Families of Galois representations and families of automorphic forms - an introduction

Tuesday, March 25, 2008
12:29 PM

Calegari: $K/\mathbb{Q}$ Galois ext'n. $G = \mathrm{Gal}(K/\mathbb{Q})$.

$\mathcal{O}_K$ = ring of integers of K
$\cup\!|$
$\mathfrak{p}$

$K_\mathfrak{p}/\mathbb{Q}_p$ a Galois ext'n. $\mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p) \twoheadrightarrow \mathrm{Gal}\left((\mathcal{O}_K/\mathfrak{p})/(\mathbb{Z}/p)\right)$

$\mathfrak{p}$ unramified $\Leftrightarrow$ this is an isomorphism

In this case, we get an distinguished element in $\mathrm{Gal}(K/\mathbb{Q})$, the Frobenius at $\mathfrak{p}$, denoted $\sigma_\mathfrak{p} \in \mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p) \subseteq \mathrm{Gal}(K/\mathbb{Q})$.

If $\tau: \mathfrak{p} \to \tau\mathfrak{p}$, then $\sigma_{\tau\mathfrak{p}} = \tau\sigma_\mathfrak{p}\tau^{-1}$.

So given $p \in \mathbb{Q}$, we get a conjugacy class $\sigma_p = \langle \sigma_\mathfrak{p} \rangle$.

=.

By Chebotarev Density thm, every element in G is a Frobenius for ∞ many conjugacy classes.

Furthermore, the collection σ_p together with G determine K.

=

the same analysis applies to any Galois extension K/F (F a # fld), now the Frobenius conjugacy classes are indexed by primes in F.

=

Fix a set of primes S of F, set $(S \supseteq \infty)$

$$G_{F,S} = \varprojlim_{\substack{K \text{ unramified} \\ \text{outside } S}} \mathrm{Gal}(K/F).$$

$G_{F,S}$ is a topological grp with neighborhood basis around the identity given by the kernels of maps

$$G_{F,S} \longrightarrow \mathrm{Gal}(K/F)$$

topologically generated by Frobenius classes over primes outside S.

=.

$G_{F,S}$ has a Frob. class $\langle \sigma_{\mathfrak{p}} \rangle$ for $\mathfrak{p} \subseteq \mathcal{O}_F$, $\mathfrak{p} \notin S$.

<u>Assumption</u>: $|S| < \infty$ ($\Rightarrow$ $\sigma_{\mathfrak{p}}$ topologically generate $G_{F,S}$)

<u>Example</u>: $S = \{\infty\}$, $F = \mathbb{Q}$, $G_{\mathbb{Q},S} = \{1\}$ (Minkowski)

A natural way to study a topological grp is to study its representations.

$S = \{p, \infty\}$ $\quad G_{\mathbb{Q},S} \supseteq G(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$

$\cong \mathbb{Z}_p^\times$.

$$\mathrm{Gal}(\mathbb{Q}(\mu_{p^k})/\mathbb{Q})$$

$$\mu_{p^k} \mapsto (\mu_{p^k})^a \quad \downarrow \wr$$

$$a \qquad (\mathbb{Z}/p^k\mathbb{Z})^\times$$

If $\ell \neq p$, then what is the image of σ_ℓ in $(\mathbb{Z}/p^k\mathbb{Z})^\times$? Answer: ℓ.

$$G_{\mathbb{Q},S} \xrightarrow{\sim} \mathbb{Z}_p^\times$$

$$\langle \sigma_\ell \rangle \mapsto \ell \qquad (\text{for } \ell \neq p).$$

Thursday, April 03, 2008
8:04 AM

Kronecker-Weber:

$$G^{ab}_{\mathbb{Q}, \{p,\infty\}} \cong \mathbb{Z}_p^\times.$$

(Dirichlet's thm on a. p. $\Rightarrow$ ℓ's generate $\mathbb{Z}_p^\times$.)

(Chebotarev's thm can be viewed as a generalization of Dirichlet's Thm to the non-abelian case.)

