11. predavanje

DJELIDBENI POLINOMI

- referenca WASHINGTON : ELLIPTIC CURVES

$E : y^2 = x^3 + Ax + B$

Definiramo DJELIDBENE POLINOME $\psi_m \in \mathbb{Z}[x, y, A, B]$

$$\psi_0 = 0 \quad \psi_1 = 1, \quad \psi_2 = 2y, \quad \psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$$

$$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$$

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad \text{za } m \geq 2$$

$$\psi_{2m} = (2y)^{-1}\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \quad \text{za } m \geq 3.$$

Def $\phi_m := x\psi_m^2 - \psi_{m+1}\psi_{m-1}$

$$\omega_m := (4y)^{-1}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)$$

TEOREM Neka je $P = (x, y)$ točka na $E : y^2 = x^3 + Ax + B$ nad K, char $K \neq 2$ i neka je $n \in \mathbb{N}$.

Tada je $nP = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x,y)}{(\psi_n(x,y))^3} \right)$.

Nap. $\psi_n^2 \in \mathbb{Z}[x, A, B]$

$\phi_n \in \mathbb{Z}[x, A, B]$

← RAČUNSKI DOKAZ

za neparni n $\psi_n \in \mathbb{Z}[x, y^2, A, B]$, jer uvrstimo relaciju $y^2 = x^3 + Ax + B$

$\Rightarrow \psi_n \in \mathbb{Z}[x, A, B]$

Iz teorema slijedi da je $|P| = d$ t.d. $d \mid n$, n neparan

$\Rightarrow$ $\boxed{\psi_n(x(P)) = 0}$

- na ovaj način možete naći najbližim polju potpuni nula točke reda $\underline{n}$.

__Nap.__ Polje cijepanja od $\psi_n(x)$ je polje

$$\mathbb{Q}(x(E[n])) := \mathbb{Q}(\{x(P) : P \in E[n]\}).$$

$$[\boxed{\mathbb{Q}(E[n])} : \mathbb{Q}(x(E[n]))] = 1, 2 \text{ ili } \boxed{4}.$$

$[\mathbb{Q}(P) : \mathbb{Q}(x(P))] = 1$ ili 2.

$\mathbb{Q}(E[n]) = \mathbb{Q}(P, R)$ gdje $\{P, R\}$ baza za $E[n]$.

$\deg \psi_n = \frac{n^2-1}{2}$ (kada n prost)

$$\frac{n^2-1}{2} \cdot \frac{n^2-3}{2}$$

za n prost

$$\Rightarrow [\mathbb{Q}(x(E[n])) : \mathbb{Q}] \le \frac{n(n^2-1)(n-1)}{4}.$$

$\boxed{\mathbb{Q}(E[n])}$ se može izračunati na ovaj način.

$$\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \cong \rho_{E,n}(G_{\mathbb{Q}})$$

MODULARNI POLINOMI

Reference: WASHINGTON: ELLIPTIC CURVES

Teorem $\exists$ polinom $\Phi_N(x,y) \in \mathbb{Z}[x,y]$ t.d. za K. polje t.d. $(\mathrm{char}\, K, N) = 1$ vrijedi:

$\exists$ cikl. izogenija (nad $\bar{K}$) stupnja N između $E_1, E_2 \iff \Phi_N(j(E_1), j(E_2)) = 0$.

Vrijede sljedeća svojstva:

Prop.: 1) Stupanj od Φ_ℓ je $\ell+1$ $\forall$ prosti broj ℓ.

2) $\Phi_N(x,y) = \Phi_N(y,x)$

3) Kažemo $\Phi_N(j(E_1), y)$ za j-invarijante E.K koje za Nužnost $\supset E_1$.

4) $\Phi_N(x,y)$ ovisi jednadžbu $X_0(N)$.

"Dokaz 4)": $\Phi_N(x_0,y_0) = 0$, $(x_0,y_0) \in K^2 \overset{TM}{\iff}$

$\exists\ E, E'/\bar{K}$ $j(E) = x_0, j(E') = y_0$ i $\phi: E \to E'$ (def nad $\bar{K}$) $\deg \phi = N$.

$(x_0,y_0) \longleftrightarrow (E, \phi: E \to E') \in X_0(N)(\bar{K})$

gdje je K polje gdje su definirani x_0 i y_0.

KORISTI SE SCHOOF-ELKIES-ATKINOV ALGORITAM ZA RAČUNANJE #$E(\mathbb{F}_p)$

E/K

$\boxed{G_K \curvearrowright E[\ell]}$, ali trdnosten deluje in na podgrupe od

$E[\ell]$ – podgrupa ima $\ell+1$ $\leftrightarrow$ predstavniki $\circ$ $\mathbb{P}^1(\mathbb{F}_\ell)$

$\langle(1, x)\rangle$ za $x \in \mathbb{F}_\ell$ $\}$ $\longleftrightarrow$ $(1 : x)$

$\langle(0,1)\rangle$ $\longleftrightarrow$ $(0:1)$

---

1. način $\boxed{G_K \to Aut(\mathbb{P}^1(\mathbb{F}_\ell)) = PGL_2(\mathbb{F}_\ell)}$ $= GL_2(\mathbb{F}_\ell)/Z(GL_2(\mathbb{F}_\ell))$

$(. G \curvearrowright X \rightsquigarrow \rho : G \to Aut(X)$.

