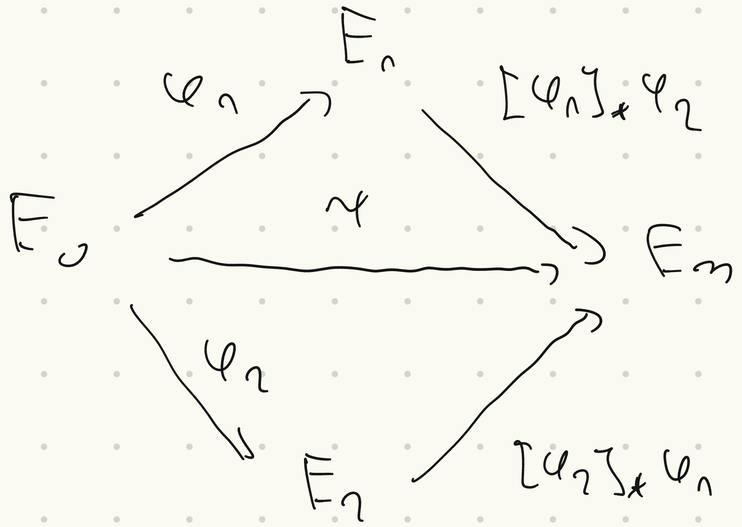
Zadnji put, za $\gcd(N_1, N_2) = 1$ $\left(N_i = \deg \varphi_i\right)$



Takodar važno:

$$[I_1]^* [I_1]_* I_2 = I_2$$

jer $\varphi_2 = [\varphi_1]^* [\varphi_1]_* \varphi_2$ (d.z.)

Po Deuringovoj korespondenciji kompoziciji izogenija odgovara produkt ideala pa npr.

"obmotati" posredak

$$\psi = [\varphi_1]_* \varphi_2 \circ \varphi_1 \quad \hookleftarrow \quad K = I_{\varphi_1} \cdot I_{[\varphi_1]_* \varphi_2}$$

$$K = I_1 \cap I_2 \qquad I_1$$

$I_1 \hookleftarrow \varphi_1$

$I_2 \hookleftarrow \varphi_2$

$K \hookleftarrow \psi$

$$I_{[\varphi_1]_* \varphi_2} = I_1 \left(I_1 \cap I_2\right)$$

Još o Eichlerovim redovima:

Na koji način $\beta \in \mathcal{O}_0 \cap \mathcal{O}$ reprezentira endomorfizam od E_1 i E_0?

Po Deuringovoj koresp.

$\theta \in \mathrm{End}(E_0) \hookrightarrow$ glavni ideal $\mathcal{O}_0\theta$

$$\mathcal{O} := \mathcal{O}_0 \cap \mathcal{O} = \mathbb{Z} + I$$

$\mathcal{O}_L(I)$ = $\mathrm{End}(E_0)$ ⤳ E_0 (glatka)

$\mathcal{O}_R(I)$ = $\mathrm{End}(E)$

$\varphi_I : E_0 \to E$

$\deg \varphi_I = [\mathcal{O} : I]$

Lema: Neka je $\beta \in \mathcal{O}_0$ norme relativno prosto s $N = \mathrm{nrd}(I)$, tada $[\mathcal{O}_0\beta] * I = I$ ako i samo ako $\beta \in \mathcal{O} \setminus (I \cup \bar{I})$. Posebno $[I]_* \mathcal{O}_0\beta$ je glavni $\mathcal{O}$-ideal jednak $\mathcal{O}\beta$.

Što ove oznake znače? Zašto je to važno? slika!

Skica dokaza: Za $\beta \in \mathcal{Y} \setminus (I \cup \bar{I})$ norma od β je relativno prosta s $nr(I)$ (zašto?) pa je $[I]_*(\mathcal{O}_0\beta) = I^{-1}(I \cap \mathcal{O}_0\beta)$

Pokažimo da je $I \cap \mathcal{O}_0\beta = I\beta$ što implicira $I^{-1}(I\beta) = \mathcal{O}\beta$

Budući da je I integralan, $I\beta \subset \mathcal{O}_0\beta$ te kako je $\beta \in \mathcal{Y} \subset \mathcal{O} = \mathcal{O}_R(I)$

$I\beta \subset I \Rightarrow I\beta \subset I \cap \mathcal{O}_0\beta$. Obratno, neka je $x \in I \cap \mathcal{O}_0\beta$.