We want to study $G_{F,S}$ by considering its continuous representations.

$$\rho: G_{F,S} \to GL_n(E)$$

together with $\langle \rho(\sigma_\ell) \rangle$

(i) $E = \mathbb{C}$

(ii) $E = \mathbb{F}_q \subseteq \overline{\mathbb{F}}_p$

(iii) $E =$ finite extension of $\mathbb{Q}_p$

In (i), (ii), $\operatorname{Im}\rho$ is finite.

In (iii) $\operatorname{Im}\rho$ may be infinite. Ex: $E = \mathbb{Q}_p$,

$$\begin{tikzcd} \chi: G_{\mathbb{Q},\{p,\infty\}} \arrow[r] \arrow[d] & \mathbb{Z}_p^\times \arrow[d] \\ GL_1(\mathbb{Q}_p) \arrow[r, phantom, "\cong"] & \mathbb{Q}_p^\times \end{tikzcd}$$

χ the (p-adic) cyclotomic character.

<u>Lemma</u>: Let $[E:\mathbb{Q}_p] < \infty$. Let $\rho: G_{F,S} \to GL_n(E)$ be continuous, then after conjugation, the image lands in $GL_n(\mathcal{O}_E)$.

Pf: Think of $\rho(g)$, for $g \in G_{F,S}$, as an endomorphism on a vector space V of dim n over E. Choose an $\mathcal{O}_E$-lattice inside V, say L. Consider the $\mathcal{O}_E[G_{F,S}]$-module generated by L, call it L'. By continuity, L' is compact $\Rightarrow$ $L' \subseteq \frac{1}{p^r} L$ for some r.

continuity, L' is compact $\Rightarrow$ $L' \subseteq \frac{1}{p^r} L$ for some r.

So L' is a lattice. $\square$.

The upshot of this is that we can consider the reduction

$$\begin{tikzcd} \rho: G_{F,S} \arrow[r] \arrow[dr, "\bar{\rho}"'] & GL_n(\mathcal{O}_E) \arrow[d] \\ & GL_n(\mathcal{O}_E/m_E) = GL_n(\mathbb{F}_q) \end{tikzcd}$$

In summary, we can break down our problem of studying ρ into:

(1) Understand all maps $\bar{\rho}: G_{F,S} \to GL_n(\mathbb{F}_q)$ (Hard)

(2) Given $\bar{\rho}$, understand all "lifts" $\bar{\rho} \rightsquigarrow \rho: G_{F,S} \to GL_n(\mathcal{O}_E) \hookrightarrow GL_n(E)$. (Easier)

(Why: $\ker(GL_n(\mathcal{O}_E) \to GL_n(\mathbb{F}_q))$ is solvable, since it's pro-p.

One therefore can utilize induction and CFT.)

Problem 2:

$\bar{\rho} : G_{F,S} \to GL_n(k) \qquad k = \mathbb{F}_q$.

[As a special case, consider lifting the Galois action on the reduction of a zero dimension variety over G_E. The answer is provided by Hensel's lemma.].

We will only consider the case that $\bar{\rho}$ is absolutely irred.

$(\bar{\rho} : G_{F,S} \to GL_n(k) \to GL_n(\overline{\mathbb{F}}_q)$ is irred.)

① Try to lift to $GL_n(k[\varepsilon]/\varepsilon^2)$

Let $\mathcal{C}$ = the category of complete local noetherian rings (A, m) with $A/m = k$.

(with a morphism $A \to k$)

The maps between objects are given by

$$\begin{tikzcd} A \arrow[r] \arrow[d] \arrow[dr, phantom, "\circlearrowright"] & A' \arrow[d] \\ A/m \cong k \arrow[r, Rightarrow, "id"'] & A'/m' \cong k \end{tikzcd}$$

A representation $\rho : G_{F,S} \to GL_n(A)$ is the same as an a free, rank n module V_A with a continuous action by $G_{F,S}$. (through ρ)

& $\bar{\rho} \leftrightarrow V_k$ over k.

