4. predavanje.

Def JEZGRA DJELOVANJA $\varphi: G \times X \to X$ je

$$\underline{\operatorname{Ker}\varphi = \{ g \in G \mid g \cdot x = x \ \forall x \in X \}}.$$

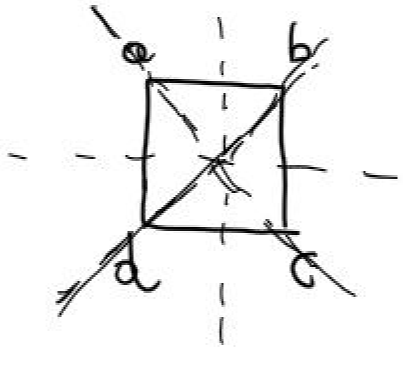
Lako je $\operatorname{Ker}\varphi \trianglelefteq G$ i $G/\operatorname{Ker}\varphi \lesssim \operatorname{Sym} X$

$\lesssim$ = je izomorfna s podgrupom

Def Neka je $\varphi: G \to GL(V)$ reprezentacija od G nad K.

Tada je DIMENZIJA od te reprezentacije $\dim_K V$.

Primjer D_4 djeluje na kvadrat rotacijama i refleksijama.



4 rotacije (0, 90, 180, 270)

id, $(abcd)$, $(ac)(bd)$, $(adcb)$

4 osne simetrije

$(ad)(bc)$, $(ab)(cd)$, (ac), (bd)

$D_4 \curvearrowright X = \{a, b, c, d\}$

VJERNO, TRANZITIVNO

$$X^{(ac)} = \{ b, d \}, \quad (D_4)_b = \{ id, (ac) \}$$

Možemo $D_4 \curvearrowright X_2 = \{ac, bd\}$.

NIJE VJERNO $\quad \varphi: D_4 \to \operatorname{Sym} X_2$ mora imati jezgru

Npr. 2-dim reprezentacija od D_n nad $\mathbb{R}$:

$$D_n = \langle \sigma, \tau \mid \sigma^n = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle$$

$$\sigma \longmapsto \begin{pmatrix} \cos\frac{2\pi}{n} & \sin\frac{2\pi}{n} \\ -\sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix} \in GL_2(\mathbb{R})$$

$$\tau \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in GL_2(\mathbb{R})$$

$$\rho : G \to GL_2(\mathbb{R}).$$

Zašto gledati Gal. rep. pridružene el. krivuljama?

mod p reprezentacija zadrži informacije ima li E torzijske točke reda p ili ne ($E[p]$) ima li izogenije stupnja p ili ne.

Zad. Koliko E/K ima p-izogenija (izogenija stupnja p) nad $\overline{K}$?

p-izogenije $\longleftrightarrow$ podgrupe reda p na E.

$E[p]$ – koliko ima podgrupa

$\cong$

$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ – ima $p+1$ podgrupa reda p.

$$\{\langle (1,a)\rangle, a \in \{0, \dots, p-1\}\} \cup \{\langle 0,1\rangle\}$$

TOREJA

$P \in E(K)[p]$, $|P| = p \iff P^\sigma = P$, $\forall \sigma \in Gal(\bar{K}/K)$.

$\iff$ za bazu $\{P, Q\}$ (za neko točko Q t.d. $\{P, Q\}$ baza za $E[p]$)

$$\rho_{E,p}(G_K) \subseteq \left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\} \leq GL_2(\mathbb{Z}/p\mathbb{Z}).$$

$E(K)[p] \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \iff \rho_{E,p}(G_K) = \{ I \}$.

IZOGENIJE: $P \in \ker \varphi$, $|P| = p$ $\iff \varphi(P) = 0 \iff (\varphi(P))^\sigma = 0^\sigma = 0$ // $\forall \sigma \in Gal(\bar{K}/K)$.

$\iff \varphi(P^\sigma) = 0$.

, kjer je $\varphi : E \to E'$ | $\deg \varphi = p$; φ def nad K

$\iff \varphi$

$P^\sigma \in \langle P \rangle = \ker \varphi$.

$\iff P^\sigma = \lambda P$ za neki $\lambda \in (\mathbb{Z}/p\mathbb{Z})^\times$.

Naj je $\{P, Q\}$ baza za nad p reprezentacijo.

$$\rho_{E,p}(G_K) \subseteq \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \leq GL_2(\mathbb{Z}/p\mathbb{Z}) \iff P \in \ker \varphi.$$

IZOGENIJA: φ je def nad $K \iff \ker \varphi$ $Gal(\bar{K}/K)$ - invarianta.

WEILOVO SPARIVANJE

Weilovo sparivanje će biti bilinearno sparivanje

$e_n : E[n] \times E[n] \longrightarrow \mu_n$ = grupa n-tih korijena iz jedinice.

$= \{ z \in \mathbb{C} \text{ t.d. } z^n = 1 \}$

Može se definirati "intrinzično" - Silvermanova AEC (pomoću divizora).

