Deformation of Galois Representations

Brian Conrad

§1. Discrete Galois modules

F = field. $F_s | F$ = sep'ble closure, $G_F = \mathrm{Gal}(F_s|F) = \varprojlim_{\substack{F'|F \\ \text{finite} \\ \text{Galois}}} \mathrm{Gal}(F'|F)$

= compact, profinite gp

Krull: closed subgps $\Longleftrightarrow$ intermediate fields

open subgps $\Longleftrightarrow$ finite subextension

Ex V = comm. gp scheme of f.t. $/F$

$G_F \curvearrowright V(F_s) \ni m$ = abelian gp

acts $\curvearrowright$ $\left[\begin{array}{l} \mathrm{Spec}\, F_s \xrightarrow{m} V \\ V = \text{q-proj.}, \text{ so } V \hookrightarrow \mathbb{P}^N_F \\ \quad \text{and act by } G_F \\ \quad \text{on homog. coord.} \end{array}\right.$ (Same action)

any such m factors as follows:

$$\begin{tikzcd} \mathrm{Spec}\, F_s \arrow[r, "m"] \arrow[d] & V \\ \mathrm{Spec}\, F' \arrow[ur, "m'"'] & \end{tikzcd}$$

finite Galois $/F$

G_F action on any $m \in V(F') \underset{\text{subgp}}{\subset} V(F_s)$

have stabilizer $\mathrm{Gal}(F_s|F') \underset{\substack{\text{open} \\ \text{subgp}}}{\subset} \mathrm{Gal}(F_s|F) = G_F$

Ex. $\begin{array}{c} X \\ \downarrow \\ \mathrm{Spec}\, F \end{array}$ sep'td, f.t. $\quad \ell \neq \mathrm{char}\, F$.

$H^i_{\text{ét}}(X_{F_s}, \mathbb{Z}/\ell^n\mathbb{Z}) \curvearrowleft G_F$ acts w/ open stabilizers

Def. A discrete G_F-module is a G_F-module M s.t. every $m \in M$ has open stabilizer in G_F.

Ex. A G_F-module M w/ $\# M < \infty$ is discrete $\Leftrightarrow$ G_F acts on M through a finite quotient $\mathrm{Gal}(F'|F)$

(i.e. $G_{F'} \subset G_F$ acts trivially on M)

Rmk. If Γ is any pro-finite gp, we can make same discussion.

(Ex. $\Gamma = \mathbb{Z}_p$, $GL_n(\mathbb{Z}_p)$, ...)

$\pi_1^{et}(X, x)$

Ex. $E|F$ is an elliptic curve, $N \in \mathbb{Z}_{>0}$, char $F \nmid N$,

$E[N] := E[N](F_s) \simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ $\circlearrowleft$ G_F acts through $\mathrm{Gal}(\underbrace{F(E[N])}_{\text{ext'n gen. by coord. of } N\text{-torsion pts.}} | F)$

$\rho_{E,N} : G_F \xrightarrow{\text{cts}} \mathrm{Aut}(E[N]) \simeq GL_2(\mathbb{Z}/N\mathbb{Z})$ — chose bases

Consider $N = p^2$, $p =$ prime $\neq$ char F.

Fact

$$\begin{array}{ccc} E[p^{2+1}] & \overset{\text{chose}}{\simeq} & \mathbb{Z}/p^{2+1}\mathbb{Z} \times \mathbb{Z}/p^{2+1}\mathbb{Z} \\ \downarrow \times p & & \downarrow \text{reduction} \\ E[p^2] & \simeq & \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \end{array}$$

$\Rightarrow$ get

$$\begin{array}{ccc} & & \vdots \\ & & GL_2(\mathbb{Z}/p^{2}\mathbb{Z}) \\ & & \vdots \\ G_F & \xrightarrow{\rho_{E,p^2}} & GL_2(\mathbb{Z}/p^2\mathbb{Z}) \\ & \searrow^{\rho_{E,p}} & \downarrow \\ & & GL_2(\mathbb{Z}/p\mathbb{Z}) \end{array}$$

"deformation" of

Digression. $F = \mathbb{C}$, $E = \mathbb{C}/\Lambda$, $E[N] \simeq \frac{1}{N}\Lambda/\Lambda \overset{\times N}{\simeq} \Lambda/N\Lambda$

$$\begin{array}{ccc} E[N] & & \Lambda/N\Lambda \\ \uparrow \times d & & \uparrow \\ E[N\cdot d] & \xrightarrow{\sim} & \Lambda/Nd\Lambda \end{array}$$