Tada je $x = \delta\beta$ za neki $\delta \in \mathcal{O}_0$. Dovoljno je dokazati da je $\delta \in I$.

Neka je $\beta = \lambda + \alpha$ gdje je $\lambda \in \mathbb{Z}$ invertibilan modulo N (jer $\beta \notin I \cup \bar{I}$)

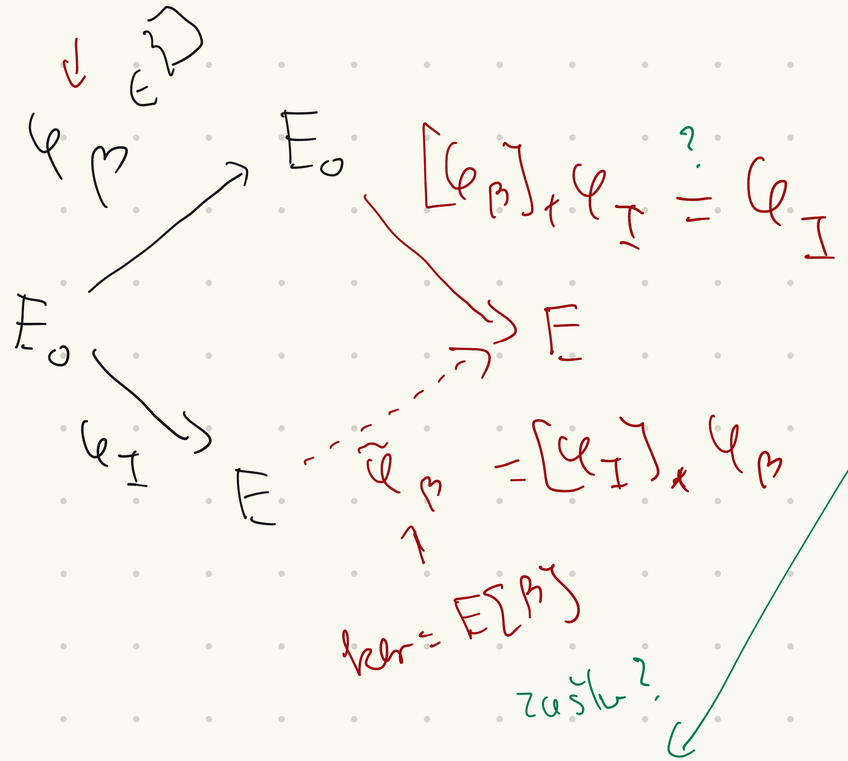
$(\mathcal{Y} = \mathbb{Z} + I)$ i $\alpha \in I$. Tada je $x = \delta\cdot\lambda + \delta\cdot\alpha \Rightarrow \lambda\delta \in I \Rightarrow \delta \in I$ jer

$\in I$ $\in I$ je λ inv. mod $nr(I)$ (zašto?)

Za drugi dio dokaza pogledajte zlumak.

za $\beta \in \Gamma$: $G_0 \cap G$

Slika:



Drugi dve dokaza: ali je

$[G_0 \beta]_* I = I$ ondo je jasno

$E_0[I]$ ali φ_I ima svojstvo $\varphi_\beta(E_0[I]) \subseteq E[I]$

↑

ciklična grupa pa β dijeli množenjem

skalarom $\lambda \in \mathbb{Z}$ očitom $\beta - \lambda$

poništimo $E_0[I] \Rightarrow \beta - \lambda \in I \Rightarrow \beta \in \mathbb{Z}I + I = I$.

$\Leftrightarrow \varphi_I$ i $[\varphi_\beta]_* \varphi_I$ imaju isto jezgro

Znamo $\ker [\varphi_\beta]_* \varphi_I = \varphi_\beta(\ker \varphi_I) = \varphi_\beta(E_0[I])$ pa tvrdnja slijedi.

