Preslikavanja modularnih krivulja u projektivna ravnina definirana modularnim formama

T. Miyake: Modular forms
(prema disertaciji Ive Kodrnji,
G. Muić: On degrees in family, ...)
-||- : On degrees and birationality ...

Neka je $\tilde{\Gamma} \leq SL_2(\mathbb{Z})$ kongruencijska podgrupa (ili bilo koja grupa konačnog indeksa). Neka je $k \geq 2$ paran broj t.d. $\dim M_k(\tilde{\Gamma}) \geq 3$. Neka su $f, g, h \in M_k(\Gamma)$ tri linearno nezavisne forme. Promatramo preslikavanje definirano formulom:

$$z \xmapsto{\varphi} (f(z) : g(z) : h(z)) \in \mathbb{P}^2(\mathbb{C}) \quad \text{za } z \in \mathbb{H}$$

Formula ima smisla ako $f(z)$, $g(z)$ i $h(z)$ istovremeno nisu 0.

Uočimo, za $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \tilde{\Gamma}$

$$\gamma z \xmapsto{\varphi} ((cz+d)^k f(z) : (cz+d)^k g(z) : (cz+d)^k h(z))$$

$$= (f(z) : g(z) : h(z)) \text{ jer } cz+d \neq 0.$$

Pa φ definira holomorfno

preslikavanje s

$$\varphi : \mathbb{H}/\tilde{\Gamma} - \left\{ \begin{matrix} \text{zajedničkih} \\ \text{nultočaka} \end{matrix} \right\} \longrightarrow \mathbb{P}^2(\mathbb{C})$$

Što ako je $z_0 \in \mathbb{H}$ zajednička nultočka?

Možemo pretp. da je $\operatorname{ord}_{z_0}(h) \le \operatorname{ord}_{z_0}(f), \operatorname{ord}_{z_0}(g)$.

za alg. analogon ove tvrdnje trebamo nesingularnu pa u z_0

Tada definiramo

ima smisla

$$\varphi(z_0) = \left(\frac{f}{h}(z_0) : \frac{g}{h}(z_0) : 1 \right)$$

tako proširujem φ do $\mathbb{H}/\tilde{\Gamma}$, a uz

do kaspova

malo truda i do holomorfne funkcije.

$$\varphi : X(\tilde{\Gamma}) \to \mathbb{P}^2(\mathbb{C})$$

kompaktna Riemannova ploha.

to je krivulja: njeno funkcijsko polje je definirano s $\frac{f}{h}, \frac{g}{h}$.

Slika preslikavanja

ćemo označiti s

$C(f,g,h) \subset \mathbb{P}^2(\mathbb{C})$

mod. fje. na $X(\tilde{\Gamma})$

Napomena: Krivulja $C(f,g,h)$ je ireducibilna.

Želimo opisati formulu za $\deg \varphi \cdot \deg C(f,g,h)$.

Odaberimo pravac

$\ell : Ax + By + Cz = 0 \subset \mathbb{P}^2$ koji

ne prolazi kroz singularne točke od $C(f,g,h)$.

$\deg C(f,g,h)$ je jednak broju točaka u presjeku

$\ell \cap C(f,g,h)$. Na ℓ možemo

gledati i kao na funkciju na $C(f,g,h)$:

$$(x:y:1) \xrightarrow{\ell} (Ax + By + C : 1)$$

koja je slično def. i na ostalim afinim okolinama od $\mathbb{P}^2$

Tada je $\varphi^*(\ell)$ funkcija

$$X(\hat{\Gamma}) \xrightarrow{\varphi} C(f,g,h) \longrightarrow \mathbb{P}^1(\mathbb{C})$$

Uočimo da je broj nultočaka funkcije

$\varphi^*(\ell)$ jednak $\deg \varphi \cdot \deg C(f,g,h)$

broj praslika od φ

broj točaka presjeka pravca ℓ i $C(f,g,h)$

pažnja! ovdje "brojimo" samo točke presjeka $\ell \cap C(f,g,h)$ koji se nalaze u afinom otv. skupu $(x:y:1)$!

No

$$\varphi^*(\ell)(z) \text{"="} A \frac{f}{h}(z) + B \cdot \frac{g}{h}(z) + C$$

Koliko nultočaka ima f-ja $\dfrac{Af+Bg}{h} + C$?

pažnja: eliptičke točke i kaspovi (Riem. plohe)

Onoliko koliko ima i polova. Koliko ima polova? Budući da su A, B i C "generički", polovi funkcije su nultočke od h s time da moramo "odbaciti" zajedničke nultočke funkcija f, g i h (s kratnostima).

ovo je malo neprecizno ... pazi na odabir afine okoline od $\mathbb{P}^2$

Stupanj kao kvadratna forma i Hasseov teorem

Teorem (Hasse) $E/\mathbb{F}_q$ el. krivulja, $q = p^s$

Tada je $\left| E(\mathbb{F}_q) - q - 1 \right| \leq 2\sqrt{q}$.

