Representaciones de Galois asociadas a curvas elípticas

Matías Alvarado

Mayo 2020

Contenido

- Representaciones mod ℓ y ℓ-ádicas asociadas a curvas elípticas
- Propiedades globales
- Propiedades locales
- Curva de Frey

Representaciones mod n

- Sea E una curva elíptica sobre $\mathbb{Q}$, y consideremos $E[n](\overline{\mathbb{Q}})$, los puntos de n-torsión sobre $\overline{\mathbb{Q}}$
- $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ actúa en $E[n](\overline{\mathbb{Q}})$
- Existe un homomorfismo

$$\rho\colon G_{\mathbb{Q}} \to \mathrm{Aut}\left(E[n](\overline{\mathbb{Q}})\right)$$

- Existe isomorfismo $E[n](\overline{\mathbb{Q}}) \simeq (\mathbb{Z}/n\mathbb{Z})^2$
- Eligiendo una base obtenemos el siguiente homomorfismo

$$\overline{\rho}_{E,n}\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

Representaciones ℓ-ádicas

- Dado un primo ℓ, consideremos el módulo de Tate ℓ-ádico $T_\ell E$
- $G_{\mathbb{Q}}$ actúa en $T_\ell E$
- Existe un homomorfismo

$$\rho\colon G_{\mathbb{Q}} \to \mathrm{Aut}(T_\ell E)$$

- $T_\ell E \simeq \mathbb{Z}_\ell^2$, pues $T_\ell E = \varprojlim E[\ell^n](\overline{\mathbb{Q}}) \simeq \varprojlim (\mathbb{Z}/\ell^n\mathbb{Z})^2$
- Eligiendo una base obtenemos el siguiente homomorfismo

$$\rho_{E,\ell}\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_\ell)$$

Notar que $\overline{\rho}_{E,\ell^n} \simeq \rho_{E,\ell} \pmod{\ell^n}$

Observación

Para denotar a la representación ℓ-ádica también se usa la notación ρ_{E,ℓ^∞}

Propiedades globales de $\rho_{E,\ell}$ y $\overline{\rho}_{E,\ell}$

Proposición

El determinante de $\rho_{E,\ell}$ es ϵ_ℓ.

Demostración:

(a) El pairing de Weil $e_\ell : E[\ell] \times E[\ell] \to \mu_\ell$ es no degenerado, alternante y Galois equivariante. Sean $x, y \in E[\ell]$ tal que forman una base, y supongamos que $\sigma(x) = ax + cy, \sigma(y) = bx + dy$. Entonces

$$\begin{aligned} e_\ell(x,y)^{\epsilon_\ell(\sigma)} &= \sigma(e_\ell(x,y)) \\ &= e_\ell(\sigma x, \sigma y) \\ &= e_\ell(ax+cy, bx+dy) \\ &= e_\ell((ad-bc)x, y) \\ &= e_\ell(x,y)^{ad-bc} \end{aligned}$$

Por lo tanto $det(\overline{\rho}_{E,\ell}(\sigma)) = \epsilon_\ell(\sigma) \bmod \ell$

Proposición

(a) $\rho_{E,\ell}$ *es irreducible para todo* ℓ.

(b) $\overline{\rho}_{E,\ell}$ *es irreducible para casi todo* ℓ.

(c) *Si* E *no tiene CM, entonces* $\rho_{E,\ell}$ *es sobreyectiva para casi todo* ℓ.

Lema

Sea $E/\mathbb{Q}$ una curva elíptica. Si $\phi\colon E' \to E$ y $\psi\colon E'' \to E$ son $\mathbb{Q}$-isogenias con núcleos cíclicos no isomorfos, entonces las curvas E' y E'' no son isomorfas sobre $\mathbb{Q}$.

Demostración.

$n = \deg\phi$, $m = \deg\psi$ y supongamos que existe un $\mathbb{Q}$-isomorfismo $\sigma\colon E' \to E''$. Consideremos la isogenia $\psi \circ \sigma \circ \phi^*\colon E \to E$ de grado mn. Esta isogenia tiene que ser multiplicación por un entero N, por lo tanto es de grado N^2. Con esto deducimos que $N^2 = mn$. Por un lado el núcleo de la isogenia debe ser $(\mathbb{Z}/N\mathbb{Z})^2$, y por otro lado debe ser una extensión de $\mathbb{Z}/m\mathbb{Z}$ por $\mathbb{Z}/n\mathbb{Z}$. Con esto se concluye que $m = n = N$. □

Proposición

(a) *$\rho_{E,\ell}$ es irreducible para todo ℓ.*

Demostración: Supongamos que existe $\mathcal{W}$ $G_{\mathbb{Q}}$-submódulo de dimensión 1 de $\mathcal{V}_\ell$ y sea $W = \mathcal{T}_\ell E \cap \mathcal{W}$. Sea W_n la imagen de W vía la proyección $\mathcal{T}_\ell E \twoheadrightarrow E[\ell^n]$. De este modo definimos $E_n = E/W_n$. Así tenemos una familia $\{E_n\}$ de curvas elípticas que son isogenas a E con núcleo cíclico de orden ℓ^n. Por lema anterior en esta familia las curvas son 2-2 no isomorfas. Luego en la clase de isogenias de E hay infinitas clases de isomorfía.