Korolar* Neka su $\mathfrak{J}_1, \mathfrak{J}_2$ $\mathcal{O}_0$-ideali, $\mathfrak{J}_1 \sim \mathfrak{J}_2$ i $\gcd(nr(\mathfrak{J}_1)\, nr(\mathfrak{J}_2), nr(I)) = 1$

Prelp. $\mathfrak{J}_1 = \chi_{\mathfrak{J}_2}(\beta)$ gdje je $\beta \in \mathfrak{J}_2 \cap \mathfrak{I}$. Tada

$$[I]_* \mathfrak{J}_1 \sim [I]_* \mathfrak{J}_2 \quad \text{i} \quad [I]_* \mathfrak{J}_1 = \chi_{[I]_* \mathfrak{J}_2}(\beta).$$

preslikavanje $[I]_*$ se pomoću dobro u odnosu na relaciju $\sim$

Dokaz: Kako je $\chi_{\mathfrak{J}_2}(\beta) = \mathfrak{J}_1$ možemo identificirati $\mathfrak{J}_2 \cdot \overline{\mathfrak{J}_1}$ s $\mathcal{O}_0 \beta$.

?

što to točno znači?

Prema prethodnoj lemi $[I]_* \mathcal{O}_0 \beta = \mathcal{O}\beta$ pa i $[I]_* \mathfrak{J}_2 \cdot \overline{[I]_* \mathfrak{J}_1} = \mathcal{O}\beta$

što implicira $\chi_{[I]_* \mathfrak{J}_2}(\beta) = [I]_* \mathfrak{J}_1$.

kasnije će biti objašnjeno!

Lema: Ako je $J = I\beta \subset O$ gdje je $\beta \in R^+_{pin}$ onda $E_I \simeq E_J$

gdje su $\varphi_I : E \to E_I$ i $\varphi_J : E \to E_J$ izogenije

identificiramo $G \simeq End(E)$ pa je β onda i za izogenije

ideja: pokazat da φ_I i φ_J imaju "jednake" jezgre

Dokaz: Prekp. prvo da je $\beta \in O$. Tada

$$E[I\beta] = \{P \in E(\bar{F}_{p^r}) : \alpha\beta(P) = O \quad \forall \alpha \in I\}$$ preslika

Tvrdnja da je $\beta(E[I\beta]) = E[I]$ (i čega slijedi $\beta^{-1}(E[I]) = E[I\beta]$ što nam zbilja treba) ← jer je ker $\beta \subseteq E[I\beta]$

$\subseteq$ očito

$\supseteq$ Neka je $Q \in E[I]$. Budući je β (izogenija) surjektivna $\exists P \in E(\bar{F}_{p^r})$

t.d. $\beta(P) = Q$. Tada za sve $\alpha \in I$ $(\alpha\beta)(P) = O \Rightarrow P \in E[I\beta]$. ← Silverman

Slijedi da $\varphi_{I\beta}$ i $\varphi_I \circ \beta$ imaju jednake jezgre $\Rightarrow E_{I\beta} \simeq E_I$.

Općenito, ako je $\beta \in B_{pos} - G$ onda postoji m t.d. $\beta \cdot m \in G$

(zašto? prikaži β u bazi za G – m je najmanji zajednički višekratnik nazivnika). Tada po prethodno dokazanom $E_I \simeq E_{I(m\beta)} = E_{(I\beta)m} \simeq E_{I\beta}$

↑ zašto?

Natrag na dokaz (Činjenica *). Ako je $\gamma_1 = \gamma_2 \overline{\frac{\beta}{nr(\gamma_2)}}$ onda $\cdot\tilde{\beta}$

$$\varphi_{\gamma_1} = \varphi_{\gamma_2} \circ \tilde{\beta} \Rightarrow \hat{\varphi}_{\gamma_2} \circ \varphi_{\gamma_1} = [nr(\gamma_2)]\,\tilde{\beta} \in End(E_0)$$

