7. PREDAVANJE

> **ISPRAVAK:** $Gal(\overline{K}/K) = \varprojlim_{L/K \text{ konačno proširenje}} Gal(L/K)$

GRANANJE

Neka je $K/\mathbb{Q}$ konačno Galoisovo proširenje, $\mathfrak{p}$ prost ideal nad p, $\mathbb{F}_\mathfrak{p} := O_K/\mathfrak{p}$ (polje ostataka od $\mathfrak{p}$).

$D_\mathfrak{p} := D(\mathfrak{p}/p)$, $I_\mathfrak{p} := I(\mathfrak{p}/p)$.

Znamo $\boxed{D_\mathfrak{p}/I_\mathfrak{p} \cong Gal(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)}$ (*)

$$\Rightarrow \quad 1 \to I_\mathfrak{p} \to D_\mathfrak{p} \to Gal(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p) \to 1. \quad (**)$$

Znamo: $Gal(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$ ciklička, generirana FROBENIUSOM σ_p, $\sigma_p(x) = x^p$ $(\forall x \in \mathbb{F}_\mathfrak{p})$.

Ako iz (*) slika od σ_p u $D_\mathfrak{p}/I_\mathfrak{p}$ je generator.
Posebno $I_\mathfrak{p} = \{id\} \Rightarrow$ Slika od σ_p generira $D_\mathfrak{p}$.

Pošto za ne $\mathfrak{p}' | p$ su $D_{\mathfrak{p}'}$ konjugirani, σ_p
$\Rightarrow$ slike od σ_p u $Gal(K/\mathbb{Q})$ daju klasu konjugacije koja se zove FROBENIUS.

__Napomena.__ Ako je $Gal(K/\mathbb{Q})$ Abelova tada je σ_p dobro definiran element iz $Gal(K/\mathbb{Q})$.

Mi promatramo $G_\mathbb{Q} := Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, p neki prost broj.
Želimo nešto ovakvo (**). (Želimo "uvrstiti" $K = \overline{\mathbb{Q}}$).

$$(**) \quad 1 \to I_p \to D_p \to Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p) \to 1$$

__Def.__ Za topološku grupu G kažemo da je $\sigma \in G$ TOPOLOŠKI GENERATOR od G ako je $\langle \sigma \rangle$ gusta u G.

Vnijedi do je σ_p topološki generator od $Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p)$.

Neka je $\mathfrak{p} \subseteq \mathcal{O}_{\overline{\mathbb{Q}}}$ (prosti ciglih algebarskih brojeva), $\mathfrak{p}|p$.

Def $\boxed{D_{\mathfrak{p}} := \{\sigma \in G_{\mathbb{Q}} \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}}$

Reformuliramo $f : D_{\mathfrak{p}} \to Gal(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$.

$\mathbb{F}_{\mathfrak{p}} = \overline{\mathbb{F}_p}$

Kao i prije: $I_{\mathfrak{p}} := \ker f$.

- zove $\mathfrak{p}' | p$ umjesto $D_{\mathfrak{p}}$ se odgovarajuće dekompozicijske grupe konjugirane.
$\Rightarrow D_{\mathfrak{p}}$ je dobro def do na konjugiranje.

VRIJEDI: $\boxed{D_{\mathfrak{p}} \simeq Gal(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)}$

Def Neka je $D_{\mathfrak{p}} \leq G_{\mathbb{Q}}$ dekompozicijska grupa; $I_{\mathfrak{p}} \trianglelefteq D_{\mathfrak{p}}$ inercijska podgrupa. Kažemo da je Galoisova reprezentacija $\rho : G_{\mathbb{Q}} \to GL_n(K)$ NERAZGRANATA ako u ρ ako je $I_{\mathfrak{p}} \leq \ker \rho$ ($\Leftrightarrow \rho(I_{\mathfrak{p}}) = \{1\}$).

Sjetimo se mod N CIKLOTOMSKOG KARAKTERA:

$\chi_N : G_K \to (\mathbb{Z}/N\mathbb{Z})^\times$ def: $\boxed{\zeta_N^\sigma = \zeta_N^{\chi_N(\sigma)}}$

~~Teorem: Neka je K PAB~~

Def Neka je $C : \mathbb{C} \to \mathbb{C}$ kompleksno konjugiranje.
Neka je K PAB, neka je $i' : K \hookrightarrow \mathbb{R}$ neko realno ulaganje koje se proširuje do $i : \overline{K} \hookrightarrow \mathbb{C}$.