Proposición

(b) *$\overline{\rho}_{E,\ell}$ es irreducible para casi todo ℓ.*

Demostración: Si $E[\ell]$ no es irreducible, entonces existe un subgrupo cíclico W_ℓ de E definido sobre $\mathbb{Q}$. De ese modo tenemos curvas $E_\ell = E/W_\ell$ e isogenias $E \to E_\ell$. Luego si existen infinitos primos primos ℓ para los cuales $E[\ell]$ no es irreducible, encontraremos infinitas curva E_ℓ isogenas a E con núcleo cíclico y tales que E_ℓ y $E_{\ell'}$ no son isomorfas para $\ell \neq \ell'$. Así llegamos a la misma contradicción anterior. Por lo tanto $\overline{\rho}_{E,\ell}$ es irreducible para casi todo ℓ.

Teorema

Sea $E/\mathbb{Q}$ una curva elíptica

(a) *$\overline{\rho}_{E,\ell}$ es irreducible para $\ell > 163$.*

(b) *Si E es semi-estable, entonces $\overline{\rho}_{E,\ell}$ es irreducible para $\ell > 7$.*

(c) *Si E es semiestable y $\overline{\rho}_{E,2}$ es trivial, entonces $\overline{\rho}$ es irreducible para $\ell > 3$.*

Demostración.

Estos resultados son consecuencia de los trabajos de Mazur.

(a) Sale del hecho que $X_0(\ell)$ no tiene punto racionales no-cuspidales para primos $\ell > 163$.

Hecho: Si E es semiestable con tiene un subgrupo racional de orden ℓ, entonces E es isogena a una curva elíptica con un punto racional de orden ℓ.

(b) Hecho + tipo de $\mathbb{Q}$-torsión en curvas elípticas.

(c) Hecho + tipo de $\mathbb{Q}$-torsión en curvas elípticas.

□

Propiedades locales de $\rho_{E,\ell}$ y $\overline{\rho}_{E,\ell}$

Proposición

Supongamos que $E/\mathbb{Q}$ es una curva elíptica con buena reducción en p. Si $\ell \neq p$, entonces $\rho_{E,\ell}$ es no ramificada en p y se tiene la siguiente identidad para la traza

$$tr\rho_{E,\ell}(Frob_p) = p + 1 - \#\widetilde{E}_p(\mathbb{F}_p) = a_p(E)$$

Demostración.

El polinomio característico de $Frob_p$ es $x^2 - a_p(E)x + p$.
$\#\widetilde{E}[p] = \#\ker(Frob_p - 1) = \deg(\mathrm{Frob}_p - 1) = (\mathrm{Frob}_p - 1)_* \circ (\mathrm{Frob}_p - 1)^*$
$\#\widetilde{E}[p] = p + 1 - Frob_{p,*} - Frob_p^*$. Entonces $a_p(E) = Frob_{p,*} + Frob_p^*$.
Tenemos entonces $a_p(E)Frob_{p,*} = Frob_{p_*}^2 + p$ sobre $Pic^0(\widetilde{E})$.Luego sobre E tenemos $Frob_p^2 - a_p(E)Frob_p + p = 0$. Como p es el determinante de $\rho_{E,\ell}$ se concluye. □

Proposición

(a) *Si E tiene buena reducción en p, entonces para $n \geq 1$ existe un esquema de grupo finito y plano $\mathcal{F}_n/\mathbb{Z}_p$ tal que*

$$E[p^n](\overline{\mathbb{Q}}_p) \simeq \mathcal{F}_n(\overline{\mathbb{Q}}_p)$$

(b) *Si E tiene buena reducción ordinaria en p, entonces*

$$\rho_{E,p}|_{I_p} \sim \begin{pmatrix} \epsilon_p & * \\ 0 & 1 \end{pmatrix}$$

(c) *Si E tiene buena reducción supersingular en p, entonces $\overline{\rho}_{E,p}|_{G_p}$ es irreducible*

