Seminario de modularidad de representaciones de Galois (2020-1)

Héctor Pastén

Pontificia Universidad Católica de Chile

2020/05/08

Contenido de hoy:

La construcción de Shimura.

- Ingrediente: una newform $f \in S_2(\Gamma)$ para el álgebra de Hecke $\mathbb{T}_{\mathbb{Z}}$.
- Resultado: una variedad abeliana A_f definida sobre $\mathbb{Q}$ cuya función L viene de la función L de f.

Si el tiempo lo permite, hablaremos de curvas elípticas modulares en más generalidad.

Más álgebra lineal

Sea L un campo, V un espacio vectorial sobre L, y sea $A \leq End(V)$ un anillo conmutativo unitario.

- Sea $v \in V$ un vector propio simultáneo para todo $t \in A$. Sea $K_v \subseteq L^{alg}$ el campo generado por todos los valores propios en v de los $t \in A$.
- Escribimos $\lambda_v(t)$ por el valor propio de t en v para todo $t \in A$. Entonces
$$\lambda_v : A \to K_v$$
es un morfismo de anillos. Tiene una imagen $im(\lambda_v) \subseteq K_v$ que es un anillo, y tiene un kernel $\mathcal{I}_v = \ker(\lambda_v) \subseteq A$.
- Si v' es otro vector propio simultáneo de todo A tal que hay un isomorfismo $\sigma : K_v \to K_{v'}$ que cumple $\lambda_{v'} = \sigma\lambda_v$ entonces el kernel es el mismo: $\mathcal{I}_v = \mathcal{I}_{v'}$.

El morfismo λ_f y el ideal $\mathcal{I}_f$

Fijamos N y un grupo $\Gamma_1(N) \subseteq \Gamma \subseteq \Gamma_0(N)$.

- Sea $f \in S_2(\Gamma)$ una newform de nivel $m|N$. Así,

$$f = q + a_2(f)q^2 + ... \in S_2(\Gamma)$$

- Sea $O_f = \mathbb{Z}[a_n(f) : n \geq 1]$ y $K_f = \mathbb{Q}(a_n(f) : n \geq 1)$. Así, O_f es un orden en el campo de números K_f. Como f es eigenform, de los valores propios de f obtenemos un morfismo de anillo:

$$\lambda_f : \mathbb{T}_\mathbb{Z} \to K_f$$

- Definimos $\mathcal{I}_f = \ker(\lambda_f) \subseteq \mathbb{T}_\mathbb{Z}$.
- Si $\sigma \in G_\mathbb{Q}$ entonces f^σ es newform de nivel m y cumple que $\sigma : K_f \to K_{f^\sigma}$ es isomorfismo. Además $\lambda_{f^\sigma} = \sigma\lambda_f$.
- Entonces $\mathcal{I}_f = \mathcal{I}_{f^\sigma} = \mathcal{I}_{[f]}$ solo depende de $[f] =$ (la $G_\mathbb{Q}$-clase de f).
- Además, λ_f induce el isomorfismo $\mathbb{T}_\mathbb{Z}/\mathcal{I}_f \simeq O_f$.

La variedad abeliana A_f, versión algebraica

- $\mathbb{T}_\mathbb{Z}$ actúa en J_Γ, y esa acción es con endomorfismos definidos sobre $\mathbb{Q}$ gracias a la interpretación modular.
- En particular $\mathcal{I}_f \cdot J_\Gamma$ es una sub-variedad abeliana de J_Γ definida sobre $\mathbb{Q}$: es subgrupo, y es conexa porque $0 \in t \cdot J_\Gamma$ para todo $t \in \mathbb{T}_\mathbb{Z}$.
- Se define $A_f := J_\Gamma / \mathcal{I}_f \cdot J_\Gamma$. Es una variedad abeliana definida sobre $\mathbb{Q}$.
- Viene con un morfismo de proyección $p_f : J_\Gamma \to A_f$ definido sobre $\mathbb{Q}$ cuyo kernel $\mathcal{I}_f J_\Gamma$ es conexo.
- Dado que J_Γ es un $\mathbb{T}_\mathbb{Z}$-módulo, tenemos que

