dokaz Propozicija: Dokazali ćemo propoziciju tako što ćemo Θ prikazati kao kompoziciju bijekcija Θ_1 i Θ_2. Za početak ćemo relaciju $\sim_{\mathfrak{I}}$ definirati za elemente ideala L.

Za $\alpha_0, \alpha_1 \in L$ normi relativno prosti s N, definiramo

$$\alpha_0 \sim_{\mathfrak{I}} \alpha_1 \iff \alpha_0 \bar{\alpha}_1 / _{Nr(L)} \in \mathbb{Z}.$$

To je relacija ekvivalencije i vrijedi $\alpha_0 \sim_{\mathfrak{I}} \alpha_1$ ako i samo ako $\chi_L(\alpha_0) \sim_{\mathfrak{I}} \chi_L(\alpha_1)$. Zaista:

(dokaz:)

Uistinu, ako vrijedi $\mathcal{X}_L(\alpha_0) \sim_{\mathfrak{P}} \mathcal{X}_L(\alpha_1)$ onda postoji $\beta \in \mathfrak{P} \cap \mathcal{X}_L(\alpha_1)$

takav da je $\mathcal{X}_L(\alpha_0) = \mathcal{X}_L\left(\alpha_1 \frac{\overline{\beta}}{nr(\mathcal{X}_L(\alpha_1))}\right) = L \cdot \frac{\overline{\alpha_1} \cdot \overline{\beta}}{nr(L) \cdot \frac{nr(\alpha_1)}{nr(L)}} = \overline{\beta \alpha_1}$

dokažite: Lemma 1. u članku $= \mathcal{X}_L\left(\beta \alpha_1 / \frac{nr(\alpha_1)}{nr(L)}\right)$ (n_1) (kako je $\alpha_1 \in L$, $\frac{nr(\alpha_1)}{nr(L)} = n_1 \in \mathbb{Z}$)

↓ pretpostavka ✓

Slijedi $\alpha_0 = \beta \alpha_1 / n_1 \cdot \delta$ gdje $\delta \in \mathcal{O}_R(L)^\times \cong \langle \pm 1 \rangle$

što implicira $\frac{\alpha_0 \overline{\alpha_1}}{nr(L)} = \frac{\beta \alpha_1 \overline{\alpha_1}}{n_1 \cdot nr(L)} \cdot \delta = \beta \cdot \delta^{\pm 1} \in \mathfrak{P}$ ✓

Dakle, pokazali smo da je preslikavanje $\Theta_2 : L/_{\sim_3} \longrightarrow Cl_3(\mathcal{O})$

$\Theta_2(\alpha) = \chi_L(\alpha)$ bijekcija. Preostaje pokazati da je

preslikavanje $\Theta_1 : \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \to L/_{\sim_3}$, $\Theta_1((c:n)) = (c+\omega_3 n)_\gamma$

bijekcija. Prvo, uočimo da je preslikavanje dobro definirano

jer je $(c+\omega_3 n) \in \mathcal{O}_0 = \mathcal{O}_L(L)$ i $\gamma \in L$. Nadalje, Θ_1

je injektivno. Kada ne bi bilo, onda bi postojali

$\mu_1, \mu_2 \in \mathbb{Z}[\omega_3]$ t.d. $0 := \dfrac{\mu_1 \gamma\ \overline{\mu_2 \gamma}}{nr(L)} = \dfrac{\mu_1 \gamma \bar{\gamma}\, \bar{\mu_2}}{nr(L)} = \dfrac{nr(\gamma)}{nr(L)}\, \mu_1 \bar{\mu_2} \in \mathbb{Z}$

Budući da je N inertan u $\mathbb{Z}[\omega_s]$ slijedi da $(nr(\theta), N) = 1$ jer bi inače μ_1 ili μ_2 imao normu djeljivu s N što bi zbog inertnosti impliciralo da N dijeli μ_1 ili μ_2 (u $\mathbb{Z}[\omega_s]$) što nije moguće jer $\mu_i = (c_i + \omega_s d_i)\gamma$ i $(nr(\gamma), N) = 1$ (zbog $\mathcal{P}^1(\mathbb{Z}/N\mathbb{Z})$) nisu oboji djeljivi s N (jer $\bar{\omega}_s = -\omega_s$).

