12. PREDAVANJE

GAL. REP. EL. KRIV. > CM (KOMPLEKSNO MNOŽENJE)

E/K, K PAB $\quad \mathrm{End}_{\bar{K}} E \supseteq \mathbb{Z}$

$\cup$ $\{f \in E \to E$ izogenija $\wedge$ def nad $K\}$

Ako je $\mathrm{End}\, E \neq \mathbb{Z}$ kažemo da E ima CM.

Toda $\mathrm{End}\, E_{\bar{K}} = \mathcal{O}$ gdje je $\mathcal{O} \subseteq \mathcal{O}_K$ za neko imaginarno kvadratno polje i $[\mathcal{O}_K : \mathcal{O}] < \infty$

Npr $E: y^2 = x^3 + x \qquad [i]: (x,y) \to (-x, iy)$

$\notin \mathbb{Z}$

$\mathrm{End}\, E = \mathbb{Z}[i]$

Endomorfizmi iz $\mathrm{End}\, E$ koji nisu iz $\mathbb{Z}$ su definirani nad K gdje je $\mathrm{End}\, E \subseteq K$ i K je kvadratno imaginarno polje.

Def Neka je $\mathfrak{p}$ max ideal u konačnom proširenju K od $\mathbb{Q}_p$.

Funkcija koja $x \in \mathcal{O}_K$ pridružuje max n t.d. je $x \in \mathfrak{p}^n$ zove se normalizirana $\mathfrak{p}$-adska valuacija na K. Proširenje je na cijeli K: $v_{\mathfrak{p}}\left(\frac{x}{y}\right) = v_{\mathfrak{p}}(x) - v_{\mathfrak{p}}(y)$.

Vrijedi $\quad v_{\mathfrak{p}}(x) = e(\mathfrak{p}/p) \cdot v_p(x). \quad \forall x \in \mathbb{Z}$.

Sjetimo se da za $K/\mathbb{Q}_p$ kon. proširenje i E/K

$v_{\mathfrak{p}}(j(E)) < \infty \iff E$ ima pot. multiplikativnu redukciju u $\mathfrak{p}$

$\iff E$ je kvadratni twist od Tatateove krivulje E_q za neki q.

Jakoster $E_q(\overline{K}) \simeq \overline{K}^*/q^{\mathbb{Z}}$

<u>Propozicija</u> (AG x86 ili Silverman ATAEC)

Neka je K kon. proširenje od $\mathbb{Q}_p$ s max idealom p. E/K el. krivulja $v_p(j(E)) < 0$, te neka je $\ell \geq 3$ prost broj koji ne dijeli $v_p(j(E))$.

Tada $\exists\ \sigma \in$ ~~Gal($\overline{K}/K$)~~ $I(\overline{K}/K)$ koji djeluje na $E[\ell]$ kao matricu $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ u nekoj bazi $\{P_1, P_2\}$ od $E[\ell]$

<u>Dokaz</u>: Primijetimo $\left|\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right| = \ell$. Neka je K' ~~polje~~ proširenje od K t.d. je $E \underset{K'}{\simeq} E_q$. (~~dovoljno~~ $[K':K] = 1$ ili 2).

Primijetimo da je $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \rho_\ell(G_{K'}) \Leftarrow\Rightarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \rho_\ell(G_K)$

Radimo u K', ~~označimo~~ BSO pretpostavimo $E \underset{K}{\simeq} E_q$.

Dalje, možemo dodati ~~K~~ ζ_ℓ u K pa dobijemo proširenje stupnja koji dijeli $\ell - 1$.

$(\ell, \ell-1) = 1 \implies$ istim argumentom možemo pretp. $\zeta_\ell \in K$.

Neka je $Q = q^{\frac{1}{\ell}} \in \overline{K}$ (gdje je $E \simeq \underline{\underline{E_q}}$)

faktor ℓ-ti korijen iz q.

~~K~~$K(Q)/K$ je potpuno razgranato Galoisovo proširenje (KUMMEROVA TEORIJA)

$\implies$ ~~...~~ $\exists\ \sigma \in Gal(K(Q)/K)$ t.d. $Q^\sigma = \zeta_\ell Q$ $(x^\ell - q)$

Sjetimo se da je $E_q(\overline{K}) \simeq \overline{K}^\times / q^{\mathbb{Z}}$.

Neka je $\phi : E_q(\overline{K}) \to \overline{K}^\times / q^{\mathbb{Z}}$ taj izomorfizam.

G_K komutira s ~~djelom~~ ϕ (pošto je ϕ def nad K).

Q i ζ_ℓ generiraju $\left(\overline{K}^\times / q^{\mathbb{Z}}\right)[\ell]$

$\Rightarrow P_1 := \phi^{-1}(\zeta_\ell)$ i $P_2 := \phi^{-1}(Q)$ bazu za $E_q[\ell]$

Imamo

$$P_1^\sigma = \phi^{-1}(\zeta_\ell^\sigma) \overset{\zeta_\ell \in K}{=} \phi^{-1}(\zeta_\ell) = P_1$$

$$P_2^\sigma = \phi^{-1}(Q^\sigma) = \phi^{-1}(\zeta_\ell Q) = \phi^{-1}(\zeta_\ell) + \phi^{-1}(Q)$$

$$= P_1 + P_2$$

$\Rightarrow \rho_{E,\ell}(\sigma) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ■

Ovaj $\sigma \in \mathrm{Gal}(K(Q)/K)$ ← $K(Q)/K$ je potpuno razgranato

$\Rightarrow \sigma$ iz inercijske podgrupe. ■

Korolar. Neka je $K/\mathbb{Q}$ PAB, E/K eliptička krivulja i pretpostavimo da $j(E) \notin O_K$. Tada za sve osim konačno mnogo prostih brojeva ℓ

$\rho_{E,\ell}(G_K)$ sadrži $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ~~za~~ u nekoj bazi od $E[\ell]$.