<u>Teorem</u> Neka je E/k eliptička krivulja i neka su m i n prirodni brojevi relativno prosti s karakteristikom od k.

Postoji BILINEARNO SPARIVANJE koje se zove WEILOVO SPARIVANJE sa sljedećim svojstvima:
$e_n : E[n] \times E[n] \to \mu_n$

a) BILINEARNO JE: $e_n(P+Q, R) = e_n(P, R)\, e_n(Q, R)$

$$e_n(P, Q+R) = e_n(P, Q)\, e_n(P, R).$$

b) ALTERNIRAJUĆE $e_n(P, P) = 1$ i $e_n(P, Q) = e_n(Q, P)^{-1}$

c) NE-DEGENERIRANO JE: Ako $P \neq O \Rightarrow$ ~~$e_n(P, Q) \neq 1$~~ $\exists Q \in E[n]$ t.d. $e_n(P, Q) \neq 1$.

d) KOMPATIBILNO JE:

$$e_{mn}(P, Q) = e_n(mP, Q)$$

$\forall P \in E[mn], \forall Q \in E[n].$

e) GALOIS-EKVIVARIJATNO JE:

$$e_n(P^\sigma, Q^\sigma) = e_n(P,Q)^\sigma \quad \forall \sigma \in Gal(\overline{K}/K).$$

f) ENDOMORFIZMI: $e_n(\alpha(P), \alpha(Q)) = e_n(P,Q)^{\deg \alpha}$

$\forall \alpha \in End\, E.$

g) SURJEKTIVNO JE: $\forall P \in E[n]$ imam: $\{e_n(P,Q) : Q \in E[n]\}$

$= \mu_m$, gdje $m = |P|$.

Korolar Postoje točke $S, T \in E[m]$ t.d

$e_m(S,T) = \zeta_m$ primitivni korijen iz 1.

Nadalje ako je $E[m] \subseteq E(K)$, tada je $\mu_m \subseteq K$ (tj $\mathbb{Q}(\zeta_m) \subseteq K$)

Mazurov tm: $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/m\mathbb{Z}$ $m = 1 \dots 10$ ili 12

ili $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$, $m = 1 \dots 4$.

Dokaz (korolara): $S = \{e_m(S,T), S,T \in E[m]\} \subseteq \mu_m$.

Neka je $S = \mu_d$ za $d \mid m$.

$$\Rightarrow 1 = e_m(S,T)^d = e_m(d \cdot S, T) \quad \forall S,T \in E[m].$$

NE-DEG $\Rightarrow$

$$\Rightarrow dS = 0.$$ Postoje $S \in E[m]$ proizvoljni

$$\Rightarrow \underline{d = m}$$

$S, T \in E(K) \Leftrightarrow S^\sigma = S$ i $T^\sigma = T$ G-I $\Leftrightarrow e_m(S^\sigma, T^\sigma) = e_m(S,T)^\sigma$ $\forall \sigma \in Gal(\overline{K}/K)$

$\Leftrightarrow e_m(\Gamma,T) \subseteq K$.

Zahtevamo da je $E[m] \subseteq K \Rightarrow \mu_m \subseteq K$ (po prvem delu korolarja).

Primjer. Naj bo E/K eliptična krivulja, $\mathbb{Q}(\zeta_3) \subseteq K$.

Naj bo $Q \in E(K)$, $|Q|=3$, $P \in E[3]$, ~~$P \notin \langle Q \rangle$~~ $P \notin \langle Q \rangle$.

T: $x(P) \in K \Rightarrow P \in K$ $\qquad y^2 = x^3+ax+b$

D: Predpostavimo $y(P) \in L$, $[L:K]=2$. Naj bo $\langle \sigma \rangle = \mathrm{Gal}(L/K)$.

$2P = -P \Rightarrow x(P) = x(2P)$,

$P \notin E(K) \Rightarrow P^\sigma \neq P$.

$$P^\sigma = (x(P), y(P))^\sigma = (x(P)^\sigma, y(P)^\sigma) = (x(P), \ldots) = -P$$

mora biti $= 2P$.

$e_3(P,Q) = \zeta_3$ (Weilova lema), ali $\sigma(\zeta_3) = \zeta_3$ $\forall$ $\sigma \in \mathrm{Gal}(\bar{K}/K)$ (ker je $\zeta_3 \in K$)

pa tudi za $\sigma \in \mathrm{Gal}(L/K)$

$$\underline{\zeta_3} = \zeta_3^\sigma = e_3(P,Q)^\sigma = e_3(P^\sigma, Q^\sigma) = e_3(2P, Q) = e_3(P,Q)^2 = \underline{\zeta_3^2}$$

$\Rightarrow$ ⚡

Lema Neka su $P, T \in E[m]$, $|P| = |T| = m$.

Tada je $e_m(P,T) = 1 \iff T = nP$ za neki $(m,n) = 1$.