$T_p(E)$ = p-adic Tate module

$\uparrow$ not a discrete G_F-module

$= \varprojlim_{\times p} E[p^n] \approx \mathbb{Z}_p \times \mathbb{Z}_p \circlearrowleft G_F$ $\mathbb{Z}_p$-linearly

$\Big(F = \mathbb{C},\ E \simeq \mathbb{C}/\Lambda,$

$T_pE = \varprojlim \Lambda/p^n\Lambda \simeq \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_p = H_1(E, \mathbb{Z}_p) \Big)$

$$\begin{tikzcd}
\rho_{E,p^\infty} : G_F \arrow[r, "cts"] \arrow[dr, bend right, "\rho_{E,p^n}"'] & GL_2(\mathbb{Z}_p) \arrow[d] \subset_{open} M_2(\mathbb{Z}_p) \\
& GL_2(\mathbb{Z}/p^n\mathbb{Z})
\end{tikzcd}$$

usually ker $\neq$ open

<u>Arithmetic application</u> – F = finite field, $\# F = q$, choose $\ell \neq \operatorname{char} F$.

$\rho_{E,\ell^\infty} : G_F \xrightarrow{cts} GL_2(\mathbb{Z}_\ell) = \operatorname{Aut}_{\mathbb{Z}_\ell}(T_\ell E)$

$\quad \ni \phi = \mathrm{Frob}_{F,q} : t \mapsto t^q$ on F_s.

char. poly. of ϕ-action $= X^2 - a_E X + q$, $\quad a_E = \boxed{\# E(F)} - (q+1) \in \mathbb{Z} \subset \mathbb{Z}_\ell$

<u>Ex</u> $\quad E$ = elliptic curve / $\mathbb{Q}_p$ $\qquad y^2 = x^3 + ax + b$

E' = elliptic curve / $\mathbb{Q}_p$ $\qquad y^2 = x^3 + a'x + b'$

Look at $G_{\mathbb{Q}_p}$-action on $E[p^7]$, $E'[p^7]$

$$G_{\mathbb{Q}_p} \rightrightarrows GL_2(\mathbb{Z}/p^7\mathbb{Z})$$

Suppose $|a'-a|, |b'-b| \ll 1$, $\quad$ <u>Fact</u>: If $|a'-a|, |b'-b| \ll 1$, $\rho_{E,p^7} \simeq \rho_{E',p^7}$ as $G_{\mathbb{Q}_p}$-modules

$$\begin{tikzcd}
& GL_2(\mathbb{Z}/p^7\mathbb{Z}) \\
\text{So}\ G_{\mathbb{Q}_p} \arrow[ur, bend left, "same"] \arrow[r, shift left, "\rho_{E,p^\infty}"] \arrow[r, shift right, "\rho_{E',p^\infty}"'] & GL_2(\mathbb{Z}_p) \arrow[u]
\end{tikzcd}$$

"two p-adic deformations" of same mod-p^7-representations.

§2. Cohomology

Γ = profinite gp. (eg. G_F)

Mod_Γ = cat. of discrete Γ-modules ($\neq \mathbb{Z}[\Gamma]$-mods)

Exer. Mod_Γ has enough injectives

$$\mathrm{Mod}_\Gamma \xrightarrow{\text{left exact}} Ab$$

$$M \longmapsto M^\Gamma := \{ m \in M : \gamma \cdot m = m, \ \forall \gamma \in \Gamma \}$$

Def. $H^*(\Gamma, -) : \mathrm{Mod}_\Gamma \to Ab$ derived functors of $(-)^\Gamma$.

Rmk. Can compute this using "cts cochains"

Ex. $H^1(\Gamma, M) = \dfrac{Z^1(\Gamma, M)}{B^1(\Gamma, M)}$ where

$$B^1(\Gamma, M) = \left\{ \Gamma \xrightarrow{cts} M : \begin{array}{l} \gamma \mapsto \gamma m_0 - m_0, \\ \text{some } m_0 \in M \end{array} \right\}$$

factors through $\Gamma / \mathrm{Stab}_\Gamma(m_0)$

$$Z^1(\Gamma, M) = \left\{ \Gamma \xrightarrow[cts]{c} M : \begin{array}{l} c(\gamma_1 \gamma_2) \\ = \gamma_1 \cdot c(\gamma_2) + c(\gamma_1) \end{array} \right\}$$

Say Γ acts trivially on M, so $B^1(\Gamma, M) = 0$, and $Z^1(\Gamma, M) = \mathrm{Hom}_{cts}(\Gamma, M)$.