Dokaz. Neka je $\mathfrak{p}$ max ideal u K t.d. $v_{\mathfrak{p}}(j(E)) < 0$.

Imamo pa je $Gal(\overline{K_{\mathfrak{p}}}/K_{\mathfrak{p}}) \leq Gal(\overline{K}/K)$.

Po prethodnoj propoziciji $\exists \sigma \in Gal(\overline{K_{\mathfrak{p}}}/K_{\mathfrak{p}})$

koji djeluje kao $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ na $E[\ell]$.

Dakle $E[\ell] \subseteq \overline{K} \subseteq \overline{K_{\mathfrak{p}}}$ ∎.

Teorem Neka je $K/\mathbb{Q}$ PAB, E/K eliptička krivulja

tako da je $j(E) \notin O_K$. Tada je $\mathrm{End}\, E = \mathbb{Z}$.

Dokaz: Neka je ℓ prost broj. Neka je $\psi \in \mathrm{End}\, E \subseteq O_K$

Želimo $\psi \in \mathbb{Z}$.

Općenito (Silverman)

$$\deg \psi \equiv \det \rho_{E,\ell}(\psi) \mod \ell$$

$\psi \in \mathrm{End}\, E$, ponaša se na $E[\ell]$

$n \in \mathbb{Z}$

$$\begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix} \equiv n^2 \mod \ell$$

Radimo nad proširenjem od K, ako treba, takvim da sadrži $\mathrm{End}\, E$. Neka je $\sigma \in Gal(\overline{K}/K)$ t.d.

$$\rho_{E,\ell}(\sigma) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

– po korolaru $\exists$ takav σ za sve osim konačno mnogo ℓ-ova.

Neka je $\rho_{E,\ell}(\sigma) = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, za neke $a, b, c, d \in \mathbb{Z}/\ell\mathbb{Z}$.

Pošto djelovanje od φ i σ komutiraju (jer je $\varphi \in K$) vrijedi

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix}$$

$$\Rightarrow c = 0 \text{ i } a = d.$$

$$\Rightarrow \rho_{E,\ell}(\psi) = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$$

Neka je $m := \deg(1+\psi) - \deg(\psi) - 1$.

Primijetimo kada bi $\psi \in \mathbb{Z}$, tada bi bilo $m = (1+\psi)^2 - \psi^2 - 1 = 2\psi$.

m

$$m = \deg(1+\psi) - \deg\psi - 1 \equiv \det(\rho_{E,\ell}(1+\psi)) - \det(\rho_{E,\ell}(\psi)) - 1$$

$$\equiv \det \begin{pmatrix} 1+a & b \\ 0 & 1+a \end{pmatrix} - \det \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} - 1 \equiv 2a \mod \ell.$$

Vrijedi za ∞ prostih ℓ-ova $\Rightarrow$ $m = 2a$

Imamo da je $\deg(m-2\psi) \equiv \det \rho_{E,\ell}(m-2\psi)$

$$\equiv \det\left[\begin{pmatrix} m & 0 \\ 0 & m\end{pmatrix} - 2\begin{pmatrix} a & b \\ 0 & a\end{pmatrix}\right] \equiv m^2-4a^2 \pmod{\ell}$$

Pošto je $m = 2a$

$\Rightarrow m^2 - 4a^2 \equiv 0 \Rightarrow \deg(m-2\psi) \equiv 0 \pmod{\ell}$

za ∞ ℓ-ova.

$\Rightarrow \deg(m-2\psi) = 0 \Rightarrow \underset{\in\mathbb{Z}}{m} = \underset{\in}{2\psi}$

$\psi \in O_K$, $\frac{m}{2} \in \mathbb{Q} \Rightarrow \psi \in \mathbb{Q}$.

$\Rightarrow \psi \in O_K \cap \mathbb{Q} \Rightarrow \psi \in \mathbb{Z}$.

■

<u>Korolar</u> Za el. krivulje s kompleksnim množenjem E/K, gdje je K PAB, $\rho_{E,\ell}(O_K)$ će biti sadržan u $\underset{2(\ell-1)^2}{C_s^+(\ell)}$ i $\underset{2(\ell^2-1)}{C_{ns}^+(\ell)}$ za sve osim konačno ℓ-ova.

<u>Dokaz</u>: Pa dokazano za sve osim konačno ℓ-ova

$\begin{pmatrix} 1 & 1 \\ 0 & 1\end{pmatrix}$ nije sadržan u $\rho_{E,\ell}(O)$

$\Rightarrow$ nije surjektivno. $\boxed{\begin{pmatrix} 1 & 1 \\ 0 & 1\end{pmatrix}}$

Ako $\begin{pmatrix} 1 & 1 \\ 0 & 1\end{pmatrix}$ nije u $\rho_{E,\ell}(O)$ onda je u $B_0(\ell)$

Tada je i u $C_s^+(\ell) \cap B_0(\ell)$.

Zielsetzung: Ab $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \notin \rho_{E,\ell}(G_K)$

$\Rightarrow \rho_{E,\ell}(G_K) \subseteq C_{ns}^+(\ell)$ oder

$G_{ns}^+(\ell)$

für $\ell > 13$.