vrijedi i obrat

$$\Rightarrow \frac{1}{nr(\gamma_2)} \hat{\varphi}_{\gamma_2} \circ \varphi_{\gamma_1} = \tilde{\beta} \in End(E) \qquad \ker \tilde{\beta} = E[\tilde{\beta}] = \{P \in E_0(\overline{\mathbb{F}_p}) : \tilde{\beta}(P) = 0\}$$

$$\Rightarrow \frac{1}{nr(\gamma_2)} \cdot \gamma_1 \cdot \bar{\gamma}_2 = G_0 \frac{\overline{\beta}}{nr(\gamma_2)} \quad / \cdot \text{involucija} \Rightarrow \bar{\gamma}_2 \gamma_1 = \bar{\beta} G_0 \Rightarrow \gamma_2 \bar{\gamma}_1 = \beta G_0$$

$$\gamma_1 \bar{\gamma}_2 = G_0 \beta \xrightarrow{[\,]_*} [\,]_* \gamma_1 \cdot \overline{[\,]_* \gamma_2} = [\,]_* G_0 \bar{\beta} = G \bar{\beta}$$

zašto? d.z. ⇒ TURDNJA

Lema

$\square$

Generalizirani KLPT algoritam: $\mathcal{O}, \mathcal{O}_0$ ← specijalni maksimalni redovi; povezani s I_γ, N_γ

Možemo pretpostaviti da je N_τ prost (zamijenimo I_τ s $I_\tau \beta$ ← prosti norme odnosno

$\mathcal{O} \leftarrow \beta^{-1}\mathcal{O}\beta$) i ireducibilan u R ($\mathcal{O}_0 = R + jR$, $R = \mathbb{Z}[\omega]$)

Neka je $\mathfrak{I} = \mathcal{O} \cap \mathcal{O}_0$ Eichlerov red nivoa N_τ.

Neka je dan lijevi $\mathcal{O}$-ideal I. Želimo pronaći $\alpha \in I$ norme ℓ^e. Ekvivalentno, treba pronaći $\beta \in I$ norme $n(I)\ell^e$.

Tada je $J = \chi_I(\beta)$. Mi ćemo tražiti takav β koji je

ne sadržan ni u I niti u $\mathfrak{I}$!

Korolar implicira: ako je $\beta \in I \cap \mathcal{D}$ onda je

$$[I_\gamma]^* f = \chi_{[I_\gamma]^* I}(\beta)$$

Posebno β se nalazi u $\mathcal{O}_0$-idealu $[I_\gamma]^* I$ kao i u $\mathcal{D}$, pa

ovo su $\mathcal{O}_0$-ideali

samo problem skupove svedi na standardan KLPT

algoritam. Jedina razlika je što sada element β koji tražimo mora biti u podringu $\mathcal{D}$ reda $\mathcal{O}_0$. I dalji sve računamo u specijalnom redu $\mathcal{O}_0$. Pullback preslikavanja $[I_\gamma]^*$ nam je bio važan jer preslikava $\mathcal{O}$-ideale u $\mathcal{O}_0$-ideale s kojima volimo više raditi.

Generalized KLPT$_{e^*}(I, I_\tau)$ - za dani lijevi $\mathcal{O}$-ideal I i I_τ lijevi $\mathcal{O}_0$ i desni $\mathcal{O}$ ideal norme N_τ relativno prosta s $nr(I)$ vraća $J \sim I$ norme ℓ^e.

1. izračunaj $K' = [I_\tau]^* I$ i odredi $L = \text{EquivalentPrimeIdeal}(K')$ gdje je $L = \chi_{K'}(\delta)$ za $\delta \in K'$ norme $N = nr(L)$ gdje je N prost

2. izračunaj $\gamma = \text{RepresentInteger}_{\mathcal{O}_0}(N\ell^{e_0})$ (kao u KLPT)

3. izračunaj $(C_0 : D_0) = \text{IdealModConstraint}(L, \gamma)$ (kao u KLPT)

4. nađi $(C_\tau : D_\tau) \in \mathbb{P}^1(\mathbb{Z}/N_\tau\mathbb{Z})$ t.d. $\forall j (C_\tau + uD_\tau)\delta \in \mathbb{Z} + I_\tau = \Gamma_J$

(nova, uvjet da element mora biti u Γ_J)

Kineshi teorem o ostat.

