Seminario de modularidad de representaciones de Galois (2020-1): Representaciones de $G_{\mathbb{Q}_\ell}$ sobre $\mathbb{Z}_\ell$-módulos, II

Héctor Pastén

Pontificia Universidad Católica de Chile

2020/06/09

Panorama:

Tenemos una representación de Galois $\rho = \rho_{E,\ell} : G_{\mathbb{Q}} \to GL_2(\mathbb{Q}_\ell)$ y queremos demostrar que es modular. El concepto clave son las deformaciones de ρ, es decir, ρ' tal que $\rho' \equiv \rho \bmod \ell$.

- El teorema de modularidad vendrá de un isomorfismo de anillos "$R_\rho \simeq T_\rho$" donde R_ρ clasifica deformaciones de ρ y T_ρ es cierta álgebra de Hecke que clasifica las deformaciones de ρ que son *modulares*. (Notación improvisada –habrá más parámetros)
- No se va a demostrar directamente el isomorfismo. Más bien se construirá un morfismo sobreyectivo $R_\rho \to T_\rho$ ("toda deformación modular es en particular una deformación") y se va a demostrar que es isomorfismo combinando resultados de álgebra conmutativa con información numérica.
- *Ejemplo de juguete*. Demostrar que una función $\mathbb{R}$-lineal $f : \mathbb{R}^m \to \mathbb{R}^n$ es isomorfismo porque (1) es sobreyectiva; (2) $m \leq n$; (3) criterio numérico $\dim im(f) + \dim \ker(f) = \dim dom(f)$.

Panorama:

- Para eso se necesitará saber un número asociado a R_ρ, la llamada "dimensión tangencial". Habrá que demostrar que es dada por una fórmula que involucra el orden de grupos de Selmer $H^1_{\mathcal{L}}(G_{\mathbb{Q}}, ad^0(\rho))$.
- ¿Por qué los Selmer? $H^1_{\mathcal{L}}(G_{\mathbb{Q}}, ad^0(\bar{\rho}))$ está "hecho" de los $H^1(G_p, ad^0(\bar{\rho}))$ que clasifican deformaciones infinitesimales (valores en $O_n[\epsilon]/\epsilon^2$ –visto clase pasada). No es lo mismo que las deformaciones clasificadas por R_ρ, pero es un punto de partida para obtener una fórmula para la dimensión tangencial de R_ρ.
- Entonces vamos a querer una fórmula para $H^1_{\mathcal{L}}(G_{\mathbb{Q}}, ad^0(\bar{\rho}))$. Wiles nos da (tomar $M = ad(\bar{\rho})$)

$$\frac{\# H^1_{\mathcal{L}}(\mathbb{Q}, M)}{\# H^1_{\mathcal{L}^*}(\mathbb{Q}, M^*)} = \frac{\# H^0(G_{\mathbb{Q}}, M)}{\# H^0(G_{\mathbb{Q}}, M^*)} \prod_v \frac{\# L_v}{\# H^0(G_v, M)}$$

- Habrá elegir bien las condiciones locales L_v de modo que esto sea calculable. La clase anterior y hoy: en el caso más difícil, $v = \ell$.

Notación

- $\ell > 2$ un primo. $G_\ell = G_{\mathbb{Q}_\ell}$, ϵ_ℓ carácter ciclotómico ℓ-ádico.
- $K/\mathbb{Q}_\ell$ extensión finita. $\mathcal{O}$ anillo de enteros de K, $k = \mathcal{O}/m$ campo residual, $\lambda \in m$ uniformizador, $\mathcal{O}_n = \mathcal{O}/\lambda^n$.
- Ejemplo: $K = \mathbb{Q}_\ell$, $\mathcal{O} = \mathbb{Z}_\ell$, $\mathcal{O}_n = \mathbb{Z}/\ell^n\mathbb{Z}$, $k = \mathbb{F}_\ell$.
- Donde haya topología, todo es continuo.
- M "discreto": un $\mathcal{O}[G]$-módulo de cardinalidad finita (así que es $\mathcal{O}_n[G]$-módulo para algún n).
- M "profinito": límite proyectivo del caso discreto.
- R una $\mathcal{O}$-álgebra local noetheriana completa con campo residual k (ejemplo: con $\mathcal{O} = \mathbb{Z}_\ell$, puede ser $R = \mathbb{Z}_\ell[[T_1, \ldots, T_n]]$)

