Sistemas compatibles día 1

Héctor Pastén

Pontificia Universidad Católica de Chile

Escuela CIMPA 2025

PARTE I: Representaciones ℓ-adicas

Definición de una representación ℓ-ádica

Sea ℓ un primo y sea V un $\mathbb{Q}_\ell$-espacio vectorial de dimensión n. Para un grupo topológico G, una representación ℓ-ádica (en V) es un morfismo continuo de grupos

$$\rho : G \to \mathrm{GL}(V)$$

donde $\mathrm{GL}(V)$ tiene la topología dada por el isomorfismo

$$\mathrm{GL}(V) \simeq \mathrm{GL}_n(\mathbb{Q}_\ell).$$

Caso relevante: L/K extensión Galois (no necesariamente finita) y $G = \mathrm{Gal}(L/K)$ con la topología profinita. Estas son **representaciones de Galois ℓ-ádicas**.

Ejemplo 1: Raíces de 1 (caracter ciclotómico)

Sea K campo de característica $p \geq 0$ y sea $\ell \neq p$. Anotamos

$$G = \mathrm{Gal}(K_s/K).$$

Tomar $r \geq 1$ entero. Para cada $\sigma \in G$ hay un $m_r(\sigma) \in (\mathbb{Z}/\ell^r\mathbb{Z})^\times$ tal que σ actúa en μ_{ℓ^r} por

$$z \mapsto \sigma(z) = z^{m_r(\sigma)}.$$

La función $\mu_{\ell^{r+1}} \to \mu_{\ell^r}$ dada por $z \mapsto z^\ell$, es compatible con los $m_r(-)$. Obtenemos que $\sigma \in G$ actúa en el **módulo de Tate ℓ-ádico** del grupo multiplicativo

$$T_\ell \mathbb{G}_m := \varprojlim \mathbb{G}_m[\ell^r] = \varprojlim \mu_{\ell^r}$$

por $\chi(\sigma) := (m_1(\sigma), m_2(\sigma), \ldots) \in \varprojlim (\mathbb{Z}/\ell^r\mathbb{Z})^\times = \mathbb{Z}_\ell^\times$.

Ejemplo 1: Raíces de 1 (caracter ciclotómico)

Esto se puede ver de otro modo:
$T_\ell \mathbb{G}_m = \lim_{\leftarrow} \mu_{\ell^r}$ es un grupo multiplicativo, pero una elección compatible de raíces primitivas da un isomorfismo con el grupo aditivo

$$T_\ell \mathbb{G}_m = \lim_{\leftarrow} \mu_{\ell^r} \simeq \lim_{\leftarrow} \mathbb{Z}/\ell^r\mathbb{Z} = \mathbb{Z}_\ell$$

donde ahora σ actúa por multiplicación escalar por $\chi(\sigma) \in \mathbb{Z}_\ell^\times$.
La versión con denominadores es

$$V = V_\ell \mathbb{G}_m := (T_\ell \mathbb{G}_m) \otimes \mathbb{Q}_\ell \simeq \mathbb{Q}_\ell$$

que es un espacio vectorial de dimensión 1. Ahora los $\chi(\sigma) \in \mathbb{Z}_\ell^\times$ dan un morfismo continuo

$$\chi : G \to \mathrm{GL}(V) = \mathrm{GL}_1(\mathbb{Q}_\ell) = \mathbb{Q}_\ell^\times.$$

Ejemplo 2: Curvas elípticas

Sea K un campo de característica $p \geq 0$ y sea $\ell \neq p$. Sea E curva elíptica sobre K. Repetimos lo anterior usando E en lugar de $\mathbb{G}_m$: ahora eligiendo base tenemos

$$E[\ell^r] \simeq (\mathbb{Z}/\ell^r\mathbb{Z})^2.$$

De este modo el módulo de Tate ℓ-ádico de E es

$$T_\ell E = \varprojlim E[\ell^r] \simeq \mathbb{Z}_\ell^2.$$

Anotando $V = (T_\ell E) \otimes \mathbb{Q}_\ell$ obtenemos un morfismo continuo

$$\rho : G = \mathrm{Gal}(K_s/K) \to \mathrm{GL}(V) \simeq \mathrm{GL}_2(\mathbb{Q}_\ell).$$

