10. PREDAVANJA

MODULARNE KRIVULJE

- Zanima nas pitanje za zadano polje K i $H \leq GL_2(\mathbb{Z}/N\mathbb{Z})$ kako naći sve (ako ih ima) E/K t.d $\rho_{E,N}(G_K)$ je konjugirana podgrupi od H.
- Ključni alat: MODULARNE KRIVULJE.

VRIJEDI postoji krivulja X_H takve da {ne-hiperboličke} točke na $X_H(K)$ $\xleftrightarrow{1-1}$ { Eliptičke krivulje nad K t.d $\rho_{E,N}(G_K) \underset{k}{\leq} H$ }

Primjetimo da ovo generalizira neprekidna pokrivanja s mogućim beskonačnim stupnjem nad K ili izomorfizam nad K.

Reference: DIAMOND – SHURMAN: INTRODUCTION TO MODULAR FORMS (nad $\mathbb{C}$)

$\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$ $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$

SILVERMAN & KNAPP (nad PAB)

MODULARNE KRIVULJE NAD $\mathbb{C}$

$X(1)$ Neka je $\mathcal{H} = \{x + yi : x, y \in \mathbb{R}, y > 0\}$.

Sjetimo se da $\forall \tau \in \mathcal{H}$ $\exists!$ E_τ t.d $E_\tau(\mathbb{C}) \simeq \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$

Izhodišče (DZ) $E_{\tau_1} \simeq E_{\tau_2}$ za $\tau_1, \tau_2 \in \mathbb{H}$

$\Leftrightarrow \exists\, \gamma \in SL_2(\mathbb{Z})$ t.d. $\gamma(\tau_1) = \tau_2$

$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $z \in \mathbb{H}$

$\gamma(z) := \frac{az+b}{cz+d}$

Rohle $SL_2(\mathbb{Z}) \backslash \mathbb{H}$ $\longleftrightarrow$ { klase izomorfizma $E/\mathbb{C}$ }.

IMA STRUKTURU RIEMANNOVA PLOHA (DS)

Mestetum nizi kompaktno def $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$

$\Rightarrow \quad SL_2(\mathbb{Z}) \backslash \mathbb{H}^*$ je kompaktna Riemannova ploha.

Izrek (Riemann tm o egzistenci) + kompaktna Riemannova ploha je algebrska krivulja.

$\rightarrow \quad SL_2(\mathbb{Z}) \backslash \mathbb{H}$ je krivulja kojoj fali 1. točka (jen vizeli $\mathbb{P}^1(\mathbb{Q})$ čini 1 orbita s obzirom na $SL_2(\mathbb{Z})$.

Može se pokazati da je $SL_2(\mathbb{Z}) \backslash \mathbb{H}^* =: X(1)$ genusa 0. $\Rightarrow$ $X(1) \simeq \mathbb{P}^1$

$j : SL_2(\mathbb{Z}) \backslash \mathbb{H}^* \longrightarrow X_1(\mathbb{C})$

$SL_2(\mathbb{Z}) \cdot \tau \longmapsto j(\tau) := \frac{1}{q} + 744 + 196884\, q^2 + \dots$

$q := \begin{cases} e^{2\pi i \tau}, & \tau \in \mathbb{H} \\ 0, & \tau \in \mathbb{P}^1(\mathbb{Q}) \end{cases}$

$j(\tau) = j(E_\tau)$

Što ako promatramo nad $K^{\times}$, K je PAB?

Isto vrijedi do odgovora

$Y_1(1) := X(1) \setminus$ hrrp

$Y_1(K) \longleftrightarrow \{ E/K$ do na $\overline{K}$ - izomorfizam$\}$

MODULARNE KRIVULJE $X_0(N)$ i $X_1(N)$ nad $\mathbb{C}$

Neka su $\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : a \equiv d \equiv 1 \pmod N \text{ i } c \equiv 0 \pmod N \right\}$

i $\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \pmod N \right\}$.

i $\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv d \equiv a-1 \equiv d-1 \equiv 0 \pmod N \right\}$

Isto $\Gamma(N) \leq \Gamma_1(N) \leq \Gamma_0(N) \leq SL_2(\mathbb{Z})$.

Promotrimo se <u>klase izomorfizam</u> (E, P) gdje je $P \in E$ t.d $|P| = N$. $(E_1, P_1) \simeq (E_2, P_2)$ ako $\exists\ \phi : E_1 \to E_2$ izom. el. krulje t.d $\phi(P_1) = P_2$.

Klasu izomorfizam od (E, P) označimo s $[(E, P)]$.

VJ: Želimo ze da $P \in E[N]$, $\underbrace{|P| = N}$, $E_\tau \simeq \mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau \Rightarrow$

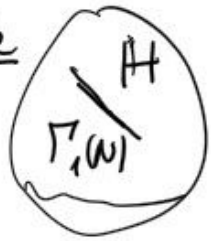
$\Rightarrow P = \frac{a}{N} + \frac{b}{N}\tau$.

Može se pokazati za (E_τ, P) da $\exists\ \tau_0 \in \mathcal{H}$ t.d $\exists\ \phi : E_\tau \to E_{\tau_0}$ izomorfizam t.d $\phi(P) = \frac{1}{N}$.