5. izračunaj $C = CRT_{N_1,N}((c_0,c_1)$ i $D = CRT_{N_1,N}(D_0,D_1)$

tako da par (C,D) zadovoljava i uvjet 3. i uvjet 4.

6. izračunaj $\mu = \text{StrongApproximation}_{e'}(NN_1, C, D)$ nome ℓ^{e_1}

7. postavi $\beta = \gamma\mu$ i $e = e_0 + e_1$ t.d. $\text{ord}(\beta) = N\ell^e$

8. vrati: $y = [I_n]_* \chi_L(\beta)$

Detaljniji o koraku 4: Za dane γ i δ norme relativno prostih s N_γ treba pronaći $\mu \in jR$ ($\mu = j(c_1 + w D_1)$) t.d. $\gamma\mu\delta \in \mathfrak{I}$.

Ovo je ekvivalentno pronalaženju β oblika $\beta = \gamma\mu$ t.d. $\beta\delta \in \mathfrak{I}$ ($\mathfrak{I}$ $\mathcal{O}_0$-ideal) što osigurava $[\mathcal{I}_\gamma]_* \mathcal{I}_L(\beta) \sim \mathcal{I}$. ($\mathcal{I}$ $\mathcal{O}$-ideal) Zato nas zanima preslikavanje

$$(C:D) \longmapsto \left[\mathcal{I}_L(\gamma(C + Dw))\right] \quad \text{(klasa ekvivalencije u } Cl(\mathcal{O}))$$

$$\mathbb{P}^1(\mathbb{Z}/N_\gamma\mathbb{Z}) \longrightarrow Cl(\mathcal{O})$$

q ↗ → ovo će kasnije biti jasnije

zašto $\mathfrak{I}$, a ne $\mathcal{O}_0$? vidjet ćemo.

Još malo teorije... $\mathfrak{I}R$... klase ideala

$\mathcal{O}_0$ je specijalni red; $R = \mathbb{Z}[w]$; $R = R_j \subset \mathcal{O}_0$; $j^2 = -p$ ← pretpostavka.

$\mathcal{I}$ ideal koji povezuje $\mathcal{O}_0$ i $\mathcal{O}$; $n(\mathcal{I}) = N$ prost

$\mathfrak{I} = \mathcal{O}_0 \cap \mathcal{O}$; $Cl(\mathcal{O}) =$ klase lijevih $\mathfrak{I}$-ideala.

$h(\mathcal{T}) = |Cl(\mathcal{T})|$. Eichler je dokazao

$$h(\mathcal{T}) = \frac{(p+1)(N+1)}{12} + \varepsilon_{N,p}$$

« mali broj koji ovisi o N i p mod 12

S druge strane $h(\mathcal{O}_0) = \frac{p}{12} + \varepsilon_p$ « ovisi o p mod 12

što sugerira da postoji $(N+1) : 1$ korespodencija između $Cl(\mathcal{T})$ i $Cl(\mathcal{O}_0)$ koja čuva sada opisuti.

Napomena: Slično vrijedi općenito između $Cl(\mathcal{O})$ i $Cl(\mathcal{T})$.

Označimo sa $I_N(\mathcal{O})$ skup ključnih ajdla $\mathcal{O}$-ideala norme relativno proste s N za bilo koji red $\mathcal{O}$.

Lema: Preslikavanje $\eta: I_N(\mathcal{O}_0) \to I_N(\mathcal{I})$

$$J \mapsto J \cap \mathcal{I}$$ je dobro definirana

bijekcija između skupa ajdla $\mathcal{O}_0$- ideala i $\mathcal{I}$- ideala norme relativno proste s N. Inverz je dan s $J \mapsto \mathcal{O}_0 J$.

Također η čuva norman.

Skica dokaza: Pokažimo $I = \mathcal{O}_0(I \cap \mathbb{Z})$ za svaki $I \in \mathcal{I}_N(\mathcal{O}_0)$.