<u>Def</u>: V_A is a <u>deformation</u> of V_k if $V_A \otimes_A A/m \simeq V_k$.

<u>Def</u>: V_A and V_A' are <u>strictly equivalent</u> if $\exists$ a commutative diagram $V_A \xrightarrow{\sim} V_A'$ such that

$$\begin{tikzcd} V_A \arrow[r, "\sim"] \arrow[d] \arrow[dr, phantom, "\circlearrowright"] & V_{A'} \arrow[d] \\ V_k \arrow[r, equal, "id"'] & V_k \end{tikzcd}$$

We have a functor $D : \mathcal{C} \to \text{Sets}$

$A \mapsto D(A) = \{\text{the strict equivalence class of deformations } [V_A]\}$

The concrete problem is: (taking $A = k[\varepsilon]/\varepsilon^2$)

What is $D(k[\varepsilon]/\varepsilon^2)$?

$=$.

Study $A = k[\varepsilon]/\varepsilon^2$:

$$0 \to \underset{\varepsilon A}{\overset{\shortparallel}{k}} \to A \to k \to 0 \qquad \text{a s.e.s. of } k\text{-modules}$$

$\Downarrow$

$$0 \to V_k \to V_A \to V_k \to 0$$

It follows that given $[c] \in D(k[\varepsilon]/\varepsilon^2)$, $[c]$ can be viewed as an element in $\mathrm{Ext}^1_{k[G_{F,S}]}(V_k, V_k)$.

Given $[c]$, choose a basis for V_k. $\sigma \in G_{F,S}$ then acts as

$$\begin{pmatrix} X(\sigma) & Y(\sigma) \\ & X(\sigma) \end{pmatrix}$$ a map from V_k to V_k

Fix a (vector space) splitting $\psi^{-1} : V_k \to V_A$, then

$\sigma \in G_{F,S} \mapsto \mathrm{Hom}(V_k, V_k)$

$(\sigma . \psi^{-1}(p) \mapsto \psi^{-1}(\sigma p))$

more explicitly $(Y(\sigma)p, X(\sigma)p) \mapsto (0, X(\sigma)p)$

form a subspace $\cong V_k$.

(Suppose $V_A \cong V_k \oplus V_k$ w.r.t. the splitting given by ψ, then $(p \overset{\psi^{-1}}{\mapsto} (0,p) \overset{\sigma}{\longrightarrow} (Y(\sigma)p, X(\sigma)p))$)

$\downarrow$

$p \mapsto \sigma \cdot p = X(\sigma) \cdot p \mapsto (0, X(\sigma) \cdot p)$

$\therefore [c]$ gives a class (on a co-cycle) $G_{F,S} \longrightarrow \mathrm{Hom}_k(V_k, V_k)$

in $H^1(G_{F,S}, \mathrm{Hom}_k(V_k, V_k))$

$\underbrace{\qquad\qquad}_{\mathrm{Ad}\,V_k}$

$=$.

$D(k[\varepsilon]/\varepsilon^2)$ "$=$" $\mathrm{Ext}^1_{k[G_{F,S}]}(V_k, V_k)$ "$=$" $H^1(G_{F,S}, \mathrm{Ad}(V_k))$

- gives k-vector space structure to $D(k[\varepsilon]/\varepsilon^2)$
- we see that $H^1(G_{F,S}, \mathrm{Ad}(V_k))$ is finite:

Let $G_{F,S}$ act on $\mathrm{Ad}\,V_k$ via $\mathrm{Gal}(K/F)$, then

(inf-res) $$0 \to \underbrace{H^1(\mathrm{Gal}(K/F), \mathrm{Ad}V_k)}_{\text{finite}} \longrightarrow H^1(G_{F,S}, \mathrm{Ad}\,V_k) \to \underbrace{H^1(G_{K,S}, \mathrm{Ad}V_k)}_{= \mathrm{Hom}_k(G_{K,S}, \mathrm{Ad}V_k)}$$

$=$.