Tada je $i^{-1} \circ C \circ i \in G_K$ element koji se zove KOMPLEKSNO KONJUGIRANJE. Umjesti $\{K K\} \hookrightarrow \{\text{ulaganja } i' : K \hookrightarrow \mathbb{R}\}$

Teorem Neka je K PAB

1) Ako je $\tau \in G_K$ kompleksno konjugiranje, tada je $\chi_N(\tau) = -1$.

2) Neka je $\lambda \nmid N$ prost ideal u K i $I_\lambda \subseteq G_K$ inercijska podgrupa od G_K. Tada je $\chi_N(I_\lambda) = \{1\}$, te za Frobenius $\sigma_\lambda \in G_K$ vrijedi $\chi_N(\sigma_\lambda) \equiv N_{K/\mathbb{Q}}(\lambda) \pmod N$.

Nap. Ako je λ prost u K, tada je $\boxed{\sigma_\lambda(x) = x^{N_{K/\mathbb{Q}}(\lambda)}}$.

Dokaz 1) Vrijedi $\zeta_N^\tau = \zeta_N^{-1} \Rightarrow \chi_N(\tau) = -1$.

2) Dokazujemo T: Razlika 2 različita N-tog korijena iz 1 dijeli N.

Dokaz T: $x^N - 1 = (x-1)(x^{N-1} + \dots + 1)$ UVRSTIMO ζ_N^a, $a \in \{1, \dots, N-1\}$

$\Rightarrow \zeta_N^a$ je nultočka od $x^{N-1} + x^{N-2} + \dots + 1$ $\forall a \in \{1, \dots, N-1\}$.

$\Rightarrow x^{N-1} + x^{N-2} + \dots + 1 = \prod_{a=1}^{N-1}(x - \zeta_N^a)$ UVRSTIMO $x = 1$

$$\Rightarrow N = \prod_{a=1}^{N-1} (1 - \zeta_N^a)$$

■

Neka je $\mu \mid \lambda$, μ ideal u O_K. Neka je $\sigma \in I_\lambda$

$\overset{DEF}{\Rightarrow} \zeta_N^\sigma \equiv \zeta_N \pmod{\mu} \Rightarrow \mu \mid (\zeta_N^\sigma - \zeta_N)$

Budući $\lambda \nmid N$ i $\mu \mid \lambda \Rightarrow \mu \nmid N \overset{T}{\Longrightarrow} \boxed{\zeta_N^\sigma = \zeta_N}$

$\Rightarrow \zeta_N^{\sigma} = \zeta_N = \zeta_N^{\chi_N(\sigma)} \Rightarrow \chi_N(\sigma) = 1$. (1. dio od 2)

Neka je σ_λ Frobenius. Tada je $\zeta_N^{\sigma_\lambda} \equiv \zeta_N^{N_{K/\mathbb{Q}}(\lambda)} \pmod{\mu}$

KAO I PRIJE

$$\Rightarrow \zeta_N^{\sigma_\lambda} = \zeta_N^{N_{K/\mathbb{Q}}(\lambda)} = \zeta_N^{\chi_N(\sigma_\lambda)}$$

$$\Rightarrow \chi_N(\sigma_\lambda) \equiv N_{K/\mathbb{Q}}(\lambda) \pmod{N} \quad \blacksquare.$$

Def Neka je K PAB. Kažemo da je $\rho: G_K \to GL_n(K)$ (λ/GR) NEPARNA ako $\forall$ kompleksno konjugiranje τ vrijedi $\det \rho(\tau) = -1$.

Nap. Sjetimo se $\det \rho_{E,N} = \chi_N$.

Korolar $\rho_{E,N}$ je neparna.

Dokaz. $\det \rho_{E,N}(\tau) = \chi_N(\tau) \overset{TM(1)}{=} -1 \quad \blacksquare$.

Nap. U TM(2) smo pokazali da je χ_N NERAZGRANAT u skoro svim prostim idealima λ. Ovo je TIPIČNO: uglavnom će G-reprezentacije biti nerazgranate skoro svugdje.

PROP 1) Neka je E/K el. krivulj., $P \in E(K)$, $|P| = N$. Tada je $\rho_{E,N} \sim \begin{pmatrix} 1 & * \\ 0 & \chi_N \end{pmatrix}$.

2) Neka E/K —"— ima izogeniju stupnja N nad K. Tada je $\rho_{E,N} \sim \begin{pmatrix} \phi & * \\ 0 & \psi \end{pmatrix}$, ϕ, ψ su KARAKTERI (HOMOMORFIZMI: $G_K \to (\mathbb{Z}/N\mathbb{Z})^\times$).

VRIJEDI $\phi \cdot \psi = \chi_N$

DOKAZ : dizeli iz $\det \rho_{E,N} = \chi_N$.