Ejemplo 3: Cohomología ℓ-ádica

Esto no será usado, pero vale la pena mencionarlo:

Si X/K es variedad suave proyectiva, para cada $i \geq 0$ hay un $\mathbb{Q}_\ell$ espacio vectorial

$$H^i_{et}(\overline{X}, \mathbb{Q}_\ell)$$

donde $\overline{X} = X \otimes K_s$. Viene con una acción de $G = \mathrm{Gal}(K_s/K)$. Esto da muchas representaciones de Galois ℓ-ádicas.

Ramificación de una representación

Sea K campo de números y $\mathfrak{p}$ un primo de K_s. Anotamos $G = \mathrm{Gal}(K_s/K)$. Entonces hay un grupo de descomposición

$$D_{\mathfrak{p}} = \{\sigma \in G : \sigma(\mathfrak{p}) = \mathfrak{p}\}$$

y su subgrupo de inercia

$$I_{\mathfrak{p}} = \{\sigma \in D_{\mathfrak{p}} : \forall x \in O_{K_s}, \quad \sigma(x) \equiv x \bmod \mathfrak{p}\}.$$

Una representacion ℓ-ádica $\rho : G \to \mathrm{GL}(V)$ es **ramificada** en $\mathfrak{p}$ si $\rho(I_{\mathfrak{p}}) \neq \{\mathrm{Id}\}$

Elementos de Frobenius

Dado que $D_{\mathfrak{p}}/I_{\mathfrak{p}} \simeq \mathrm{Gal}(\mathbb{F}_v^{\mathrm{alg}}/\mathbb{F}_v)$ para $\mathbb{F}_v = O_K/\mathfrak{p}$, hay un generador topológico de este grupo dado por el **Frobenius** $F_{\mathfrak{p}} \in D_{\mathfrak{p}}/I_{\mathfrak{p}}$. Hechos importantes:

- $F_{\mathfrak{p}}$ se puede ver en G módulo inercia.
- Si $\rho : G \to \mathrm{GL}(V)$ no ramifica en $\mathfrak{p}$ entonces $\rho(F_{\mathfrak{p}})$ es bien definido.
- Dado v primo de K, todos los $F_{\mathfrak{p}}$ son conjugados, para primos $\mathfrak{p}|v$. En particular, si no hay ramificación sobre v, entonces podemos hablar de $\rho(F_v) \in \mathrm{GL}(V)$ salvo conjugación. Su polinomio característico es bien definido.
- **Teorema de densidad de Chebotarev**: Si $\rho : G \to \mathrm{GL}(V)$ es no ramificada fuera de un conjunto finito de primos de K, entonces los $\rho(F_v)$ con $v \notin S$ primos de K forman un denso de $\rho(G) \subseteq \mathrm{GL}(V)$.

Representaciones racionales

Seguimos con K campo de números. Una representación ℓ-ádica

$$\rho : G \to \mathrm{GL}(V)$$

se dice **racional** si es no-ramificada fuera de un conjunto finito S de primos de K, y para todos salvo finitos $v \notin S$ primos de K se tiene que

$$\det(1 - \rho(F_v)\, T) \in \mathbb{Q}[T]$$

donde T es una variable.
Esta condición es bien definida porque el polinomio característico es invariante por conjugación.

Ejemplo: Raíces de 1

Recordemos $\chi_\ell = \chi : G \to \mathbb{Q}_\ell^\times$. Uno chequea que

$$\chi_\ell(F_v) = \mathrm{Norm}(v) \in \mathbb{Q}$$

para cualquier v que no divide a ℓ (ver cómo actúa el Frobenius en raíces de 1). En particular es no ramificada fuera de los primos sobre ℓ y se tiene

$$\det(1 - \chi_\ell(F_v)\,T) = 1 - (\mathrm{Norm}(v))\,T \in \mathbb{Q}[T].$$

así que χ_ℓ es racional.
Observación: De hecho, el polinomio característico es independiente de ℓ.