Thm (Mazur): The functor D is representable.
i.e., $\exists\, R$ in $\mathcal{C}$ s.t. $D(A) = \mathrm{Hom}_{\mathcal{C}}(R, A)$.

(only finite many exts of a fixed degree that are unramified outside a finite set of primes.)

Interpretation: $\exists$ (an equivalence class of) $\rho_{univ}: G_{F,S} \longrightarrow GL(V_R)$ lifting $\bar{\rho}$

s.t. given any $\rho_A: G_{F,S} \longrightarrow GL(V_A)$ lifting $\bar{\rho}$,

$$\begin{tikzcd} & GL(V_A) \arrow[d] \\ & GL(V_k) \arrow[from=ul, phantom] \end{tikzcd}$$

$\bar{\rho} \searrow$ $GL(V_k)$

$\exists!\; R \xrightarrow{\varphi} A$ s.t.

$$\begin{tikzcd} G_{F,S} \arrow[r, "\rho_{univ}"] & GL_n(R) \arrow[r, "\varphi"] \arrow[d] & GL_n(A) \arrow[dl] \\ & GL_n(k) & \end{tikzcd}$$

$\varphi \circ \rho_{univ} = \rho_A$. (up to equivalence)

$\llcorner$.

Ex:

$S = \{p, \infty\}$ $\quad F = \mathbb{Q}$, $\quad n = 1$.

$$\begin{tikzcd} G_{\mathbb{Q},S} \arrow[r] \arrow[dr] & A^\times \\ & \mathbb{Z}_p^\times \arrow[u] \end{tikzcd}$$

$\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \cong \mathbb{Z}_p^\times$

Fix $\bar{\rho} : G_{\mathbb{Q},S} \longrightarrow k^\times = \mathbb{F}_q^\times$ $\left(\overset{\bar{\rho}}{\underset{\text{powers of } \chi}{=}}\right)$

then $\rho : G_{\mathbb{Q},S} \longrightarrow A^\times$

$$\begin{tikzcd} G_{\mathbb{Q},S} \arrow[d] & & \\ \mathbb{Z}_p^\times \arrow[r] & k^\times \hookrightarrow A^\times & \\ (\mathbb{Z}/p\mathbb{Z})^\times \oplus (1+p\mathbb{Z}_p) & 1+m_A & \end{tikzcd}$$

$\mathbb{Z}_p^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \oplus (1+p\mathbb{Z}_p)$, $(\mathbb{Z}/p\mathbb{Z})^\times \xrightarrow{\bar{\rho}} k^\times$, $(1+p\mathbb{Z}_p) \to 1+m_A$

$D(A) = 1+m_A$. (different choices of uniformizer do not give equivalent representations.)

$R = \mathbb{Z}_p[[T]]$

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p[[T]], A) & = & m_A \\ \downarrow & & \downarrow \\ \mathbb{F}_p & = & \mathbb{F}_p \end{array}$$

Given R, what is $D(k[\varepsilon]/\varepsilon^2)$?

$\mathrm{Hom}(R, k[\varepsilon]/\varepsilon^2)$

$m_R \to \varepsilon k[\varepsilon]/\varepsilon^2$

$$\begin{array}{ccc} R & \longrightarrow & k[\varepsilon]/\varepsilon^2 \\ \downarrow & & \downarrow \\ k & = & k \end{array}$$

So $\underset{k\text{-modules}}{\mathrm{Hom}}(m_R, k) = \mathrm{Hom}(m_R/(m_R^2, p), k) = D(k[\varepsilon]/\varepsilon^2)$

If $R = \mathbb{Z}_p[[T]]$, $\quad \overset{(p,T)\cdot\mathbb{Z}_p[[T]]}{\overset{\shortparallel}{m}} / \overset{(T^2,p)\mathbb{Z}_p[[T]]}{(m^2, p)} \cong \mathbb{F}_p \cdot T \Rightarrow D(\mathbb{F}_p[\varepsilon]/\varepsilon^2) = \mathbb{F}_p$.