$\mathcal{O}[G_\ell]$-módulos semiestables

Sea M un $\mathcal{O}[G_\ell]$-módulo profinito.

- M es *bueno* si todo cuoeciente discreto M' de M tiene un esquema de grupo finito plano $\mathcal{F}/\mathbb{Z}_\ell$ tal que $M' \simeq \mathcal{F}(\overline{\mathbb{Q}_\ell})$ como $\mathbb{Z}_\ell[G]$-módulo.
- M es *ordinario* si hay una secuencia exacta

$$(0) \to M^{(-1)} \to M \to M^{(0)} \to (0)$$

de $\mathcal{O}[G_\ell]$-módulos profinitos tal que I_ℓ actúa trivial en $M^{(0)}$ y actúa como multiplicación por ϵ_ℓ en $M^{(-1)}$. (Ojo: ¡la inercia!)

Cualquiera de los dos casos se dice *semiestable*.

Representaciones semiestables

Sea R una $\mathcal{O}$-álgebra local noetheriana completa con campo residual k. Una representación $\rho : G_\ell \to GL_2(R)$ es buena/ordinaria/semiestable si el módulo subyacente M_ρ ($\simeq R^2$) lo es, y además

$$\det(\rho|_{I_\ell}) = \epsilon_\ell.$$

Notación: $\overline{\rho} = \rho \bmod \mathfrak{m}_R$, a valores en $GL_2(k)$.

$ad(\rho)$ clasificando deformaciones infinitesimales

$\rho : G_\ell \to GL_2(\mathcal{O}_n)$. $ad(\rho) : G_\ell \to GL(End(\mathcal{O}_n^2))$ acción
$\sigma \cdot f = \rho(\sigma) f \rho(\sigma)^{-1}$. Subespacio de traza 0: $ad^0(\rho)$.
Dado $\xi : G_\ell \to M_{ad(\rho)}$ cociclo tenemos una representación deformada infinitesimalmente:

$$\rho_\xi : G_\ell \to GL_2(R_n), \quad \sigma \mapsto (Id + \epsilon \xi(\sigma))\rho(\sigma)$$

donde $R_n = \mathcal{O}_n[\epsilon]/(\epsilon^2)$. Notar: $\rho_\xi \bmod \epsilon = \rho$.
Sea $D_\rho(R_n)$ el conjunto de ϵ-deformaciones de ρ módulo equivalencia por conjugación de $Id + \epsilon M_{2\times 2}(R_n)$.

Lema

La construcción anterior da una biyección $H^1(G_\ell, ad(\rho)) \approx D_\rho(R_n)$.

Nota: $H^1(G_\ell, ad(\rho)) := H^1(G_\ell, M_{ad(\rho)})$ y $M_{ad(\rho)} \simeq \mathcal{O}_n^4$.

$ad^0(\rho)$ clasificando deformaciones infinitesimales

Definimos $D_\rho^{\det}(R_n)$ como el conjunto de ϵ-deformaciones $\rho' : G_\ell \to GL_2(R_n)$ de ρ, salvo conjugación por $\mathrm{Id} + \epsilon M_{2\times 2}(R_n)$, con la condición que $\det \rho' = \det \rho$. Notar:

$$\det((1+\epsilon\xi(\sigma))\rho(\sigma)) = \det \rho(\sigma) \iff tr(\xi(\sigma)) = 0.$$

Lema

La construcción $\xi \mapsto \rho_\xi$ induce una biyección $H^1(G_\ell, ad^0(\rho)) \approx D_\rho^{\det}(R_n)$.