Tvrdnja: Svaki $I \in \mathcal{I}_M(\mathcal{O}_0)$ se može zapisati kao $\mathcal{O}_0\langle \alpha, nr(I)\rangle = \mathcal{O}_0\alpha + \mathcal{O}_0 nr(I)$ za neki $\alpha \in \mathbb{Z}$.

generatori od I su i iz $\mathbb{Z}$

Tada je $I \cap \mathbb{Z} = \mathbb{Z}\langle \alpha, nr(I)\rangle$ i $\mathcal{O}_0\mathbb{Z}\langle \alpha, nr(I)\rangle = I$.

↳ znamo, općenito $I = \mathcal{O}_0\langle \xi, nr(I)\rangle$ za neki $\xi \in \mathcal{O}_0$.

Kako je $\gcd(nr(I), N) = 1$ onda postoji $\alpha \in \mathbb{Z}$ t.d. $\xi \equiv \alpha \pmod{nr(I)}$

pa je $\mathcal{O}_0\langle \xi, nr(I)\rangle = \mathcal{O}_0\langle \alpha, nr(I)\rangle$.

zašto? svaki $\xi \in \mathcal{O}_0$ se može u obliku $\alpha + \gamma$ pri čemu je $\alpha \in \mathbb{Z}$ prirodni s svojstvom koji kao nazivnik ima 1 ili N. Ti nazivnici modulo $nr(I)$ zbog $\gcd(nr(I), N) = 1$ nestanu.

$N\xi \in \mathbb{Z}$. Kako je $N \cdot M = n(\mathcal{O}_0)$ onda $M\xi \in \mathbb{Z} \Rightarrow \xi + k \cdot nr(I) = \alpha \in \mathbb{Z} \Rightarrow \xi \equiv \alpha \pmod{nr(I)}$

Def. Kažemo $f \sim_{\mathfrak{I}} K$ za $f, K \in I_M(0_0)$ ako i samo ako

$\varphi(f) \sim \varphi(K)$ kao $\mathfrak{I}$ - ideali. To je relacija

ekvivalencija čije klase označavamo s $\mathcal{O}_{\mathfrak{I}}(0_0)$.

Iz definicije preslikavanja φ vidimo da je $\mathcal{O}_{\mathfrak{I}}(0_0)$ u

bijekciji s $\mathcal{O}(\mathfrak{I})$

Propozicija: $f \sim_D K$ akko i samo akko postoji $\beta \in \Sigma$ t.d. $K = \chi_f(\beta)$. Tada je $\beta^{-1}[K]_* \mathcal{I} \beta = [f]_* \mathcal{I}$.

Skica dokaza: $\Rightarrow$ $f \sim_D K \Rightarrow \exists \beta \in K \cap \Sigma$ t.d. $f \cap \Sigma = \chi_{K \cap \Sigma}(\beta)$

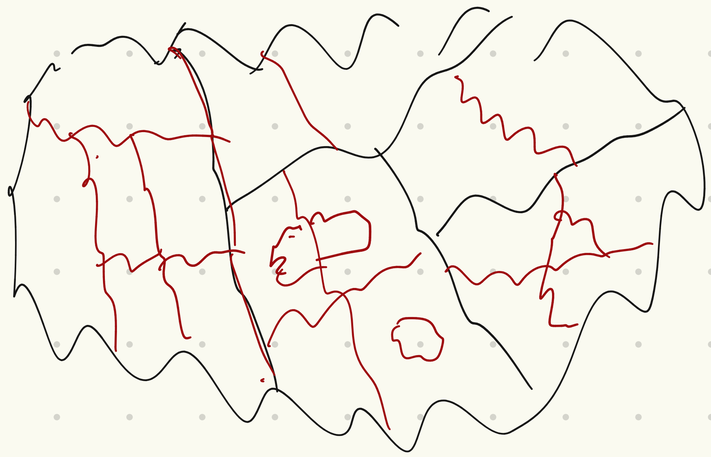
$$\Rightarrow f = \sigma_0(f \cap \Sigma) = \sigma_0 \chi_{K \cap \Sigma}(\beta) = \sigma_0(K \cap \Sigma) \cdot \frac{\overline{\beta}}{nr(K \cap \Sigma)} = K \cdot \frac{\overline{\beta}}{nr(K \cap \Sigma)}$$

$= \chi_K(\beta)$ jer β čuva norme pa i $nr(K \cap \Sigma) = nr(K)$.