Ejemplo: Curvas elípticas

Sea $\rho_\ell : G \to \mathrm{GL}_2(\mathbb{Q}_\ell)$ la representación ℓ-ádica asociada a una curva elíptica E/K.
Si E tiene buena reducción módulo v entonces se puede contar puntos y uno chequea

$$\#E(\mathbb{F}_v) = \mathrm{Norm}(v) + 1 - Tr(\rho_\ell(F_v)).$$

(Idea: puntos fijos del Frobenius en $E(\mathbb{F}_v^{\mathrm{alg}})$ son los $\mathbb{F}_v$-racionales.)
Así, ρ_ℓ es no ramificada fuera de los primos malos de E y se cumple que el polinomio característico de $\rho_\ell(F_v)$ es

$$1 - a_v(E)T + \mathrm{Norm}(v)T^2 \in \mathbb{Q}[T]$$

donde $a_v(E) = \mathrm{Norm}(v) + 1 - \#E(\mathbb{F}_v)$.
Observación: El polinomio característico es independiente de ℓ.

Sistemas compatibles

Un sistema compatible de representaciones ℓ-adicas $\rho_\ell : G \to \mathrm{GL}(V_\ell)$ (con el primo ℓ variando) es una colección de dichas representaciones (una para cada ℓ) tales que

- son racionales (en particular, no ramificadas salvo finitos primos), y
- dados cualquier ℓ, ℓ', todos salvo finitos v cumplen que

$$\rho_\ell(F_v) \quad y \quad \rho_{\ell'}(F_v)$$

tienen el mismo polinomio característico.

Es estrictamente compatible si además las excepciones de v son un conjunto finito fijo (salvo el ℓ y ℓ' tomados, obviamente). En particular, son no ramificadas fuera de un conjunto finito de primos fijo.

Ejemplos: Las que vienen de raíces de 1 y de curvas elípticas.

PARTE II: Los grupos T y S.

Restricción de escalares

Sea K/k una extensión finita. Si X es una variedad afín o proyectiva sobre K, entonces hay una variedad $Y = R_{K/k}X$ sobre k definida por la propiedad siguiente:
Dada cualquier k-álgebra A, se tiene una biyección funtorial

$$Y(A) = X(A \otimes K).$$

(En realidad se define lo anterior como un funtor, y en el caso afín y proyectivo se demuestra que es representable.)
Y se llama la **restricción de escalares** de X.

Toros: Grupos T

Si X es un grupo algebraico, entonces $Y = R_{K/k}X$ también.

Un caso importante pero sencillo es el de los toros:

$$T := R_{K/k}\mathbb{G}_m$$

Es un grupo algebraico sobre k de dimensión $n = [K : k]$.
NOTA: $\mathbb{G}_m = Spec\, \mathbb{Q}[x, y]/(xy - 1)$

Ejemplo: $\mathbb{Q}(i)/\mathbb{Q}$

Consideramos $k = \mathbb{Q}$ y $K = \mathbb{Q}(i)$ de modo que $n = 2$. Entonces

$$T = R_{\mathbb{Q}(i)/\mathbb{Q}}\mathbb{G}_m$$

cumple que

$$\begin{aligned} T(\mathbb{Q}) &= \{(a, b) \in \mathbb{Q}^2 : a^2 + b^2 \neq 0\} \\ &= \mathbb{Q}^2 - \{(0, 0)\} \end{aligned}$$

con la operación

$$(s, t) * (a, b) = (sa - tb, sb + ta).$$

Ideles

Sea K campo de números y

$$\mathbb{A}_K = \prod_v{}' (K_v, O_v)$$

su anillo de **adeles**. El grupo de **ideles** es $\mathbb{I}_K = \mathbb{A}_K^\times$. Tenemos la incrustación diagonal $K^\times \to \mathbb{I}_K^\times$ dada por $x \mapsto (x)_v$ y con ella el **grupo de clases de ideles**

$$C_K := \mathbb{I}_K / K^\times.$$

Esto es mucho más grande que el $Cl(K)$. De hecho

Teorema (Morfismo de Artin, teoría de campos de clases)