Štoviše može se pokazati $\left(E_{\tau_1}, \frac{1}{N}\right) \simeq \left(E_{\tau_2}, \frac{1}{N}\right)$

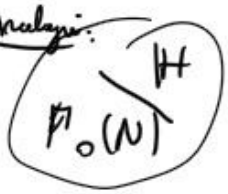
$\Leftrightarrow \gamma(\tau_1) = \tau_2$ za neki $\gamma \in \Gamma_1(N)$

Dedekind

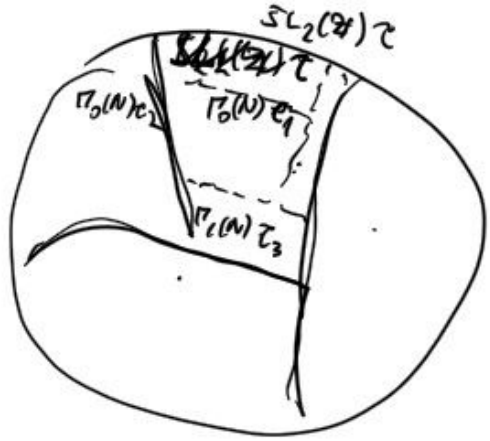


$\longleftrightarrow$ {klase izomorfizama (E_τ, P), $|P|=N$}.

Analogno:



$\longleftrightarrow$ { klase izomorfizama $(\mathbb{E}_\tau, \langle P \rangle)$, $|P|=N$ }.



Def $Y_1(N) := \backslash^{H}_{\Gamma_1(N)}$ $\quad Y_0(N) := \backslash^{H}_{\Gamma_0(N)}$

$X_1(N) := \backslash^{H^*}_{\Gamma_1(N)}$ $\quad X_0(N) := \backslash^{H^*}_{\Gamma_0(N)}$

Činjenice $X_1(N)$ i $X_0(N)$ su def nad $\mathbb{Q}$.

Nad PBB K

$X_1(N)(K) \longleftrightarrow \{ [(E,P)]$ gdje je E/K, i $P \in E(K) \}$ do na izomorfizam nad K

$X_0(N)(K) \longleftrightarrow \{ [(E,C)]$ gdje je E/K i C je G_K-invarijantna $\}$ do na izomorfizam nad K

Primjer $E: Y^2 = X^3 + 2$.

$P = (0, \sqrt{2})$ $\quad |P| = 3$ $\quad P \notin E(\mathbb{Q})$.

$(E, P) \in Y_1(3)(\mathbb{Q})$?

Da bi odgovorili $[(E,P)] = [(\bar{E}, \bar{P})]^\sigma$ $\forall \sigma \in G_{\mathbb{Q}}$??

~~$[(E,P)]^\sigma = [(E^\sigma, P^\sigma)]$~~ $\quad \sigma(\sqrt{2}) = -\sqrt{2}$

$$[(E,P)]^\sigma = [(E,P)^\sigma] = [(E^\sigma, P^\sigma)] = [(E, P^\sigma)]$$

$$= [(E, (0, -\sqrt{2}))] = [(E, -P)]$$

Mestrićin

$[-1] : E \to E$ je automorfizam

$$[-1](E,P) = (E, -P) \Rightarrow [(E,P)] = [(E,-P)]$$

$$\Rightarrow [(E,P)] = [(E,P)]^\sigma$$

$$= [(E,P)] \in Y_1(3)(\mathbb{Q}).$$

$Y_1(11), X_1(11)$, dijamo skraćeno da ne postoji e.k. s torzijom reda 11 nad $\mathbb{Q}$.

$\exists$ Prekp. do $\exists$ $E/\mathbb{Q}$ t.d. $P \in E(\mathbb{Q})$ $\quad |P| = 11$.

$\Rightarrow [(E,P)] \in Y_1(11)(\mathbb{Q})$

Reći da ne postoji eliptičkih krivulja s torzijom reda 11 nad $\mathbb{Q}$

$\Leftrightarrow$ $Y_1(11)(\mathbb{Q}) = \emptyset$

Dz. Ne postoji e.k. s torzijom reda 11 nad $\mathbb{Q}$.

E, Pic , $|P|=11$ $\quad E_{b,a}: y^2+(1-a)xy-by=x^3-bx^2$

$6P=-5P \Rightarrow x(6P)=x(-5P)$

$$\frac{(a-b)(a^3+ba-b^2)}{(a-b+a^2)^2}=\frac{-ba(b-a-a^2)}{(b-a)^2}$$

$b=a$

$\sim \Leftrightarrow$ $b^2-b=a^3-a^2$ = jednačba od $X_1(11)$

ono je eliptička krivulja

koegumi na $X_1(11)$ za one (b,a) t.d

$E_{b,a}$ singularna.

Nisu pustinji $\Leftrightarrow$ da postoji $\exists\ (b,a)\neq Y_1(11)(\mathbb{Q})$

t.d $E_{b,a}$ nije singularna?

$|X_1(11)(\mathbb{Q})|=5$ i za točke (b,a) za

t.d $\Delta(E_{b,a})=0$.

$\Rightarrow$ Nema E.K. s torzijom reda 11

nad $\mathbb{Q}$.