Budući da je $\#\mathcal{P}^1(\mathbb{Z}/N\mathbb{Z}) = N+1$, za bijektivnost je dovoljno pokazati da je $\#L/_{\sim_\Sigma} = \#Cl_\Sigma(\mathcal{C}) \leq N+1$.

Sada čemo svakoj klasi iz $Cl_D(\mathcal{O}_c)$ pridružiti jedinstveni ideal $\mathcal{O}_c$-ideal norme N (različitima klasama ji pridružen različit ideal). Kako postoji $N+1$ takav ideal (jer svaki takav ideal $M = \mathcal{O}_c\langle \alpha_M, N\rangle$ odgovara cikličkoj podgrupi reda N $E'[M] \subset E'[N]$ kojih ima $N+1$ jer $E'[N] \simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$) tvrdnja $\#Cl_D(\mathcal{O}) \leq N+1$ slijedi.

Pridruživanje Ψ ćemo ovako definirati. Neka je $[\mathcal{J}] \in Cl_{\mathcal{B}}(\mathcal{O}_\alpha)$

t.d. $\mathcal{J} = \mathcal{I}_L(\beta)$ za neki $\beta \in L$. Tada je

$$\Psi(\mathcal{J}) := \beta^{-1}[\mathcal{J}]_* I \beta \quad \text{gdje } \mathcal{O}_c\text{- ideal}$$

(Propos. 4 iz članka)

koji po Propoziciji iz prethodnog predavanja je jednak

$[L]_* I$ ako je $L \sim_{\mathcal{B}} \mathcal{J}$ (tj. ako je $\beta \in \mathcal{J}$). Malo općenitije,

ako su $\mathcal{J}_1 \sim_{\mathcal{B}} \mathcal{J}_2$ onda $\Psi(\mathcal{J}_1) = \Psi(\mathcal{J}_2)$ (po Propoziciji su

$[\mathcal{J}_1]_* I$ i $[\mathcal{J}_2]_* I$ "konjugirani" ideali nad $\mathcal{O}$ pa su $\Psi(\mathcal{J}_1)$ i

$\Psi(\mathcal{J}_2)$ jednaki jer općenito $\mathcal{I}_L(\beta_1) = \mathcal{I}_L(\beta_2) \Leftrightarrow \beta_1 = \beta_2 \cdot \delta$ gdje $\delta \in \mathcal{O}_R(I) = \mathcal{O}_c = \{\pm 1\}$

Dakle, Ψ definiran preslikavanje $Cl_{23}(C) \xrightarrow{\Psi}$ {klijan G_c - ideali norme $N = nr(I)$}

Preostaje još pokazati da je preslikavanje

injektivno. Dokazimo to koristeći Deuringovu

korespondenciju. Pretp. da je $\Psi(j_1) = \Psi(j_2)$ gdje je $j_1 := \chi_{j_2}(\beta)$

za neki $\beta \in j_2$. Želimo dokazati da je $\beta \in \mathbb{Z}$. Tada

$[\varphi_{j_1}]_* \varphi_I$ i $[\varphi_{j_2}]_* \varphi_I$ imaju jednaka jezgra, tj. $\varphi_{j_1}(E_0[I]) = \varphi_{j_2}(E_0[I])$.

Budući da su j_1 i j_2 ekvivalentni u proporciji s prošlog predavanja slijedi

da φ_{j_1} i $\varphi_{j_2} \circ \bar{\beta}$ imaju isto jezgro. Neka je P_0 generator

cikličke grupe $E_0[I] \simeq \mathbb{Z}/N\mathbb{Z}$ (N je prost).

$[\cdot]_*$ čuva norme

$\varphi_{J_1}(F_0[I]) = \varphi_{J_2}(F_0[I]) \Rightarrow \langle \varphi_{J_1}(P_0) \rangle = \langle \varphi_{J_2}(P_0) \rangle$

$\Leftarrow$ $\quad \neq 0$ jer $\quad \neq 0$

0 jer $(\min(J_1), N) = 1$

$\varphi_{J_1}(P_0) = k \cdot \varphi_{J_2}(P_0)$ za neki $k \in K[.$

$\Rightarrow \varphi_{J_2}(\bar{\beta}(P_0)) = \tilde{k}\, \varphi_{J_2}(P_0)$ za neki $\tilde{k} \in K[.$ $\Rightarrow \bar{\beta}(P_0) - \tilde{k} \cdot P_0 \in \ker J_2$