El morfismo de Artin

$$\theta : C_K \to \mathrm{Gal}(K^{ab}/K)$$

es sobreyectivo con kernel la componente de la identidad de C_K.

Módulos y subgrupos de $\mathbb{I}_K$

Un **módulo** m es una función $m : \Sigma_K \to \mathbb{Z}_{\geq 0}$ de soporte finito que se anula en los lugares complejos y puede ser 0 o 1 en los reales. Asociado a un módulo hay un subgrupo abierto

$$U_m \leq I_K$$

que en su coordenada v (no-arquimediana) es

$$U_{v,m} = 1 + \mathfrak{p}_v^{m(v)}.$$

Si v es complejo entonces $U_{v,m} = \mathbb{C}^\times$. Si v es real entonces

$$U_{v,m} = \begin{cases} \mathbb{R}^\times & \text{si } m(v) = 0 \\ \mathbb{R}_{>0} & \text{si } m(v) = 1. \end{cases}$$

Grupos de clases de rayos

El **grupo de clases de rayos** asociado a un módulo m es

$$C_m := C_K / U_m$$

(abuso de notación: debería ser $\overline{U_m}$.) Es finito. Aquí sí aparece $Cl(K)$ como caso especial, con el módulo $m \equiv 0$.

Los grupos T_m

Recordemos la incrustación diagonal $K^\times \to \mathbb{I}_K$. Entonces tiene sentido la intersección $O_K^\times \cap U_m$ que ahora es un subgrupo de $K^\times$.

Fijamos un módulo m. Notar que $T = R_{K/\mathbb{Q}}\mathbb{G}_m$ cumple $T(\mathbb{Q}) = \mathbb{G}_m(K) = K^\times$. Entonces $O_K^\times \cap U_m$ es un subgrupo de $T(\mathbb{Q}) = K^\times$ y su clausura de Zariski será $Z_m \leq T$.

Para el módulo m definimos $T_m = T/Z_m$ que es otro grupo algebraico sobre $\mathbb{Q}$. Notar que viene con un morfismo

$$K^\times/(O_K^\times \cap U_m) \to T_m(\mathbb{Q}).$$

Grupos S_m

Todo lo anterior nos da una secuencia exacta

$$1 \to K^\times / O_K^\times \cap U_m \to \mathbb{I}_K / U_m \to C_m \to 1. \tag{1}$$

Tenemos el morfismo $K^\times / (O_K^\times \cap U_m) \to T_m(\mathbb{Q})$.

Teorema

Existe un grupo algebraico S_m sobre $\mathbb{Q}$ que es una extensión de C_m por T_m, o sea tenemos la secuencia exacta

$$1 \to T_m \to S_m \to C_m \to 1.$$

Además, nivel de $\mathbb{Q}$-puntos se tiene un morfismo

$$\mathbb{I}_K / U_m \to S_m(\mathbb{Q})$$

que da compatibilidad de la secuencia anterior con (1).

¿Para qué queremos los grupos S_m?

Los S_m darán origen a sistemas compatibles de representaciones ℓ-ádicas de $\mathrm{Gal}(K^{ab}/K)$ bastante sencillos en estructura. Demasiado sencillos.

El punto es que que las curvas elípticas sin CM no pueden tener sistemas compatibles tan sencillos. Esto da una herramienta para estudiar la imagen de dichas representaciones de Galois siempre que la imagen no sea abeliana.

Fin día 1.

Día 2: representaciones de los S_m.
Día 3: representaciones localmente algebraicas.