Esto es lo que realmente nos va a interesar: ϵ-deformaciones de ρ que tienen su mismo determinante. Es un conjunto más pequeño que todas las ϵ- deformaciones, y es suficiente.

$ad(\rho)$ clasificando extensiones

ξ cociclo $\mapsto E_\xi$ el $R_n[G_\ell]$-módulo subyacente a ρ_ξ.
Obs: $E_\xi/\epsilon E_\xi \simeq M_\rho$ y además $\epsilon E_\xi \simeq M_\rho$. Así que tenemos una secuencia exacta

$$0 \to M_\rho \to E_\xi \to M_\rho \to 0.$$

Esta es una clase en $Ext^1_{\mathcal{O}_n[G_\ell]}(M_\rho, M_\rho)$ en la categoría de $\mathcal{O}_n[G_\ell]$-módulos profinitos.

Lema

La construcción anterior da $H^1(G_\ell, ad(\rho)) \simeq Ext^1_{\mathcal{O}_n[G_\ell]}(M_\rho, M_\rho)$.

$ad(\rho)$ clasificando extensiones

Estamos calculando cohomologías de O_n-módulos, no simplemente grupos abelianos. Así que los H^1 son O_n-módulos.

Lema

La construcción anterior da $H^1(G_\ell, ad(\rho)) \simeq Ext^1_{\mathcal{O}_n[G_\ell]}(M_\rho, M_\rho)$.

- $H^1_{ss}(G_\ell, ad(\rho)) \subseteq H^1(G_\ell, ad(\rho))$ de define como la imagen de aquellas extensiones en la categoría de $\mathcal{O}_n[G_\ell]$-módulos profinitos semiestables.
- $H^1_f(G_\ell, ad(\rho)) \subseteq H^1_{ss}(G_\ell, ad(\rho))$ es lo mismo, salvo que ρ sea buena, en cuyo caso se usa la sub-categoría de extensiones buenas.
- $H^1_\bullet(G_\ell, ad^0(\rho)) := H^1_\bullet(G_\ell, ad(\rho)) \cap H^1(G_\ell, ad^0(\rho))$

El caso ordinario

En el caso ordinario: Elegir base $\rho = \left(\begin{smallmatrix} \epsilon_\ell \psi_1 & * \\ 0 & \psi_2 \end{smallmatrix}\right)$ con ψ_j no-ramificados

- $W = \{\left(\begin{smallmatrix} 0 & * \\ 0 & 0 \end{smallmatrix}\right)\} \subseteq ad^0(\rho)$ cf. p.67 [DDT] $W = ad^{(-1)}(\rho)$
- $L_\ell = \ker\left(H^1(G_\ell, ad^0(\rho)) \to H^1(I_\ell, ad^0(\rho)/W)\right)$
  Esto esencialmente pide que $\xi|_{I_\ell} \in W$, de modo que ρ_ξ también es ordinaria.

En el caso ordinario tenemos $H^1_{ss}(G_\ell, ad^0(\rho)) = L_\ell$. Usaremos esta presentación alternativa. La acción en W es

$$\begin{pmatrix} \epsilon_\ell \psi_1 & * \\ 0 & \psi_2 \end{pmatrix} \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \epsilon_\ell \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & \epsilon_\ell \psi_1 \psi_2^{-1} x \\ 0 & 0 \end{pmatrix}$$

De esto, un cálculo da
Lema. $\#H^0(G_\ell, W^*) = \#\mathcal{O}_n / (\frac{\psi_1}{\psi_2}(Frob_\ell) - 1)\mathcal{O}_n$ con la acción en $\mathcal{O}_n \simeq W$.

