8. PREDAVANJA

MOD P REPREZENTACIJE p-IZOGENIH KRIVULJA

"IMAGES OF MOD P REPRESENTATIONS ASSOCIATED TO ELLIPTIC CURVES"
REVERTER, VILA, 2001 CANAD. MATH. BULL.

Lema Neka je K polje ~~ch~~, char $K = 0$, E_1, E_2 eliptičke krivulje nad K, i $\phi : E_1 \to E_2$ K-izogenija (ϕ def nad K) stupnja p.
Tada je ekvivalentno:

(i) $\exists$ jednodimenzionalni G_K-stabilan potprostor od $E_1[p]$ kojeg ne poništava ϕ.

(ii) $\rho_{E_1,p}(G_K)$ je ~~izo~~ ~~izomorfna~~ konjugirana ~~dijagonalnoj~~ grupi koja je sadržana u dijagonali.

(iii) $\exists$ E_3/K, $E_3 \not\cong E_2$ i K-izogenija ~~ϕ'~~ $\phi' : E_1 \to E_3$ stupnja p.

Dokaz: Neka je $\ker \phi = \langle P \rangle$, $|P| = p$.

(i) $\Rightarrow$ (ii) Neka je $C \leq E_1[p] \Rightarrow C = \langle Q \rangle$

Vidimo da je $\phi(P) = 0$ i $\phi(\alpha P) = 0$ $\forall \alpha$, a $\phi(Q) \neq 0$. $\Rightarrow P, Q$ lin nez $\Rightarrow \{P, Q\}$ baza

$$\Rightarrow \rho_{E,p}(G_K) \subseteq \left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \right\}$$

(ii) $\Rightarrow$ (iii) Postoji bijekcija $\{$podgrupe od $E\} \leftrightarrow \{$izogenije $\to E\}$

$\exists$ 2 izogenije nad $K \Rightarrow \exists \phi' : E_1 \to E_3$ nad K

(iii) $\Rightarrow$ (i) tvrdnja $C = \ker \phi'$

Slučaj $K = \mathbb{Q}$

PROPOZICIJA Neka je E/K el. kr. s torzijskom redu p nad K. Tada je

$$\rho_{E,p}(G_K) = \begin{cases} \left\{ \begin{pmatrix} 1 & * \\ 0 & \chi_p(G_K) \end{pmatrix} \right\} & \text{ako } E \text{ ima 1 izogeniju} \\ \left\{ \begin{pmatrix} 1 & 0 \\ 0 & \chi_p(G_K) \end{pmatrix} \right\} & \text{ako ima } > 1 \text{ -u-} \end{cases}$$

Dokaz: iz Lema.

PROPOZICIJA Neka su E_1/K, E_2/K e.k. i neka je $\phi: E_1 \to E_2$ K-izogenija stupnja p. Pretpostavimo da je

(i) $\chi_p(G_K) \neq \{1\}$ $\left(\Leftrightarrow \zeta_p \notin K\right)$

(ii) $E_1(K)$ i $E_2(K)$ imaju točke reda p,

(iii) $\rho_{E_1,p}(G_K)$ je konjugirana s $\left\{ \begin{pmatrix} 1 & * \\ 0 & \chi_p(G_K) \end{pmatrix} \right\}$.

Tada je $\rho_{E_2,p}(G_K)$ konjugirana $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & \chi_p(G_K) \end{pmatrix} \right\}$.

Dokaz: T: $\phi(E_1[p])$ je G_K-invarijantna.

Neka je $\{P, Q\}$ baza od $E_1[p]$ i neka je $\langle P \rangle = \ker \phi$.

$\forall \sigma \in G_K$ $\quad \phi(P)^\sigma = \phi(P^\sigma) = \phi(\lambda P) = \lambda \phi(P) = 0$.

ϕ def/K.

$\phi(Q)^\sigma = \phi(Q^\sigma) = \phi(\alpha Q + \beta P) = \alpha \phi(Q) + \beta \phi(P)$

$= \alpha \phi(Q) \Rightarrow \phi(E_1[p]) = \langle \phi(Q) \rangle$ je G_K-inv.

$\boxed{\phi(Q)^\sigma = \beta\,\phi(Q)}$ $\quad Q^\sigma = \delta P + \beta Q$

$\rho_{E_1,P}(\sigma) = \begin{pmatrix} \alpha & \delta \\ 0 & \beta \end{pmatrix}$ $\Big\}^{(\alpha=1)}$ $\boxed{\beta = \chi_\rho(\sigma)}$

PRETP $\Rightarrow$ $\rho_{E_1,P}(\sigma_K) = \left\{ \begin{pmatrix} 1 & * \\ 0 & \chi_\rho(\sigma_K) \end{pmatrix} \right\}$

σ_K djeluje na $\langle \phi(Q) \rangle$ kao $\chi_\rho(\sigma_K) \neq \{1\}$

$E_2(K)$ ima točku R reda $p \Rightarrow R$ i $\phi(Q)$ lin. nez.

i djeluje reprezentacija σ_K - cikličke permutacije $\Rightarrow$

$\rho_{E_2,P}(\sigma_K) \in \left\{ \begin{pmatrix} 1 & 0 \\ 0 & \chi_\rho(\sigma_K) \end{pmatrix} \right\}$

Lema Neka su $E_1, E_2 / \mathbb{Q}K$ i neka je $\phi : E_1 \to E_2$ n-izogenija ($=$ izogenija čija je $\ker \phi \cong \mathbb{Z}/n\mathbb{Z}$) čije jezgre su $\langle P_1 \rangle$ i neka je $\hat{\phi} : E_2 \to E_1$ dualna izogenija.