$$A_f = J_\Gamma / \mathcal{I}_f J_\Gamma \simeq J_\Gamma \otimes_{\mathbb{T}_\mathbb{Z}} \mathbb{T}_\mathbb{Z} / \mathcal{I}_f \simeq J_\Gamma \otimes_{\mathbb{T}_\mathbb{Z}, \lambda_f} O_f$$

  donde O_f es una $\mathbb{T}_\mathbb{Z}$-álgebra via $\lambda_f : \mathbb{T}_\mathbb{Z} \to O_f$.
- En particular, A_f adquiere una estructura de O_f-módulo, y por ende, de $\mathbb{T}_\mathbb{Z}$-módulo via λ_f. Con esta acción, el cuociente $p_f : J_\Gamma \to A_f$ es $\mathbb{T}_\mathbb{Z}$-equivariante.

La variedad abeliana A_f, versión analítica

Vamos a calcular la dimensión de A_f. Para eso basta ver su construcción cerca de $0 \in J_\Gamma$, o más formalmente, en el espacio tangente en 0 sobre $\mathbb{C}$:

$$Tan_0 J_\Gamma^{an} = H^0(J_\Gamma^{an}, \Omega^1)^\vee \simeq H^0(X_\Gamma^{an}, \Omega^1)^\vee \simeq S_2(\Gamma)^\vee$$

como módulos sobre $\mathbb{T}_\mathbb{Z}$.

- $S_2(\Gamma)^\vee \simeq \mathbb{T}_\mathbb{C} \simeq S_2(\Gamma)$ como $\mathbb{T}_\mathbb{C}$-módulos, en particular como $\mathbb{T}_\mathbb{Z}$-módulos. Así que $Tan_0 J_\Gamma^{an} \simeq S_2(\Gamma)$ como $\mathbb{T}_\mathbb{Z}$-módulos.
- Entonces $Tan_0(\mathcal{I}_f J_\Gamma) \simeq \mathcal{I}_f Tan_0(J_\Gamma) \simeq \mathcal{I}_f \cdot S_2(\Gamma)$.
- Escribimos $S_2(\Gamma) = \bigoplus_g S_g$ (suma sobre g newforms de nivel $d|N$)
- $\mathcal{I}_f S_2(\Gamma) = \bigoplus_{g \notin [f]} S_g$. Así, $Tan_0(A_f) \simeq S_2(\Gamma)/\mathcal{I}_f S_2(\Gamma) \simeq \bigoplus_{g \in [f]} S_g$.
- $\dim A_f = \dim Tan_0(A_f) = \dim \bigoplus_{g \in [f]} S_g = [K_f : \mathbb{Q}]\sigma_0(N/m)$.
- **Teorema.** Si f es newform de nivel N, entonces $\boxed{\dim A_f = [K_f : \mathbb{Q}].}$

La variedad abeliana A_f, versión aritmética

Desde ahora asumimos f newform de nivel N.

- $\mathbb{T}_{\mathbb{Z}}$ actúa en A_f via λ_f, es decir, $End_{\mathbb{Q}}(A_f)$ es una O_f-álgebra.
- Hay un resultado más preciso, pero difícil (f newform de nivel N): **Teorema.** $End_{\mathbb{Q}}(A_f) \otimes \mathbb{Q} \simeq K_f$. En particular A_f es simple sobre $\mathbb{Q}$.
- La acción de O_f en A_f da a $\mathcal{V}_\ell(A_f)$ la estructuda de un $K_f \otimes \mathbb{Q}_\ell$-módulo, y por ende, un $\mathbb{T}_{\mathbb{Q}_\ell}$-módulo via λ_f.
- Obtenemos un morfismo $p_{f,*} : \mathcal{V}_\ell(J_\Gamma) \to \mathcal{V}_\ell(A_f)$ que es
  - $G_{\mathbb{Q}}$-equivariante, y
  - $\mathbb{T}_{\mathbb{Q}_\ell}$-equivariante.
- Las acciones de $G_{\mathbb{Q}}$ y $\mathbb{T}_{\mathbb{Q}_\ell}$ en $\mathcal{V}_\ell(J_\Gamma)$ y $\mathcal{V}_\ell(A_f)$ conmutan porque $\mathbb{T}_{\mathbb{Z}}$ actua en J_Γ por endomorfismos definidos sobre $\mathbb{Q}$.
- Notamos que $p_{f,*} : \mathcal{V}_\ell(J_\Gamma) \to \mathcal{V}_\ell(A_f)$ es lo mismo que $\mathcal{V}_\ell(J_\Gamma) \to \mathcal{V}_\ell(J_\Gamma)/\mathcal{V}_\ell(\mathcal{I}_f J_\Gamma) \simeq \mathcal{V}_\ell(J_\Gamma) \otimes_{\mathbb{T}_{\mathbb{Q}_\ell}} (K_f \otimes \mathbb{Q}_\ell)$.
- Como $\mathcal{V}_\ell(J_\Gamma)$ es libre de rango 2 sobre $\mathbb{T}_{\mathbb{Q}_\ell}$ obtenemos **Corolario.** $\mathcal{V}_\ell(A_f)$ es libre de rango 2 sobre $K_f \otimes \mathbb{Q}_\ell$.