Rmk. Given $\Gamma \xrightarrow[\varphi]{cts} \Gamma'$, then $\mathrm{Mod}_{\Gamma'} \longrightarrow \mathrm{Mod}_\Gamma$, and for $M' \in \mathrm{Mod}_{\Gamma'}$, have $(M')^{\Gamma'} \subset (M')^\Gamma$.

This induces $H^*(\Gamma', M') \longrightarrow H^*(\Gamma, M')$ (just comp. w/ φ on cochains)

$\underline{\text{Ex}}$. $F' | F$ field ext'n $(\mathbb{Q}_p | \mathbb{Q})$

$$\begin{array}{ccc} F_s & \overset{\text{choose}}{\hookrightarrow} & F'_s \\ | & & | \\ F & \hookrightarrow & F' \end{array}$$

induces $G_{F'} \xrightarrow{\text{cts}} G_F$ well-defined up to conjugation.

and $H^*(\Gamma', M') \longrightarrow H^*(\Gamma, M')$ is $\underline{\text{invariant}}$ under conjugation action by Γ'.

$$\Rightarrow H^*(G_F, M) \xrightarrow{\text{canonical}} H^*(G_{F'}, M)$$

$$(= H^*(F, M) \longrightarrow H^*(F', M))$$

pullback w.r.t. $\operatorname{Spec} F' \longrightarrow \operatorname{Spec} F$.

$\underline{\text{Ex}}$ $F = \mathbb{Q}$, $H^1(G_{\mathbb{Q}}, \mathbb{Z}/2\mathbb{Z}) = \operatorname{Hom}_{\text{cts}}(G_{\mathbb{Q}}, \mathbb{Z}/2\mathbb{Z})$

$$\overset{\text{set}}{=} \{ \underset{\mathbb{Q}(\sqrt{1})}{\overset{\shortparallel}{\mathbb{Q}}},\ \mathbb{Q}(\sqrt{d}),\ d \in \mathbb{Z} - \{0\} \text{ square free} \}$$

$\underline{\text{NOT}}$ f.dim'l over $\mathbb{Z}/2\mathbb{Z}$

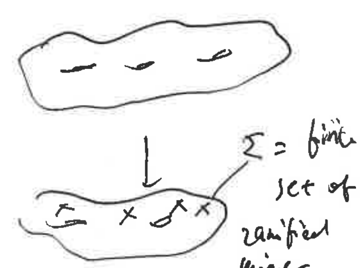
We want to work w/ a quotient of $G_{\mathbb{Q}}$ subject to restricted ramification.

F = # field $([F:\mathbb{Q}] < \infty)$, $\operatorname{Spec} \mathcal{O}_F$

What should replace G_F ? for $F' | F$ finite, $\operatorname{Spec} \mathcal{O}_{F'}$

$$\downarrow$$

want to consider $F' | F$ ramified $\subset \Sigma$ = fixed finite set $\operatorname{Spec} \mathcal{O}_F$ of max'l ideals of $\mathcal{O}_F$



i.e. replace G_F w/ $\pi_1^{et}(\mathrm{Spec}\, \mathcal{O}_{F,\Sigma})$

i.e. $G_{F,\Sigma} = \mathrm{Gal}(F_\Sigma | F)$ — compositum of $F'|F$ finite unramified outside Σ.

= profinite gp

Basic algebraic no. theory $(+\varepsilon) \Rightarrow$

Thm (Tate) (1) If M is a finite discrete $G_{F,\Sigma}$-module, then $\# H^i(G_{F,\Sigma}, M) < \infty$, $\forall i$

$(= 0$ for $i > 2$ if $\# M =$ odd$)$

(2) If $[L : \mathbb{Q}_p] < \infty$, then $H^i(G_L, M) =$ finite for $M =$ finite discrete G_L-module

and $= 0$, $\forall i > 2$.

Ex. $F = \mathbb{Q}$, $\Sigma = \{2, 3, 7\}$, $H^1(G_{\mathbb{Q},\Sigma}; \mathbb{Z}/2\mathbb{Z}) \overset{\text{set}}{=} \{ \mathbb{Q}(\sqrt{d}) : \text{sq free } d \mid 42 \}$

$=$ finite.

§3. Deformations (Motivation: Hida constructed certain rep'n $\rho : G_{\mathbb{Q},\Sigma} \to GL_2(\mathbb{Z}_p[\![X]\!])$

s.t. under $X \mapsto (1+p)^k - 1$ $(k \geq 2)$

gave interesting rep'ns

$\rho_k : G_{\mathbb{Q},\Sigma} \to GL_2(\mathbb{Z}_p)$).