also can be realized as:

- $(\mathrm{Hom}_{\mathbb{F}_p}(\mathbb{F}_p[T], \mathbb{F}_p)) \cong \mathbb{F}_p$.
- $\mathrm{Ext}^1_{\mathbb{F}_p[G_{\mathbb{Q},\{p,\infty\}}]}(\mathbb{F}_p, \mathbb{F}_p)$ $\qquad \begin{pmatrix} 1 & * \\ & 1 \end{pmatrix}$, $* \in \mathbb{F}_p$
- $H^1(G_{\mathbb{Q},\{p,\infty\}}, \mathbb{F}_p)$

Thursday, April 03, 2008
2:13 PM

$\dim \mathrm{Hom}_{k\text{-mod}}(\mathfrak{m}, k)$ $=$ $\dim T_{(m)}$

Let $d_1 = \dim H^1(G_{F,S}, \mathrm{Ad}\,V_k) = \dim \mathrm{Hom}_{k\text{-mod}}(R, k[\varepsilon]/\varepsilon^2)$

$\rightsquigarrow R = W(k)[[T_1, T_2, \ldots, T_{d_1}]]/I.$ (Because $\mathrm{Hom}_{k\text{-mod}}(R, k[\varepsilon]/\varepsilon^2)$ $=$ Tangent space of R at the closed pt)

What is the obstruction to lifting?

$$\rho : G_{F,S} \to GL_n(A/I)$$
$$\downarrow$$
$$GL_n(A/I^2)$$

consider a set-theoretic lift γ

$c(\sigma, \tau) := \gamma(\sigma\tau)\gamma(\tau)^{-1}\gamma(\sigma)^{-1}$

$\in \mathbb{1} + \underbrace{M_n(I)}$ mod I^2

$I \otimes \mathrm{Ad}(V_{A/I})$ $n \times n$ matrix with entries in I

$\in H^2(G_{F,S}, \mathrm{Ad}(V_{A/I}) \otimes I)$

If $H^2(G_{F,S}, \mathrm{Ad}\,V_k) = 0$, then R = smooth $\Rightarrow I = 0$.

Let $d_2 = \dim H^2(G_{F,S}, \mathrm{Ad}\,V_k)$

$I \otimes R/\mathfrak{m}$ has dimension $= d_2$.

# of generators of $I = d_2$.

We can't say much about d_1, d_2.

But we can say something about $d_1 - d_2$. (using Euler characteristic)

Assume $S \supseteq$ primes dividing p. Then $d_1 - d_2 = 1 + n^2[F:\mathbb{Q}] - \sum_{v|\infty} \dim H^0(G_v, \mathrm{Ad}\,V_k)$

n^2 if $G_v = \{1\}$

(If $n=1$, then $d_1 - d_2 = 1 + r_1 + 2r_2 - r_1 - r_2$

$\dim (\mathrm{Ad}\, V_k)^{\{\pm 1\}}$ $G_v = \{\pm 1\}$

(depends on the sign of the rep $\bar{\rho}$)

n^2 if even

n if odd (?)

Conj: $d_1 - d_2 =$ Krull dim of R/pR

($\leq$ we know)

(Hard: even for $n=1$, correct Krull dim (i.e. equality above) $\Leftrightarrow$ Leopoldt's conj.)

$n=2$, $\bar{\rho}(c) = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ even $\qquad$ $\bar{\rho}(c) = \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$ odd

$d_1 - d_2 = 1 + 4 - 4 = 1$ $\qquad$ $d_1 - d_2 = 1 + 4 - 2 = 3$

Roughly how to prove $R = T$?

- dim of the tangent space : $\dim_k \mathrm{Hom}_{k\text{-mod}}(R, k[\varepsilon]/\varepsilon^2)$
- replace R by something closer to the smooth one ...