$\Rightarrow \#\ker J_2 (\bar{\beta}(P_0) - \tilde{k} P_0) = 0 \Rightarrow \bar{\beta}(MP_0) = M\tilde{k} P_0 \neq 0$ jer $(M, N) = 1.$

$\#\ker J_2 = M$

$\bar{\beta}(F_0[I]) = F_0[I]$ $\Leftarrow$ generiše ol $F_0[I]$

$\Downarrow$

Lema iz prošlog predavanja - karakterizacija Eichlerovog reda $\mathcal{O}$.

$[\mathcal{O}_0 \bar{\beta}]_* I = I \Rightarrow \bar{\beta} \in \mathcal{O}$

$\Rightarrow \beta \in \mathcal{O}$ ✓

$\simeq Cl_{\mathcal{O}}(\mathcal{O}_0)$

Propozicija: $Cl(\mathcal{O})$ je u bijekciji sa skupom N-izogenija do na izomorfizam

Dokaz: Dekuringova koresp.:

$$C \subset Cl(\mathcal{O}_0) \longleftrightarrow j(E_C)$$

$E_0/E_0[J]$ za bilo koji $J \in C$ (zato što $J_1 \sim J_2 \Rightarrow E_{J_1} \simeq E_{J_2}$ (dokazano ranije))

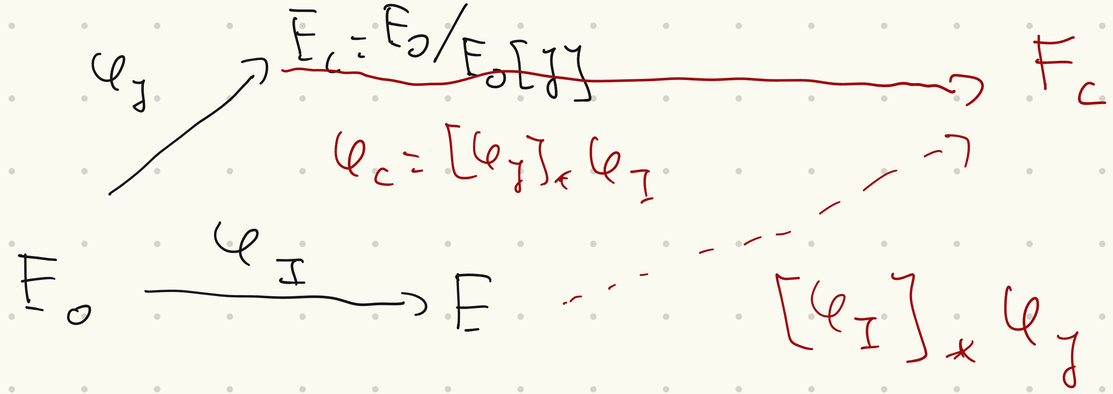
Slično, za $C \in Cl_{\mathcal{O}}(\mathcal{O}_0) \simeq Cl(\mathcal{O})$ i $J \in C$

$$C \rightsquigarrow \varphi_C : E_C \longrightarrow E_C$$ gdje je $E_C = E_0/E_0[J]$

preslikavanje Ψ iz prethodne propozicije

i $E_C = E/E[K]$ sa $K = [I]_* J$ i $\varphi_C = [\varphi_J]_* \varphi_I$ za bilokoje $J \in C$

$\deg \varphi_C = \deg \varphi_I = N$



$$\ker \varphi_c = \varphi_J(F_0[I]) \simeq F_c[[J]_* I]$$

$$\Rightarrow F_c \simeq F/\varphi_I(F_0[J]) = F/F[K]$$

- Zašto φ_c (do na izomorfizam) ovisi samo o klasi C, a ne o reprezentanti $J \in C$?

  a) F_c do na izom. ovisi samo o $C \in Cl_B(O_0)$

  b) $[J]_* I$ ne ovisi o reprezentanti $J \in C$ različiti ideali

  (vidi definiciju preslikavanja Ψ iz prošle propozicije.)

- Injektivnost presl. Ψ implicira da različitim klasama odgovaraju različiti reogmri
- Surjektivnost od Ψ implicira bijektivnost korespondencije.