Neka je $\{P_1, Q_1\} = E_1[n]$, neka je $P_2 = \phi(Q_1)$ i pretpostavimo kao da $\{P_2, Q_2\}$ za $E_2[n]$.

Neka je $\rho_{E_1,n}(\sigma) = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ ($\cdot$ obzirom na $\{P_1, Q_1\}$

Tada $\exists\, \beta \in \mathbb{Z}/n\mathbb{Z}$ t.d.

$\rho_{E_2,n}(\sigma) = \begin{pmatrix} d & \beta \\ 0 & a \end{pmatrix}$ ($-\!\!-\!\!-$ $\{P_2, Q_2\}$.

Dokaz: Nekaj je $\sigma \in G_K$.

Tedaj je $P_1^\sigma = a P_1$

$Q_1^\sigma = b P_1 + d Q_1$.

$$P_2^\sigma = \phi(Q_1)^\sigma = \phi(Q_1^\sigma) = \phi(bP_1 + dQ_1)$$

ϕ/K

$$= b\,\phi(P_1) + d\,\phi(Q_1) = dP_2$$

($\phi(P_1) = O$)

Primerjamo: $\det \rho_{E_1,p}(\sigma) = \chi_p(\sigma) = \det \rho_{E_2,p}(\sigma)$

$a \cdot d$ $\qquad$ $a \cdot d$

$$\Rightarrow \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \qquad \begin{pmatrix} d & \beta \\ 0 & a \end{pmatrix}$$

$$\Rightarrow \rho_{E_2,p}(\sigma) = \begin{pmatrix} d & \beta \\ 0 & d \end{pmatrix}. \qquad \blacksquare$$

Korolar Naj bo $E_1, E_2/K$, $\phi: E_1 \to E_2$ p-izog. nad K.

Naj je $E_2(K)[p] = \{O\}$. Tedaj $E_1(K)$ vsebuje

natko $p \Leftrightarrow \rho_{E_2,p}(G_K) \subseteq \left\{ \begin{pmatrix} \chi_p(G_K) & * \\ 0 & 1 \end{pmatrix} \right\}$. $\blacksquare$

TATEOVE KRIVULJE

SILVERMAN: ADVANCED TOPICS IN A.E.C.

IDEJA: Nad $\mathbb{C}$ $\mathbb{C}/\Lambda_E \simeq E(\mathbb{C})$

ŽELJA Analogon nad $\mathbb{Q}_p$? ISTO $\mathbb{Q}_p/$"Λ" ?

PROBLEM: $(\mathbb{Q}_p, +)$ nema diskretnih podgrupa.

$t \in \Lambda$ (diskr. podgrupa)

$\Rightarrow p^n t \in \Lambda \Rightarrow \lim_{n \to \infty} p^n t = 0 \in \Lambda$

$\Rightarrow 0$ je gomilište.

"RJEŠENJE": BSO $\Lambda \simeq \mathbb{Z} + \mathbb{Z}\tau$

~~eksponencijalno~~ preslikavanje exp $X \mapsto e^{2\pi i X}$

$q := e^{2\pi i \tau}$

$\Rightarrow E(\mathbb{C}) \simeq \mathbb{C}/\Lambda \simeq \mathbb{C}^\times/q^{\mathbb{Z}}$, gdje je $q^{\mathbb{Z}} = \langle q \rangle$

Ako uzmemo istu stvar za $\mathbb{Q}_p$ zato $\mathbb{Q}_p^\times$ ima puno diskretnih podgrupa: $q^{\mathbb{Z}}$ t.d. $|q|_p \neq 1$. ~~$E(\mathbb{Q}_p) \simeq \mathbb{Q}_p^\times/q^{\mathbb{Z}}$~~

DIJAGRAM

$\mathbb{C}$	p-adska polja
$\mathbb{C}/\Lambda$	NEMA
$\downarrow$ exp	NE POSTOJI EXP
$\mathbb{C}^\times/q^{\mathbb{Z}}$ - - - - →	$\mathbb{Q}_p^\times/q^{\mathbb{Z}}$

$G/\Lambda \cong E(\mathbb{C})$

Neka je K p-adsko polje (npr. $K = \mathbb{Q}_p$). Neka je $q \in K^\times$ t.d. $|q|<1$.