Neka su x i y funkcije na E iz nekog Weierstrassovog modela $y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$

Definiramo morfizam $\phi : E \to E$

$(x, y) \mapsto (x^q, y^q)$ koji zovemo

Frobeniusov (endo)morfizam.

(jer vrijedi $(\tilde{x} + \tilde{y})^q = \tilde{x}^q + \tilde{y}^q$ nad $\mathbb{F}_q[\tilde{x}, \tilde{y}]$

kao i $a^q = a \ \forall a \in \mathbb{F}_q$).

Vrijedi:
$$\forall \alpha \in \overline{\mathbb{F}_q}, \ \alpha \in \mathbb{F}_q \Leftrightarrow \alpha^q = \alpha$$

(jer je $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ topološki generirana

s $x \mapsto x^q \ldots$) pa za $P \in E(\overline{\mathbb{F}_q})$ vrijedi

$$P \in E(\mathbb{F}_q) \Leftrightarrow \phi(P) = P$$

pa je $E(\mathbb{F}_q) = \ker(1-\phi)$, odnosno

$$|E(\mathbb{F}_q)| = |\ker(1-\phi)| = \deg(1-\phi)$$

jer je preslikavanje $1-\phi$ separabilno

kako se provjeri separabilnost? mora vrijediti:
$(1-\phi)^*\omega \neq 0$ gdje je ω invarijantan diferencijal

Ključna opservacija: $1-\phi$

$$\deg : \mathrm{End}(E) \longrightarrow \mathbb{Z} \quad \text{je}$$

pozitivno definitna kvadratna forma.

Što to znači i zašto je to važno?

Kvadratne forme = homogeni polinomi stupnja 2

Primjer: x^2+y^2 ... koji brojevi se mogu prikazati pomoću kvadratne forme? = koji stupnjevi izogenija se postižu?

Generalizacija:

Neka je M $\mathbb{Z}$-modul.

$b: M \times M \to \mathbb{Z}$ $\longmapsto$ $q: M \to \mathbb{Z}$

$\mathbb{Z}$-bilinearna forma $\qquad$ kvadratna forma

$$q(v) = b(v,v) \qquad \left[\; b(u,v) = \frac{q(u+v)-q(u)-q(v)}{2} \;\right]$$

Npr. za $M=\mathbb{Z}^2$ možemo definirati

$$q(x,y) = x^2+y^2$$

$$\longleftrightarrow b((x_1,y_1),(x_2,y_2)) = x_1x_2 + y_1y_2$$

vrijedi: $q(x,y) = b((x,y),(x,y))$

i $b((x_1,y_1),(x_2,y_2)) = ((x_1+x_2)^2 + (y_1+y_2)^2 - x_1^2 - y_1^2 - x_2^2 - y_2^2)/2$

$= 2(x_1x_2+y_1y_2)\cdot\frac{1}{2} = x_1x_2+y_1y_2$

Definicija: Neka je A abelova grupa ($\mathbb{Z}$ - modul)

Fja. $d: A \to \mathbb{Z}$ je kvadratna forma ako

i) $d(\alpha) = d(-\alpha)$ $\forall \alpha \in A$

ii) Sparivanje $A \times A \to \mathbb{Z}$ definirano s

$(\alpha, \beta) \mapsto d(\alpha+\beta) - d(\alpha) - d(\beta)$ je (simetrično)

bilinearno.

Kvadratna forma je pozitivno definitna ako

iii) $d(\alpha) \geq 0$ za sve $\alpha \in A$

i $d(\alpha) = 0$ ako i samo ako $\alpha = 0$.

Napomena:

i) $(\alpha, \beta) + (\alpha, 0) = (\alpha, \beta) \Rightarrow (\alpha, 0) = 0 \Rightarrow d(0) = 0$

ii) $(\alpha, -\alpha) = -2d(\alpha)$, $(\alpha, \alpha) = d(2\alpha) - 2d(\alpha)$

$\Rightarrow (\alpha, -\alpha) + (\alpha, \alpha) = (\alpha, \alpha - \alpha) = 0 \Rightarrow 2d(\alpha) = d(2\alpha) - 2d(\alpha)$

$\Rightarrow d(2\alpha) = 4d(\alpha) \Rightarrow \frac{1}{2}(\alpha, \alpha) = d(\alpha)$

$\Downarrow$ indukcija

$d(n\alpha) = n^2 d(\alpha)$

(iii) Ako su $\alpha, \beta \in M$ i $x, y \in \mathbb{Z}$ onda

$$q(x\alpha + y\beta) = \frac{1}{2}(x\alpha + y\beta, x\alpha + y\beta)$$

$$= \frac{1}{2}\Big((\alpha,\alpha)x^2 + \big((\beta,\alpha)+(\alpha,\beta)\big)xy + (\beta,\beta)y^2\Big)$$

standardna kvadratna forma

ako su α i β generatori, onda

iz gornje jednadžbe možemo vidjeti koje se

vrijednosti postižu.

izogenije definirane nad $\overline{\mathbb{F}_q}$

$\mathbb{Q}$ - algebra

$R \leq K$

potprsten koji je konačno generiran kao $\mathbb{Z}$-modul t.d. $R \otimes_{\mathbb{Z}} \mathbb{Q} = K$

Kako izgleda End(E)?