Reducción de J_Γ módulo p, con $p \nmid N$

Si $p \nmid N$ entonces X_Γ tiene buena reducción, y por ende J_Γ también. Como A_f es cuociente de J_Γ, también tiene buena reducción en p.

Teorema. Si $p \nmid N\ell$, entonces el polinomio característico de *Frob* en $\mathcal{V}_\ell(J_\Gamma)$ visto como $\mathbb{T}_{\mathbb{Q}_\ell}$-módulo (libre de rango 2) es $X^2 - T_pX + p\langle p\rangle$.

Dem. Eichler-Shimura: T_p y $Frob + \langle p\rangle Ver$ actúan igual en $\mathcal{V}_\ell(J_\Gamma \otimes \mathbb{F}_p) \simeq \mathcal{V}_\ell(J_\Gamma)$ (usamos $\ell \neq p$). Así que como endomorfismos de $\mathcal{V}_\ell(J_\Gamma)$ obtenemos

$$F^2 - T_pF + p\langle p\rangle = F^2 - (F + \langle p\rangle V)F + p\langle p\rangle = -\langle p\rangle VF + p\langle p\rangle = 0.$$

Finalmente basta que $tr(F) = T_p$. Con el pairing de Weil modificado se calcula que $tr(F) = tr(\langle p\rangle V)$ (ver cálculo de p.42-43 [DDT]) y así

$$2tr(F) = tr(F) + tr(\langle p\rangle V) = tr(F + \langle p\rangle V) = tr(T_p) = 2T_p.$$

$\square$

Interludio: curvas elípticas

La teoría de Weil para conteo de puntos en variedades abelianas no se suele ver en pregrado. Así que recordaremos el caso elemental de una curva elíptica $E/\mathbb{F}_p$ que es suficiente para aclarar ideas. Fijar $\ell \neq p$.

- Contando puntos fijos de $F = Frob$ actuando en $E(\mathbb{F}_p^{alg})$ llegamos a

$$\#E(\mathbb{F}_p) = 1 - a_p(E) + p = 1 - tr_{\mathbb{Q}_\ell}(F|\mathcal{V}_\ell(E)) + p.$$

- El teorema de Hasse nos da que los valores propios de F son $\alpha, \beta \in \mathbb{Q}^{alg} \subseteq \mathbb{Q}_\ell^{alg}$ con $|\alpha|_{\mathbb{C}} = |\beta|_{\mathbb{C}} = \sqrt{p}$ y $\alpha\beta = p$. En particular se obtiene la conocida cota de Hasse: $|a_p(E)| = |\alpha + \beta| \leq 2\sqrt{p}$
- Otra forma de escribir lo anterior es:

$$\#E(\mathbb{F}_p) = 1 - (\alpha + \beta) + \alpha\beta = (1 - \alpha)(1 - \beta) = det_{\mathbb{Q}_\ell}(1 - F|\mathcal{V}_\ell(E)).$$

Reducción de A_f módulo p, con $p \nmid N$

Si $p \nmid N$ entonces A_f también tiene buena reducción en p porque es cuociente de J_Γ.