Fix a rep'n $\bar{\rho} : \Gamma \xrightarrow{\text{cts}} GL(V_0)$

Γ = profinite

$GL(V_0)$: V_0 = f. dim'l vec. sp. $/k$ = finite field

$(\simeq GL_N(k))$

$\hat{\mathcal{C}}_k$ = complete local noeth. rings w/ residue field k $(=$ coeff. ring $\Lambda = W(k))$

Pancb

A <u>lifting</u> of $\bar\rho$ to $A \in \hat{\mathcal{C}}_k$ is a pair (V_A, θ) where V_A = finite free A-module

equipped w/ cts $\rho: \Gamma \to GL(V_A)$ $(\simeq GL_N(A))$

and $\theta: V_A/m_A V_A \simeq V_0$ as $k[\Gamma]$-modules.

Say $(V_A, \theta) \simeq (V_A', \theta')$ if $\exists\, V_A \simeq V_A'$ as $A[\Gamma]$-modules s.t.

mod m_A carries θ to θ' (i.e. respect identification w/ V_0)

A <u>deformation</u> of $\bar\rho$ to A is an $\simeq$ class of lifts.

$\bar\rho: \Gamma \longrightarrow GL_N(k)$

<u>Matrix meaning</u>. lifting: $\rho: \Gamma \xrightarrow{cts} GL_N(A)$ s.t. $\rho \bmod m_A = \bar\rho$

$\rho \sim \rho'$: $\rho = M \circ \rho' \cdot M^{-1}$, $M \in GL_N(A)$, $M \equiv 1 \bmod m_A$.

? If $\begin{matrix} E \\ \downarrow \\ S \end{matrix}$ = p-adic variety, is a family of ell. curves

$\forall s \in S(\mathbb{Q}_p)$, get $\rho_s: G_{\mathbb{Q}_p} \to GL_2(\mathbb{Z}_p)$ from E_s,

but these don't come from a single rep'n $G_{\mathbb{Q}_p} \longrightarrow GL_2(\mathbb{Z}_p[[x_1, x_2, \cdots]])$

<u>Def</u>: $\mathrm{Def}_{\bar\rho}: \hat{\mathcal{C}}_k \longrightarrow \mathrm{Set}$

$A \mapsto \{\text{deformations of } \bar\rho \text{ to } A\}$ <u>NOT</u> liftings

Functor ✓ (using $V_A \rightsquigarrow A' \underset{A}{\otimes} V_A$)

<u>Ex</u>. $\mathrm{Def}_{\bar\rho}(k[\varepsilon]) = H^1(\Gamma, \mathrm{End}_k(V_0))$ ← Γ acts by conjugation on $\Gamma: V_0 \to V_0$.

"Pf"

$$\bar{\rho} : \Gamma \longrightarrow GL_N(k)$$

$$\rho : \Gamma \longrightarrow GL_N(k[\varepsilon]) \quad \text{lifting } \bar{\rho} = ??$$

$$\rho(\gamma) = \big(1 + \varepsilon \cdot \underset{\substack{\uparrow \\ M_N(k)}}{c(\gamma)}\big)\bar{\rho}(\gamma)$$

ρ = cts homomorphism (lifting) $\iff$ $c \in Z^1_{cts}(\Gamma, \mathrm{End}(V_0))$

$\rho \sim \rho'$ $\iff$ $c - c' \in B^1(\Gamma, \mathrm{End}(V_0))$

<u>Thm</u> (Mazur) If $\dim H^1(\Gamma, \mathrm{End}\, V_0) < \infty$, then $\mathrm{Def}_{\bar{\rho}}$ satisfies (H1) – (H3)

If $\mathrm{End}_\Gamma(V_0) = k$, (e.g. $\bar{\rho}$ = abs irred.), then (H4) holds, so get a <u>universal</u> deformation $\bar{\rho}^{univ} : \Gamma \longrightarrow GL_N(R^{univ}_{\bar{\rho}})$.

i.e.
$$\begin{tikzcd}
\Gamma \arrow[r, "\bar{\rho}^{univ}"] \arrow[rr, bend left, "\rho"] \arrow[dr, "\bar{\rho}"'] & GL_N(R^{univ}_{\bar{\rho}}) \arrow[r] \arrow[d] & GL_N(A) \arrow[dl] \\
& GL_N(k) &
\end{tikzcd}$$

$\exists!\ R^{univ}_{\bar{\rho}} \longrightarrow A$

(carries $\bar{\rho}^{univ}$ to ρ up to 1-unit matrix conjugation !!!

<u>Ex.</u> $\Gamma = G_{\mathbb{Q},\Sigma}$.

Want to impose <u>more</u> condition!