}] \mapsto ([a_{ij}])_{ij}$$

now send

$$g_{\alpha} \mapsto (X_{ij}^{\alpha}) + [\bar{\rho}(g_{\alpha})] \in \text{GL}_d(R)$$

this does not give a map

$$G \rightarrow \text{GL}_d(R)$$

because of relations between g_{α} .

Example 2.30 Take the relation

$$g_1 g_2^{-1} = e$$

need

$$((X_{ij}^1) + [\bar{\rho}(g_1)])((X_{ij}^2) + [\bar{\rho}(g_2)])^{-1} - 1 = 0$$

this gives d^2 equations in R . □

Can do this in general. In fact the LHS is in \mathfrak{m}_R . So if I is the ideal of all relations, then $I \subseteq \mathfrak{m}_R$. And let

$$R_{\bar{\rho}}^{univ, \square} = R/I.$$

$$\rho: G \rightarrow \mathrm{GL}_d(R/I)$$

$$g_\alpha \mapsto (X_{ij}^\alpha) + [\bar{\rho}(g_\alpha)] \pmod{I}$$

is a well-defined homomorphism. And it is universal: If

$$\rho_A: G \rightarrow \mathrm{GL}_d(A)$$

$$R \xrightarrow{\pi} A$$

$$(X_{ij}^\alpha)_{ij} \mapsto (\rho_A(g_\alpha) - [\bar{\rho}(g_\alpha)])_{ij}$$

then π kills I (exercise).

$$R/I \xrightarrow{\bar{\pi}} A.$$

Exercise 2.31 Check this induces ρ_A from the universal.

There are two problems with this, it is not necessary that the universal deformation we have constructed be continuous, or that the universal deformation ring be continuous.

The root of these problems is that there are potentially too many g_α . introduce a condition Φ_p that for all open finite index

$$G_0 \subseteq G$$

we have

$$\mathrm{Hom}(G_0, \mathbb{F}_p)$$

is finite.

Exercise 2.32

$$\mathrm{Hom}(G_0, \mathbb{F}_p)$$

is finite if and only if G^{pro-p} is topologically finitely generated. (this is Gouvea lemma 2.1)

If $G = G_K$ with K/\mathbb{Q}_ℓ finite, WLOG

$$G = G_0 = G_K$$

and Φ_p holds in this case

$$G_K^{\mathrm{ab}} \simeq \hat{K}^* \simeq \hat{\mathbf{Z}} \times \mathcal{O}_K^*$$

an exercise in LCFT

$$G_0 \subseteq G_K$$

fin index open then

$$G_0 = G_L$$

with L/\mathbb{Q}_p

Lecture 4 4/2/2020

Redo.

$$D_{\bar{\rho}}^{\square}: C \rightarrow \text{Set}$$

$$A \mapsto \left\{ \begin{array}{ccc} G & \xrightarrow{\rho} & \text{GL}_d(A) \\ & \searrow \bar{\rho} & \downarrow \\ & & \text{GL}_d(k) \end{array} \right\}$$

$$D_{\bar{\rho}}: C \rightarrow \text{Set}$$

$$A \mapsto D_{\bar{\rho}}^{\square} / \text{strict equiv.}$$

Theorem 2.33

1. $D_{\bar{\rho}}^{\square}$ is representable (by $R_{\bar{\rho}}^{\square}$)
2. If $\text{Aut}_G \bar{\rho} = k^{\times}$ then $D_{\bar{\rho}}$ is representable ($R_{\bar{\rho}}$).

Universal property: framed case:

$$\exists \rho_{univ}^{\square}: G \rightarrow \text{GL}_d(R_{\bar{\rho}}^{\square})$$

s.t. if ρ_A is a lift of $\bar{\rho}$ to A then there exists a unique

$$R_{\bar{\rho}}^{\square} \xrightarrow{\phi} A$$

which is in C s.t.

$$\begin{array}{ccc} G & \xrightarrow{\rho_{univ}^{\square}} & \text{GL}_d(A) \\ & \searrow \rho_A & \downarrow \phi^* \\ & & \text{GL}_d(A) \end{array}$$

unframed case: there exists a deformation $[\rho_{univ}]$ of $\bar{\rho}$ to $R_{\bar{\rho}}$ s.t. if $[\rho_A]$ is a deformation of $\bar{\rho}$ to A then there exists a unique

$$R_{\bar{\rho}} \xrightarrow{\phi} A$$

s.t

$$\phi^*([\rho_{univ}]) = [\rho_A].$$

$$D_{\bar{\rho}}^{\square}(R_{\bar{\rho}}^{\square}) = \text{Hom}(R_{\bar{\rho}}^{\square}, R_{\bar{\rho}}^{\square})$$

$$\rho_{univ}^{\square} \leftrightarrow 1.$$

Exercise 2.34 Check this universal property (also unframed case).

Last time.

$$R_{\bar{\rho}}^{\square} = W(k)[[\{X_{ij}^{\alpha}\}_{i,j,\alpha}]]/I_{relations}.$$

Introduced the condition

$$\Phi_p \forall \text{ open finite index } G_0 \subseteq G, \text{ Hom}(G_0, \mathbb{F}_p) \text{ is finite.}$$

This condition holds for G_K when K/\mathbf{Q}_ℓ is finite.