Reducción multiplicativa en p

Recuerdo: Sea E es una curva elíptica sobre $\mathbb{Q}_p$ con reducción multiplicativa, entonces existe un isomorfismo analítico

$$\Phi\colon \overline{\mathbb{Q}}_p^*/q^{\mathbb{Z}} \to E(\overline{\mathbb{Q}}_p)$$

tal que $\sigma(\Phi(x)) = \Phi(\sigma(x)^{\delta(\sigma)})$. Donde δ es trivial si E tiene reducción split. Por otro lado, si E tiene reducción non-split entonces $\delta\colon G_{\mathbb{Q}_p} \to \{\pm 1\}$ es el caracter cuadrático no ramificado.
De este modelo vemos que la ℓ-torsión es $\{\zeta_\ell^a (q^{1/\ell})^b; 0 \leq a, b \leq \ell - 1\}$. El grupo de raices de la unidad es estable por la acción de $G_{\mathbb{Q}_p}$. Por lo tanto la acción de $G_{\mathbb{Q}_p}$ en $E[\ell]$ viene dada por

$$\rho_{E,\ell}|_{G_p} \sim \begin{pmatrix} \epsilon_\ell & * \\ 0 & 1 \end{pmatrix} \otimes \delta$$

Del mismo modo

$$\overline{\rho}_{E,\ell}|_{G_p} \sim \begin{pmatrix} \epsilon_\ell & * \\ 0 & 1 \end{pmatrix} \otimes \delta$$

¿Podemos decir algo mas de *?
Supongamos que

$$\overline{\rho}_{E,\ell}|_{G_p} \sim \begin{pmatrix} \epsilon_\ell & \Psi \\ 0 & 1 \end{pmatrix}$$

Si $\sigma_1, \sigma_2 \in G_p$, entonces

$$\begin{pmatrix} \epsilon_\ell(\sigma_1\sigma_2) & \Psi(\sigma_1\sigma_2) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \epsilon_\ell(\sigma_1) & \Psi(\sigma_1) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \epsilon_\ell(\sigma_2) & \Psi(\sigma_2) \\ 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} \star & \epsilon_\ell(\sigma_1)\Psi(\sigma_2) + \Psi(\sigma_1) \\ 0 & 1 \end{pmatrix}$$

Asi Ψ es un homomorfismo cruzado, por lo tanto es un elemento en

$$H^1(G_{\mathbb{Q}_p}, \mathbb{Z}/\ell\mathbb{Z}(1)) \simeq \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^\ell$$

Mas aún, $[\Psi]$ corresponde (vía el isomorfismo) a la clase de q mod $(\mathbb{Q}_p^*)^\ell$

Proposición

Sea E una curva elíptica con reducción multiplicativa en p.

(a) *Si $\ell \neq p$,entonces $\overline{\rho}_{E,\ell}$ es no ramificada en p si y solo si $\ell | v_p(\Delta_E^{min}) = -v_p(j_E) = v_p(q)$*

(b) *Existe un esquema en grupo finito y plano $\mathcal{F}/\mathbb{Z}_p$ tal que $E[p](\overline{\mathbb{Q}}_p) \simeq \mathcal{F}(\overline{\mathbb{Q}}_p)$ si y solo si $p | v_p(\Delta_E^{min})$*

Demostración.

(a) Sea $K/\mathbb{Q}_p$ una extensión no ramificada donde E tiene reducción split. Entonces

$$K_\ell := K(E[\ell]) = K(\zeta_\ell, q^{1/\ell})$$

K_ℓ/K es no ramificada si y solo si $\ell \neq p$ y $\ell | v_p(q)$

Curva de Frey

Conjetura

Sea $\ell > 2$ un número primo, entonces la ecuación

$$x^\ell + y^\ell = z^\ell, \quad xyz \neq 0$$

no tiene soluciones enteras.

Supongamos que existen enteros a, b y c tal que $a^\ell + b^\ell = c^\ell$ con $abc \neq 0$. Frey estudió una curva elíptica construida a partir de esta supuesta solución

$$E : y^2 = x(x - a^\ell)(x + b^\ell)$$

- E es una curva elíptica semi-estable
- $\Delta_E^{\min} = \dfrac{(abc)^{2\ell}}{2^8}$

Propiedades de la curva de Frey

Supongamos que $\ell > 3$ un número primo.

- $\overline{\rho}_{E,\ell}$ es irreducible.
- $\overline{\rho}_{E,\ell}$ es no ramificada fuera de 2 y ℓ.
  - Si E tiene buena reducción en p, entonces $\overline{\rho}_{E,\ell}$ no ramifica en p.
  - Si E red. multiplicativa, entonces $\overline{\rho}_{E,\ell}$ no ramifica en p, pues $\ell | v_p(\Delta_E^{\min})$
- Existe un esquema de grupo $\mathcal{F}/\mathbb{Z}_\ell$ tal que $\mathcal{F}(\overline{\mathbb{Q}}_\ell) \simeq E[\ell](\overline{\mathbb{Q}}_\ell)$ como G_ℓ-módulos.
- $\overline{\rho}_{E,\ell}(I_2)$ es no trivial

Conjetura Taniyama-Shimura y último teorema de Fermat

Corolario

Si la conjetura Taniyama-Shimura (al menos para curvas semi-estables) es cierta, entonces la ecuación $x^\ell + y^\ell = z^\ell$ no tiene soluciones no triviales.