Teorema.[1] Sea ψ el nebentypus de f. Tenemos que

$$\#A_f(\mathbb{F}_p) = Nr_{K_f/\mathbb{Q}}(1 - a_p(f) + \psi(p)p)\,.$$

En particular, si $K_f = \mathbb{Q}$ (i.e. A_f curva elíptica) entonces $a_p(f) = a_p(A_f)$.

Dem. Elegir $\ell \neq p$. Veremos el caso $K_f = \mathbb{Q}$, i.e. A_f curva elíptica. Así $\psi = \chi_0$. Del polinomio característico de F en $\mathcal{V}_\ell(J_\Gamma)$ obtenemos:

$$\#A_f(\mathbb{F}_p) = det_{\mathbb{Q}_\ell}(1 - F|\mathcal{V}_\ell(A_f)) = \lambda_f(1 - T_p + p) = 1 - a_p(f) + p.$$

$\square$

[1] Ver Prop. 1.51 en [DDT]. Está mal enunciada.

$L(A_f, s)$

Para una variedad abeliana $A/\mathbb{Q}$ definimos su función L

$$L(A,s) = (*)\prod_p \det(1 - Fp^{-s}|\mathcal{V}_\ell(A))^{-1}, \quad \Re(s) \gg 1$$

donde (*) denota finitos factores de Euler que se definen de acuerdo al tipo de reducción mala de A.
Por ejemplo, si E es curva elíptica de conductor N entonces

$$L(E,s) = \prod_{p|N} \frac{1}{1 - a_p(E)p^{-s}} \prod_{p\nmid N} \frac{1}{1 - a_p(E)p^{-s} + p^{1-2s}}$$

donde si $p|N$ entonces

$$a_p(E) = \begin{cases} 0 & \text{aditiva} \\ 1 & \text{multiplicativa split} \\ -1 & \text{multiplicativa non-split.} \end{cases}$$

$L(A_f, s)$

Teorema. Sea f newform de nivel N. Entonces A_f tiene conductor $N^{\dim A_f} = N^{[K_f:\mathbb{Q}]}$ y su función L cumple

$$L(A_f, s) = \prod_{g\in[f]} L(g, s).$$

En particular, $L(A_f, s)$ tiene ecuación funcional y continuación analítica.

Dem. Igualar los productos de Euler de ambos lados primo por primo.

- $p|N$: Es un cálculo muy delicado y no lo haremos. Este cálculo da el conductor también. (Ver ejemplo en siguiente diapositiva.)
- $p \nmid N$: Viene del resultado $\#A_f(\mathbb{F}_p) = Nr_{K_f/\mathbb{Q}}(1 - a_p(f) + \psi(p)p)$. Por ejemplo, si $K_f = \mathbb{Q}$ entonces A_f es curva elíptica y tenemos

$$\frac{1}{1 - a_p(A_f)p^{-s} + p^{1-2s}} = \frac{1}{1 - a_p(f)p^{-s} + p^{1-2s}}. \quad \square$$

$L(A_f, s)$: ejemplo de factor de Euler en $p|N$

Si $K_f = \mathbb{Q}$ entonces el nebentypus de f es trivial así que $f \in S_2(\Gamma_0(N))$. Asumir $p||N$.

- $X_0(N) \otimes \mathbb{F}_p$ son dos copias de $X_0(N/p) \otimes \mathbb{F}_p$ que se cortan transversalmente en algunos puntos. Así, $X_0(N)$ una curva de reducción *semi-estable* en p.
- Entonces $J_0(N)$ tiene reducción multiplicativa en p.
- A_f tiene reducción multiplicativa en p (es cuociente de $J_0(N)$).
- Así que el conductor $cond(A_f)$ de A_f cumple $p||cond(A_f)$.
- Además $a_p(A_f) = \pm 1$ debido a la reducción multiplicativa.
- Dado que $p||N$, la teoría de los operadores U_p nos da que $a_p(f) = \pm 1$.

Así que $a_p(f) = \pm a_p(A_f)$ en el caso que A_f es curva elíptica y $p||N$. Con un poco más de trabajo se obtiene igualdad.
Además, el mismo razonamiento muestra que si N es libre de cuadrados entonces $cond(A_f) = N$.