KVADRATNO TVISTANJE (ZAKRETANJE)

Slijedeći SILVERMANA skripta.

LEMA Neka je $d \in K^*$, pritom je K PAB, char $K \neq 2$.

Neka je E' kvadratni twist (zavoj) od E za d (E^d).

Neka je $\psi : G_K \to \{1, -1\}$ kvadratni karakter definiran sa $\sqrt{d}^\sigma = \psi(\sigma)\sqrt{d}$. Tada je $\rho_{E,N} \sim \psi \cdot \rho_{E',N}$.

Dokaz: E i E' imaju oblike:

$$E : Y^2 = X^3 + aX^2 + bX + c$$

$$E' : Y^2 = X^3 + da X^2 + d^2 b X + d^3$$

$$\phi : E(\bar{K}) \to E'(\bar{K}) \qquad \phi(x,y) = \left(\frac{x}{d}, \frac{y}{d\sqrt{d}}\right)$$

je izomorfizam Abelovih grupa.

$\Rightarrow$ Dakle imamo izomorfizam $\phi : E[N] \to E'[N]$

Neka je $P \in E[N] \setminus \{\mathcal{O}\}$, $P = (x,y)$. Pritom $-P = (x,-y)$.

Vrijedi da je $\phi(P)^\sigma = \left(\frac{x^\sigma}{d}, \frac{y^\sigma}{d(\sqrt{d})^\sigma}\right) = \left(\frac{x^\sigma}{d}, \frac{y^\sigma}{d\,\psi(\sigma)\sqrt{d}}\right)$

$$= \left(\frac{x^\sigma}{d}, \psi(\sigma)\frac{y^\sigma}{d\sqrt{d}}\right) = \psi(\sigma)\left(\frac{x^\sigma}{d}, \frac{y^\sigma}{d\sqrt{d}}\right) = \psi(\sigma)\phi(P^\sigma)$$

Neka je P, Q točka iz $E[N]$ i neka je $\phi(P), \phi(Q)$ točka iz $E'[N]$. Po onom tvrdnom vidimo da je

$$\rho_{E,N} = \psi \cdot \rho_{E',N}.$$

∎

Teorem Neka je $H \leq GL_2(\mathbb{Z}/N\mathbb{Z})$. Pretpostavimo da $\rho_{E,N}(G_K) \subseteq H$, neka je E' kvadratni twist za neki $d' \in K^*$. Ako je $-I \in H$, tada je $\rho_{E',N}(G_K)$ ~~...~~ sadržano u konjugatu od H.

Dokaz slijedi iz prošle leme.

Korolar Ako E ima ... K-izogeniju stupnja N, tada ima i neki kvadratni twist E' od E.

~~...~~ GRANANJE MOD N G.R. $\rho_{E,K}$.

TM Neka je K PAB, E/K el.kr., λ prost ideal u K, I_λ grupa inercije. ~~...~~ Neka ~~...~~ E ima dobru redukciju u λ. Tada je $\rho_{E,N}$ nerazgranata u λ.

Nap Neka E ima DR u λ. Tada ~~...~~

1) $E(K)[N] \hookrightarrow E(\mathbb{F}_\lambda)[N]$ za sve $\lambda \nmid N$ (Silverman).

2) $E(K)[\ell] \hookrightarrow E(\mathbb{F}_\lambda)[\ell]$ za $\lambda \mid \ell$, $\ell \in \mathbb{Z}$ prost ~~...~~ ako $e(\lambda/\ell) < \ell - 1$. (Katz, Appendix)

Nap u 2) je uvjet $e(\lambda/\ell) < \ell - 1$ NUŽAN, npr $E/\mathbb{Q}$ t.d. $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ DR u 2.

$E(\mathbb{Q})[2] \xrightarrow{\quad} E(\mathbb{F}_2)[2] \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \\ \{0\} \end{cases}$

$\|$

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

ne može biti injekcija!

Dokaz: Izdelamo $\mu \leq O_K$ nad λ.

$\overset{NAP}{\Rightarrow}$ Razširitev ima DR v λ $\Rightarrow$ DR v μ

$\overset{NAP}{\Rightarrow}$ red. $E[N] \hookrightarrow E(\mathbb{F}_\lambda)$ $Q \mapsto \overline{Q}$ (mod μ)

je injekcija

Naj bo $\sigma \in I_\lambda$. Tedaj $\forall Q \in E[N]$ velja: $\overline{Q^\sigma} = \overline{Q}$

po definiciji inercije $\overset{\text{injektivnost}}{\Rightarrow}$ $Q^\sigma = Q$

$\Rightarrow \rho_{E,N}(\sigma) = 1$ ∎.