Def $s_k(q) := \sum_{n\geq 1} \frac{n^k q^n}{1-q^n}$ $\quad a_4(q) := -s_3(q)$

$a_6(q) := -\frac{5s_3(q) + 7s_5(q)}{12}$.

Ovo sve konvergira u K.

TATEOVA KRIVULJA PRIDRUŽENA q je

$$E_q : Y^2 + XY = X^3 + a_4(q)X + a_6(q).$$

Ovo je eliptička krivulja s $\Delta(E_q) = q\prod_{n\geq 1}(1-q^n)^{24}$

i $j(E_q) = \frac{1}{q} + 744 + 196884\, q^2 + \ldots$

TEOREM (TATE) Postoji analitički izomorfizam

$$\phi : E_q(\overline{K}) \longrightarrow \overline{K}^\times / q^{\mathbb{Z}}$$

koji je kompatibilan s djelovanjem od G_K. (ovdje je K p-adsko polje).

($\Leftrightarrow$ IZOMORFIZAM G_K – modula)

LEMA Neka $E/\mathbb{Q}$ ima rascjepivu multiplikativnu redukciju. Tada $E/\mathbb{Q}_p$ je izomorfna s $E_q/\mathbb{Q}_p$ nad za neki q. Dakle E je Tateova krivulja.

Ako $E/\mathbb{Q}_p$ ima potencijalnu multiplikativnu redukciju* tada je E kvadratni twist od neke E_q.

$\Rightarrow$ $\boxed{- \mathcal{G}_Y(E)/\mathcal{G}_0(E).}$

PROMJENA REDUKCIJE $E/K_1 \to E/K_2$, $K_2 \supseteq K_1$

$p \in K_1$ $\qquad \mathfrak{p} \in K_2$, $\mathfrak{p} \mid p$.

DOBRA	$\longrightarrow$	DOBRA
MULTIPL	$\longrightarrow$	MULTIPL

$(p \nmid \Delta \Rightarrow \mathfrak{p} \nmid \Delta)$

ADIT $\overset{\text{NAKON DOVOLJNO PROŠ}}{\Longrightarrow}$ DOBRA ili MULTIP

EL. krivulje koje ongi znaglje DOBRU ili MULTIPL = POLU-STABILNE

POTENCIJALNO DOBRA = DOBRA ili ADITIVNA koja POSTANE DOBRA

— || — MULT = MULT — || — MULT.

POT. MULT

E ima POT. MULT. red u p $\Longleftrightarrow$ $|j(E)|_p > 1$

$\left(\Leftrightarrow v_p(j(E)) < 1 \right.$

$\left. \Leftrightarrow p \text{ dijeli nazivnik od } E \right)$

KOROLAR $E_q(\bar{K}) \xrightarrow{\sim} \boxed{\bar{K}^\times / q^{\mathbb{Z}}}$

KOROLAR Neka je $E = E_q$ Tatova krivulja. Tada je

$$\rho_{E,N}(G_K) \sim \begin{pmatrix} \chi_N & * \\ 0 & 1 \end{pmatrix}.$$

Dokaz Što je $E_q(\bar{K})[n] = \langle \zeta_N, q^{\frac{1}{N}} \rangle$.

1 $E_q[N] \simeq \langle \zeta_N, q^{\frac{1}{N}} \rangle$ $\qquad \phi : E_q[N] \to K^*/q^{\mathbb{Z}}$

$\sigma \in G_K$

$$\zeta_N^{\sigma} = \zeta_N^{\chi_N(\sigma)}, \quad \left(q^{\frac{1}{N}}\right)^{\sigma} = \zeta_N^{a_\sigma} q^{\frac{1}{N}}$$

Neka je $P = \phi^{-1}(\zeta_N)$, $Q = \phi^{-1}(q^{\frac{1}{N}})$

$$\Rightarrow P^{\sigma} = \chi_N(\sigma) P, \quad Q^{\sigma} = a_\sigma P + Q$$

$$\Rightarrow \rho_{E,N}(\sigma) = \begin{pmatrix} \chi_N(\sigma) & a_\sigma \\ 0 & 1 \end{pmatrix}$$ ∎

<u>Korolar</u> Neka je $E/\mathbb{Q}$ ima potencijalno mult. redukciju

Neka je $D_p \le G_{\mathbb{Q}}$ dekompozicijska grupa, $D_p \simeq Gal(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Po prošlom korolaru

$$\Rightarrow \rho_{E,N}(D_p) = \begin{pmatrix} \chi_N & * \\ 0 & 1 \end{pmatrix}.$$

Ali E ima pot. mult. red. u p tada je

$$\rho_{E,N}\big|_{D_p} \sim \psi \cdot \begin{pmatrix} \chi_N & * \\ 0 & 1 \end{pmatrix} \quad \text{gdje}$$

$$\sigma\left(\sqrt{-\frac{c_4}{c_6}}\right) = \psi(\sigma) \cdot \sqrt{-c_4/c_6}.$$