---

2. način do sedaj do G_K deluje na podgrupe od $E[\ell]$ prek $PGL_2(\mathbb{F}_\ell)$ je do prinjetna da

$A \in Z(GL_2(\mathbb{F}_\ell))$ $\quad A \cdot P = \lambda P \Rightarrow A \cdot \langle P\rangle = \langle P\rangle$.

$\Rightarrow Z(GL_2(\mathbb{F}_\ell)) \leq \ker \rho \Rightarrow G_K$ deluje prek $PGL_2(\mathbb{F}_\ell)$

$\boxed{GL_2(\mathbb{F}_\ell)} \to \underline{PGL_2(\mathbb{F}_\ell)}$

Galoisova grupa polja razpada od $\Phi_\ell(j(E), X)$ za neko E/K. je polje nad katerim so definirane vse ℓ-izogenije od E.

Ako je to polje F, tedaj je $[F : K] \leq \# PGL_2(\mathbb{F}_\ell) = \ell(\ell^2-1)$

Def ~~...~~ Neka je ℓ prost broj, def $\ell^* = \begin{cases} \ell & \ell \equiv 1 \mod 4 \\ -\ell & \ell \equiv 3 \mod 4 \end{cases}$

Vrijedi $\mathbb{Q}(\sqrt{\ell^*}) \subseteq \mathbb{Q}(\zeta_\ell)$ za $\ell > 2$

Ovo vidimo jer je $\mathbb{Q}(\zeta_\ell)$ jedino ℓ grana.

~~...~~ $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\zeta_\ell) \Rightarrow |\Delta(\mathbb{Q}(\sqrt{d}))| = \ell$

$\Rightarrow \mathbb{Q}(\sqrt{\ell^*}) \subseteq \mathbb{Q}(E[\ell])$

Def $\mathbb{Q}(\mathbb{P}(E[\ell])) :=$ polje ~~...~~ cijepanja od $\boxed{\Phi_\ell(j(E), X)}$.

Nap $\mathbb{Q}(\mathbb{P}(E[\ell])) \subseteq \mathbb{Q}(E[\ell])$

| $Gal(\mathbb{Q}(\mathbb{P}(E[\ell]))/\mathbb{Q})$ $= P(\rho_{E,\ell}(G_\mathbb{Q}))$, gdje je $P: GL_2(\mathbb{F}_\ell) \to PGL_2(\mathbb{F}_\ell)$ kan. proj.

Prop. 1) $\mathbb{Q}(\sqrt{\ell^*}) \subseteq \mathbb{Q}(\mathbb{P}(E[\ell]))$

2) $\operatorname{disc}(\Phi_\ell(j(E), X)) \equiv \ell^* \ (\operatorname{mod} (\mathbb{Q}^*)^2)$.

~~Dokaz~~ Trebat će nam:

Teorem Neka je $f \in K[X]$ separabilan polinom stupnja n, char $K \neq 2$. Tada slika od Galoisove grupe od $f(X)$ u S_n ima sliku u $A_n \iff \operatorname{disc} f \in (K^*)^2$.

Důkaz: Nechť f normální

$$\Rightarrow \operatorname{desc} f \overset{\text{def}}{=} \prod_{i<j} (\alpha_i - \alpha_j)^2 .$$

definujeme $\delta := \prod_{i<j} (\alpha_i - \alpha_j) \neq 0$

$\Rightarrow \delta \in K(\alpha_1, \dots \alpha_n)$ (pole rozkladu od f) a

$\delta^2 = \operatorname{desc} f$.

Dohle $\operatorname{desc} f \in (K^*)^2 \iff \delta \in K$

Nechť $\sigma \in \mathrm{Gal}(K(\alpha_1, \dots \alpha_n)/K)$ a $\operatorname{sign}(\sigma) = \pm 1$ znaménko permutace.

Dohle $\sigma(\delta) = \prod_{i<j} (\sigma(\alpha_i) - \sigma(\alpha_j)) \overset{\text{def}}{=} \operatorname{sign}(\sigma) \cdot \delta$.

$\Rightarrow \sigma(\delta) = \pm \delta$ ($\operatorname{char} K \neq 2 \Rightarrow \delta \neq -\delta$).