However it is false for G_K when K/\mathbf{Q} is finite. Such as $K = \mathbf{Q}$. As for $\ell \equiv 1 \pmod{p}$ then

$$G_{\mathbf{Q}} \rightarrow \text{Gal}(\mathbf{Q}(\mu_\ell)/\mathbf{Q}) \rightarrow \mathbf{F}_p$$

and there are infinitely many such ℓ 's

This is not a problem as the representations we are interested in, those coming from elliptic curves and modular forms, have good reduction outside a finite set of primes S . We may encode this into our deformation problem as follows: Let K/\mathbf{Q} finite and S a finite set of places of K and

$$K_S$$

be the maximal extension of K unramified outside of S . Then

$$G_{K,S} = \text{Gal}(K_S/K).$$

And Φ_p is true of $G_{K,S}$. The proof is an exercise in Global CFT. Silverman VIII prop. 1.6.

H profinite, let $H^{\text{pro-}p}$ be the maximal pro- p quotient of H .

Exercise 2.35 $\text{Hom}(H, \mathbf{F}_p)$ finite implies that $H^{\text{pro-}p}$ is topologically finitely generated. This is an equivalence in fact (lemma 2.1 Gouvea).

Existence of the framed deformation ring (take II). Assume G satisfies Φ_p .

$$\bar{\rho}: G \rightarrow \text{GL}_d(k),$$

$H = \ker(\bar{\rho})$ is finite index in G . Let

$$\rho_A: G \rightarrow \text{GL}_d(A)$$

lift $\bar{\rho}$.

$$\rho_A(H) \subseteq \ker(\text{GL}_d(A) \rightarrow \text{GL}_d(k)).$$

Exercise 2.36 Prove this is pro- p .

Hence $\rho_A|_H$ factors through $H^{\text{pro-}p}$.

Pick topological generators g_1, \dots, g_s of $H^{\text{pro-}p}$ (via Φ_p). Pick coset representatives g_s, \dots, g_t of G/H .

Run the argument from last time to get

$$R_{\bar{\rho}}^{\square} = W(k)[[\{X_{ij}^{\alpha}\}_{\alpha=1, \dots, t, i, j=1, \dots, d}]]/\overline{I_{\text{rel}}}.$$

Space of universal framed deformations.

$$\text{Hom}(R_{\bar{\rho}}^{\square}, A)$$

For unframed deformations it can be the case that we even have that

$$R_{\bar{\rho}} \simeq \mathbf{Z}_p[[X_1, X_2, X_3]]$$

$$A = \mathbf{Z}_p$$

$$D_{\bar{\rho}}(\mathbf{Z}_p) = \text{Hom}_C(\mathbf{Z}_p[[X_1, X_2, X_3]], \mathbf{Z}_p) \simeq (p\mathbf{Z}_p)^3.$$

To prove this space exists for unframed deformations, we have 3 options

1. We should have a bigger space of framed deformations in general, which should quotient down to that of unframed deformations, by forgetting the framing. Then we could construct $R_{\bar{\rho}}$ using this quotient. Kisin's notes chapter 3.
2. Pseudo-deformations (for later).
3. Schlessinger's criterion.

One dimensional examples.

$$\begin{array}{ccc} G & \xrightarrow{\bar{\rho}=\tilde{\chi}} & \mathrm{GL}_1(k) = k^\times \\ & \searrow \chi_A & \uparrow \\ & & A^\times \end{array}$$

$$1 \rightarrow 1 + \mathfrak{m}_A \rightarrow A^\times \rightarrow k^\times \rightarrow 1$$

$$A^\times \simeq k^\times \times (1 + \mathfrak{m}_A)$$

last term is free and k^\times is determined by $\bar{\chi}$.

Need

$$\begin{array}{ccc} G & \longrightarrow & 1 + \mathfrak{m}_A \\ & & \uparrow \\ & & G^{\mathrm{ab}, \mathrm{pro}-p} \end{array}$$

Any

$$\chi: G^{\mathrm{ab}, \mathrm{pro}-p} \rightarrow 1 + \mathfrak{m}_A$$

gives a deformation of $\tilde{\chi}$.

Claim 2.37

$$W(k)[[G^{\mathrm{ab}, \mathrm{pro}-p}]] \simeq R_{\tilde{\chi}}$$

$$\mathrm{Hom}_C(W(k)[[G^{\mathrm{ab}, \mathrm{pro}-p}]], A) \simeq \mathrm{Hom}(G^{\mathrm{ab}, \mathrm{pro}-p}, A^\times).$$

The universal character is then

$$G \rightarrow G^{\mathrm{ab}, \mathrm{pro}-p} \rightarrow W(k)[[G^{\mathrm{ab}, \mathrm{pro}-p}]]$$

$$\sigma \mapsto \sigma \mapsto \langle \sigma \rangle [\tilde{\chi}(\sigma)].$$

$$\chi_A: G \rightarrow A^{\ast} \text{????????}$$

check commutes

Example 2.38 $G = G_{\mathbf{Q}, \{p, \infty\}}$

$$G^{\mathrm{ab}} = G_{\mathbf{Q}, \{p, \infty\}}^a \quad b = \mathrm{Gal}(\mathbf{Q}(\mu_{p^\infty})/\mathbf{Q}) \simeq \mathbf{Z}_p^\ast$$

$$G^{\mathrm{ab}, \mathrm{pro}-p} \simeq 1 + p\mathbf{Z}_p \simeq \mathbf{Z}_p$$

$$R_{\tilde{\chi}} = \mathbf{Z}_p[[1 + p\mathbf{Z}_p]] \simeq \mathbf{Z}_p[[T]]$$

□