End(E) je poredak (order) u
red

$\mathbb{Z} + f \cdot \mathcal{O}$

kvadratnom imaginarnom polju ili u

kvaternionskoj (definitnoj) algebri nad $\mathbb{Q}$

$K = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$ gdje je

$\alpha^2 < 0$, $\beta^2 < 0$ i $\alpha\beta = -\beta\alpha$.
$\in \mathbb{Q}$ $\in \mathbb{Q}$

Propozicija: $\deg$ je kvadratna forma na $\mathrm{End}(E)$

Dokaz: Treba provjeriti da je sparivanje

$$\langle \phi, \psi \rangle = \deg(\phi + \psi) - \deg \phi - \deg \psi$$

bilinearno. Označimo s $[\cdot] : \mathbb{Z} \to \mathrm{End}(E)$ standardno množenje. Računamo

homomorfizam

$$[\langle \phi, \psi \rangle] = [\deg(\phi + \psi)] - [\deg(\phi)] - [\deg \psi]$$

$$= \widehat{\phi + \psi} \circ (\phi + \psi) - \hat{\phi}\phi - \hat{\psi}\psi$$

dualna izogenija

$$= \hat{\phi} \circ \psi + \hat{\psi} \circ \phi$$

ovaj izraz je očito linearan u ϕ i ψ

$\Rightarrow [\langle \phi, \psi \rangle]$ je bilinearno

$\Rightarrow \langle \phi, \psi \rangle$ je bilinearno (jer je $[\cdot]$ ulaganje)

$\blacksquare$

Zašto nam je to važno? Zbog Cauchy-Schwartzove nejednakosti:

$$|x_1 x_2 + y_1 y_2| \le \sqrt{(x_1^2+y_1^2)(x_2^2+y_2^2)}$$

ili

$$\frac{1}{2}\,|q(\alpha+\beta)-q(\alpha)-q(\beta)| \le \sqrt{q(\alpha)\,q(\beta)}$$

za sve $\psi, \phi \in A$

dokažite za d.z.

Posebno

$$|\deg(1-\phi)-\deg(1)-\overbrace{\deg(-\phi)}^{q}| \le 2\sqrt{\deg 1 \cdot \deg(-\phi)}$$

$$\Rightarrow \big|\,|E(\mathbb{F}_q)|-1-q\,\big| \le 2\sqrt{q}$$ ∎

ϕ je inseparabilno preslikavanje stupnja

oznaka za funkcije polja od E.

q jer je $\deg\varphi = \left|\mathrm{Aut}\left(\overline{\mathbb{F}_q}(x,y)\big/\phi^*\overline{\mathbb{F}_q}(x,y)\right)\right|$

$$= \left|\mathrm{Aut}\left(\overline{\mathbb{F}_q}(x,y)\big/\overline{\mathbb{F}_q}(x^q,y^q)\right)\right|$$

$= q$ jer je $\overline{\mathbb{F}_q}(x,y) = \overline{\mathbb{F}_q}(x^q,y^q)(x)$

Još jedna kvadratna forma ... determinanta

za 2×2 matrice.

Vrijedi: $\det(A+B) - \det A - \det B = \operatorname{tr}(A^* B)$

gdje je $A^* = \operatorname{tr} A \cdot I - A$

$(\det(1-A) - 1 - \det A = \operatorname{tr} A)$

deg i det su povezani preko Tate-ovog modula $T_\ell(E)$ je $\phi \in \operatorname{End}(E)$ inducira linearno preslikavanje $\phi_\ell : T_\ell(E) \to T_\ell(E)$ na Tateovom modulu. Vrijedi

$$\det \phi_\ell = \deg \phi \quad \text{i} \quad \operatorname{tr}(\phi_\ell) = 1 + \deg \phi - \deg(1-\phi)$$

pa Hasseov teorem implicira

$$|\operatorname{tr}(\phi_\ell)| \leq 2\sqrt{q}$$

pažnja: $\det \phi_\ell$ i $\operatorname{tr}(\phi_\ell)$ su a priori u $\mathbb{Z}_\ell$ ali iz gornjeg se vidi da su u $\mathbb{Z}$! tj. karakt. polinom od ϕ_ℓ je iz $\mathbb{Z}$!