El caso ordinario

$$u : H^1(G_\ell, ad^0(\rho)) \to H^1(G_\ell, ad^0(\rho)/W)$$

Por inflación-restricción tenemos la sec. exacta

$$0 \to H^1(G/I, (ad^0(\rho)/W)^I) \to H^1(G, ad^0(\rho)/W) \to_r H^1(I, ad^0(\rho)/W)^{G/I}$$

entonces $L_\ell = \ker(r \circ u)$ y $H^1(G, ad^0(\rho))/L_\ell \simeq im(r \circ u)$. Por exactitud

$$\begin{aligned}
\#im(r \circ u) &\geq \#im(u)/\ker(r) \\
&= \#im(u)/\#H^1(G/I, (ad^0(\rho)/W)^I) \\
&= \#im(u)/\#H^0(G, ad^0(\rho)/W)
\end{aligned}$$

El caso ordinario

Tomando $H^*(G,-)$ en la sec exacta $0 \to W \to ad^0(\rho) \to ad^0(\rho)/W \to 0$ obtenemos

$$\begin{aligned} 0 &\to H^0(W) \to H^0(ad^0) \to H^0(ad^0/W) \\ &\to H^1(W) \to H^1(ad^0) \to im(u) \to 0 \end{aligned}$$

y usando que el orden es multiplicativo en secuencias exactas nos da

$$\begin{aligned} \frac{\#L_\ell}{\#H^0(G,ad^0(\rho))} &= \frac{\#H^1(G,ad^0)}{\#H^0(G,ad^0)\#im(r\circ u)} \\ &\le \frac{\#H^1(G,ad^0)\#H^0(G,ad^0(\rho)/W)}{\#H^0(G,ad^0)\#im(u)} \\ &= \frac{\#H^1(G,W)}{\#H^0(G,W)} \\ &= \#\mathcal{O}_n \cdot \#H^0(G,W^*) \end{aligned}$$

donde lo último es inmediato de la fórmula para característica de Euler.

El caso ordinario

Finalmente podemos acotar el factor en $v=\ell$ de la fórmula de Wiles:

$$\begin{aligned}\frac{\#L_\ell}{\#H^0(G,ad^0(\rho))} &\leq \#\mathcal{O}_n\cdot\#H^0(G,W^*)\\ &= \#\mathcal{O}_n\cdot\#\mathcal{O}_n/(\frac{\psi_1}{\psi_2}(Frob_\ell)-1)\mathcal{O}_n.\end{aligned}$$

El caso ordinario

En resumen:
Teorema. En el caso ordinario definir

$$L_\ell = \ker\left(H^1(G_\ell, ad^0(\rho)) \to H^1(I_\ell, ad^0(\rho)/W)\right)$$

Entonces $H^1_{ss}(G_\ell, ad^0(\rho)) = L_\ell$ y el factor en $v = \ell$ en la fórmula de Wiles para grupos de Selmer de $ad^0(\rho)$ cumple

$$\frac{\#L_\ell}{\#H^0(G, ad^0(\rho))} \leq \#\mathcal{O}_n \cdot \#\mathcal{O}_n/(\frac{\psi_1}{\psi_2}(Frob_\ell) - 1)\mathcal{O}_n.$$

El caso ordinario

Con cálculos similares se puede demostrar una mejor fórmula si ρ es ordinaria pero no-buena. Los cálculos están en la p.116 del capítulo de Washington en [Modular forms and Fermat's Last Theorem] (editado por Cornell-Silverman-Stevens)

Teorema. En el caso ordinario no-bueno definir

$$L'_\ell = \ker\left(H^1(G_\ell, ad^0(\rho)) \to H^1(G_\ell, ad^0(\rho)/W)\right)$$

Entonces $H^1_{ss}(G_\ell, ad^0(\rho)) = H^1_f(G_\ell, ad^0(\rho)) = L'_\ell$ y el factor en $v = \ell$ en la fórmula de Wiles para grupos de Selmer de $ad^0(\rho)$ cumple

$$\frac{\# L'_\ell}{\# H^0(G, ad^0(\rho))} = \#\mathcal{O}_n.$$

El caso bueno no-ordinario será explicado en la próxima charla.