↑ zašto?

S druge strane, $\beta^{-1}[K]_* \mathcal{I} \beta = \ldots$

Primijetimo da $J \sim_{\mathcal{B}} K$ implicira $J \sim K$ (prema skici dokazu prethodne propozicije) takve da vrijedi činjenica skupova klasa možemo ovako vizualizirati - svaka klasa iz $Cl(G_0)$ je unija nekih klasa iz $Cl_{\mathcal{B}}(G_0)$ pa pišemo



$$Cl_{\mathcal{B}}(G_0) = \bigcup_{C \in Cl(G_0)} Cl_{\mathcal{B}}(C)$$

↑ skup klasa iz $Cl_{\mathcal{B}}(G_0)$ koji su sadržani u klasi C

Očekujemo da svaka klasa C sadrži $N+1$ klasu ideala $Cl_D(\mathcal{O}_0) \simeq Cl(\mathcal{O})$.

Propozicija ⊙: Za $C \in Cl(\mathcal{O}_0)$ odaberemo $L \in C$ i definiramo $\mathcal{O}_C := \mathcal{O}_R(L)$. Ako je $\mathcal{O}_C^* = \langle \pm 1 \rangle$, tada za svaki $\gamma \in L \setminus N\mathcal{O}_C$ i kvadratni red $S = \mathbb{Z}[\omega_S]$ diskriminante Δ_S unutar $\mathcal{O}_0$ u kojem je N *čudesan* je preslikavanje

$$\Theta : \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \longrightarrow Cl_D(\mathcal{O})$$

$$(C:D) \longmapsto \chi_L((C + \omega_S D)\gamma)$$

bijekcija. Posebno $|Cl_D(\mathcal{O})| = N+1$.

Prvi dokaza vratimo se na korak 4 generalizacije KLPT algoritma.

$$I \rightsquigarrow K' = [I_\gamma]^* I \sim L = \chi_{K'}(\delta) \,;\ \delta \in K' \,;\ nr\,\delta = N \text{ prost}$$

↑ lijevi $\mathcal{O}$-ideal ↑ lijevi $\mathcal{O}_2$-ideal ↑ isti korak kao i u KLPT algoritmu.

Kao i u KLPT, pronaćemo $\beta = \gamma\mu$; $nr(\beta) = N\ell^e$; $\beta \in L$.

pa je $\chi_L(\beta) \sim L$ tražene norme. Ali da bi dobili analogan rezultat

za $\mathcal{O}$-ideale primijenimo $[I_\gamma]_* \chi_L(\beta) = [I_\gamma]_* \chi_{K'}(\beta\delta) \sim [I_\gamma]_* K'$

$= [I_\gamma]_* [I_\gamma]^* I$

$= I$

prema Kordumu * to će biti tako ako je $\beta\delta \in I_\gamma$.

→ želimo ovaj zaključak.

Kako osigurati $\beta_\sigma \in \mathfrak{Z}^2$? Pa $\beta_\sigma \in \mathfrak{Z}$ ako i samo ako

$$\chi_{K'}(\beta_\sigma) \sim_{\mathfrak{Z}} K'$$ odnosno

$$\chi_L(\beta) \sim_{\mathfrak{Z}} K'$$. Kako je $\beta = \gamma\mu$ i $\mu = j(\zeta + w D)$

to će vrijediti ako je $\chi_L(\gamma j(C_n + w D_n)) \sim_{\mathfrak{Z}} K'$ gdje je

$C \equiv C_n \pmod{N_n}$ i $D \equiv C_n \pmod{N_n}$. Prema (analogonu) Propoziciji ⊙

↘ kvarci redoslijed.

takvi $(C_n : D_n) \in \mathbb{P}^1(\mathbb{Z}/N_n\mathbb{Z})$ će uvijek postojati!

(No u članku nije opisan algoritam za pronalaženje takvih $(C_n : D_n)$.)