(Općenito $\langle P,T \rangle = \mathbb{Z}/m'\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \iff e_m(P,T) = \zeta_{m'}$)
$m' | m$.

Dokaz: ~~$e_m(P,T) = 1 \iff$~~

$\boxed{\Leftarrow}$

$$e_m(P, nP) \underset{BIL}{=} e_m(P,P)^n \underset{ALT}{=} 1^n = 1. \quad \checkmark$$

$\boxed{\Rightarrow}$

Pretp. suprotno $\langle P,T \rangle \simeq \mathbb{Z}/m'\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, $m'|m$, $m'>1$.
Neka je $m = d \cdot m'$

~~$e_{m'}(P, dT) \overset{KOMP}{=} e_{dm'}(dP, dT) = e_m(dP, dT)$~~

~~$e_{m'}(P,T)^d$~~

$$e_m(P, dT) = e_m(P,T)^d = 1^d = 1.$$

$$e_{m'd}(P, dT) = 1 \overset{KOMP}{\Rightarrow} e_{m'}(dP, dT) = 1$$

A s druge strane znamo da je $\langle dP, dT \rangle = E[m']$. $\Rightarrow\Leftarrow$

$\Rightarrow e_m(a(dP) + b(dT), c(dP) + e(dT)) = 1 \quad \forall a,b,c,e \in \mathbb{Z}/m'\mathbb{Z}$ NEDEG ⊠

Lema: Neka je $n \in \mathbb{N}$ i ζ_n n-ti korijen iz 1. Tada $\forall \sigma \in Gal(\mathbb{Q}(E[n])/\mathbb{Q})$ vrijedi

$$\sigma(\zeta_n) = \zeta_n^{\det \rho_n(\sigma)}.$$

Dokaz: Neka je $\langle P, Q \rangle = E[n]$, $e_n(P,Q) = \zeta_n$.

$\forall$ ... n-ti korijen iz 1. ζ vrijedi $\zeta = \zeta_n^m$, $m \in \mathbb{Z}/n\mathbb{Z}$

$\Rightarrow$ $\sigma(\zeta_n) = \zeta_n^{\det \rho_n(\sigma)}$ je dosta da bi se dokazala Lema.

Vrijedi $P^\sigma = aP + bQ$, $Q^\sigma = cP + dQ$ za neke $a, b, c, d \in \mathbb{Z}/n\mathbb{Z}$.

$$\sigma(\zeta_n) = \sigma(e_n(P,Q)) \overset{G-I}{=} e_n(P^\sigma, Q^\sigma) = e_n(aP+bQ, cP+dQ)$$

$$= \underbrace{e_n(P,P)^{ac}}_{1} \cdot e_n(P,Q)^{ad} \, e_n(Q,P)^{bc} \, \underbrace{e_n(Q,Q)^{bd}}_{1} =$$

$$= 1 \cdot \zeta_n^{ad} \cdot \left((\zeta_n)^{-1}\right)^{bc} \cdot 1 = \zeta_n^{ad-bc} = \zeta_n^{\det \rho_n(\sigma)}$$

$$\left(\rho_n(\sigma) = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \right).$$

$\square$

Propozicija $n \in \mathbb{N}$; ζ_n je prim. n-ti korijen od 1.

K PAB, E/K, $G_K = Gal(\bar{K}/K)$.

$\Rightarrow$ $\det \rho_{E,n}(G_K) \cong Gal(\mathbb{Q}(\zeta_n)/K \cap \mathbb{Q}(\zeta_n))$.

Dokaz: Znamo $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

$\{\sigma_a : \zeta_n \mapsto \zeta_n^a\}$

$a \in (\mathbb{Z}/n\mathbb{Z})^\times$.

$\sigma_a \longmapsto a$

Dokaz: Neka je $f : G_K \to Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$

$\sigma \mapsto g \circ \det \circ \rho_{E,n}(\sigma)$

gdje je g kanonski izomorfizam $(\mathbb{Z}/n\mathbb{Z})^\times \to Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$

$a \mapsto \sigma_a$

$(\sigma_a(\zeta_n) = \zeta_n^a)$

Prije je $\det(\rho_{E,n}(G_K)) \leq (\mathbb{Z}/n\mathbb{Z})^\times \Rightarrow f(G_K) \leq Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$

G-T

$\Rightarrow f(G_K) = Gal(\mathbb{Q}(\zeta_n)/K')$ za neki $K' \subseteq \mathbb{Q}(\zeta_n)$.

Prethodna lema $\Rightarrow$ f je restrikcija na

$\sigma \in G_K \longmapsto \sigma|_{\mathbb{Q}(\zeta_n)}$.

$\Rightarrow f(G_K)$ se sestoji od teh avt. σ_a ki fiksirajo $K \cap \mathbb{Q}(\zeta_n) \Rightarrow K' = K \cap \mathbb{Q}(\zeta_n)$. ∎.

<u>Korolar</u> $E/\mathbb{Q} \Rightarrow \det \rho_{E,n}(G_{\mathbb{Q}}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.