$\sigma \in A_n \overset{\text{def}}{\iff} \operatorname{sign}(\sigma) = 1$

$G := \mathrm{Gal}(K(\alpha_1, \dots \alpha_n)/K) \subseteq A_n \iff \operatorname{sign}(\sigma) = 1 \ \forall \sigma \in G$

$\iff \sigma(\delta) = \delta \ \forall \sigma \in G$

$\iff \delta \in K$

$\iff \operatorname{desc} f \in K^2$

∎

Dokaz prop.

$PGL_2(\mathbb{F}_q)$ djeluje na $q+1$ podgrupa oz. $E \subset \mathbb{F}_q^2$ i na $q+1$ baznih vektora od $\Phi_q(x, y : (E))$ te određuje

hom $\pi : PGL_2(\mathbb{F}_q) \to S_{q+1}$

Pretpostavka da $\operatorname{im} \pi \leq A_{q+1}$

npr $\pi\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\right)$ djeluje je $\langle a \rangle = \mathbb{F}_q^\times$

~~$(1,x)$~~ ~~$(0,1)$~~ ~~$\{(x,1) : x \in \mathbb{F}_q\} \cup \{(0,1)\}$~~

$\{\langle (x,1) \rangle, x \in \mathbb{F}_q\} \cup \{\langle (1,0) \rangle\}$

ORBITE: $\{\langle (1,0) \rangle\}$, $\{\langle (0,1) \rangle\}$, $\{(1,x) : x \in \mathbb{F}_q^\times\}$.

$\Rightarrow \pi\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\right)$ je cikl. duljine $q-1 \Rightarrow$ neparna permutacija.

$\pi^{-1}(A_{q+1}) = : H. \leq PGL_2(\mathbb{F}_q)$

T: ~~Alternirajuća~~ H je $= \underbrace{PSL_2(\mathbb{F}_q)}_{SL_2(\mathbb{F}_q)/\langle \pm I \rangle} = \{A \in PGL_2(\mathbb{F}_q) \mid \det A = 1\}$.

$[PGL_2(\mathbb{F}_q) : PSL_2(\mathbb{F}_q)] = 2$ $PSL_2(\mathbb{F}_q)$ je prava grupa.

Vrijedi da je $PSL_2(\mathbb{F}_q)$ jedina podgrupa indeksa 2.

Pp. suprotno $\exists H_2 [PGL_2(\mathbb{F}_q) : H_2] = 2$. ~~Iz~~ i $H_2 \neq PSL_2(\mathbb{F}_q)$

~~Iz~~ $PSL_2(\mathbb{F}_q) \cap H_2$ je indeksa 2u $PSL_2(\mathbb{F}_q)$.

$\Rightarrow \in$ $PSL_2(\mathbb{F}_q)$ prosta.

Nebo je $\mathrm{sign} : G_{\mathbb{Q}} \to \{\pm 1\}$

$$\mathrm{sign}(\sigma) = \begin{cases} 1 & \text{pro je } \det \rho_{E,\ell}(\sigma) = \square \\ -1 & \text{jinak.} \end{cases}$$

Připomeňme $P : GL_2(\mathbb{F}_\ell) \to PGL_2(\mathbb{F}_\ell)$

$\det GL_2(\mathbb{F}_\ell) = \square$

$\det P(A) = \square \iff \det(A) = \square$.

$\Updownarrow$

$P(\sigma) \in PSL_2(\mathbb{F}_\ell)$

$\mathrm{sign}(\sigma) = 1 \iff P(\rho_{E,\ell}(\sigma)) \in PSL_2(\mathbb{F}_\ell)$

Protože je $\det$ je zobrazení homomorfismus

$P\rho_{E,\ell}(\sigma) \in PSL_2(\mathbb{F}_\ell) \iff \det \rho_{E,\ell}(\sigma) \in (\mathbb{F}_\ell^*)^2$

$\iff \chi_\ell(\sigma) \in (\mathbb{F}_\ell^*)^2$

$\iff \sigma$ [illegible]

σ je v podgrupě indexu 2 odpovídající $\mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q})$

$\iff \sigma$ fixuje $\mathbb{Q}(\sqrt{\ell^*})$.

Dáno $\Phi_\ell(\gamma_{1,j}(E)) \in (\mathbb{K}^*)^2 \iff \mathrm{sign}(\sigma) = 1 \quad \forall \sigma \in G_{\mathbb{K}}$

$\iff \sigma$ fixuje $\mathbb{Q}(\sqrt{\ell^*})$ $\forall \sigma \in G_{\mathbb{K}}$.

K [illegible] v K pokud v kterém je $\det(\Phi_\ell(\gamma_{1,j}(E))) = \square$

$\iff \mathbb{K} \supseteq \mathbb{Q}(\sqrt{\ell^*})$.

$\Rightarrow \operatorname{disc}\left(\Phi_\ell(\varphi_{1,j}(E))\right) = \square$ ili $\boxed{\ell^* \square}$ nad $\mathbb{Q}$.

ne može biti $\square$ jer χ_ℓ surjektivan.