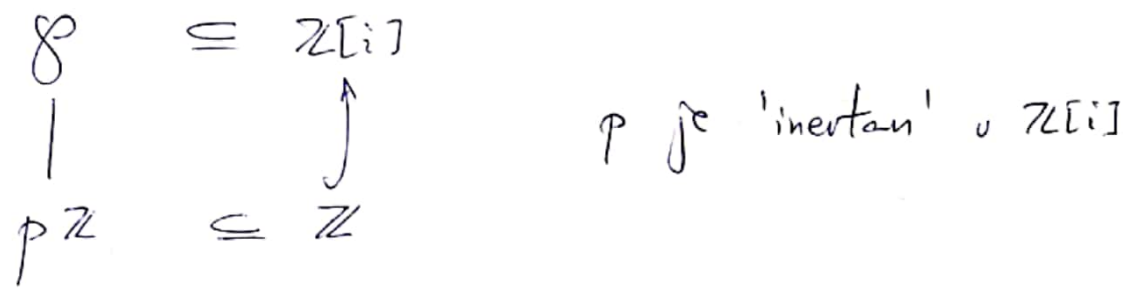


Ideali u prstenu Gausovih celih $\mathbb{Z}[i]$

Prosti ideali u $\mathbb{Z}[i]$ su oblika:

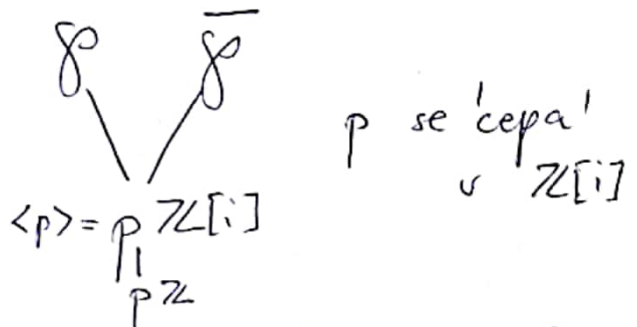
- $\mathfrak{p} = \langle p \rangle = p \cdot \mathbb{Z}[i] = \{p(c+di) \mid c+di \in \mathbb{Z}[i]\}$ za $p \equiv 3 \pmod{4}$



- $\mathfrak{p} = \langle a+bi \rangle = \{(a+bi)(c+di) \mid c+di \in \mathbb{Z}[i]\}$ za $a^2+b^2=p \equiv 1 \pmod{4}$

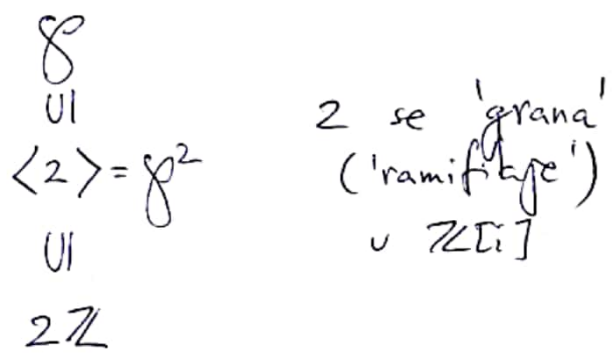
$\overline{\mathfrak{p}} = \langle a-bi \rangle$

$\langle p \rangle = p \cdot \mathbb{Z}[i] = \mathfrak{p} \cdot \overline{\mathfrak{p}}$



- $\mathfrak{p} = \langle 1+i \rangle = \{(1+i)(c+di) \mid c+di \in \mathbb{Z}[i]\} = \{c_1+di_1 \mid c_1 \equiv d_1 \pmod{2}\}$

$\langle 2 \rangle = 2 \cdot \mathbb{Z}[i] = \mathfrak{p}^2$



(Ideal $\mathfrak{p}$ u prstenu R je prost ako je $\mathfrak{p} \subsetneq R$ i ako kad god $r_1 r_2 \in \mathfrak{p}$, onda $r_1 \in \mathfrak{p}$ ili $r_2 \in \mathfrak{p}$)

• Prsteni celih algebarskih brojeva su Dedekindovi domeni (knjiga TB, Tvrdjenje 9.5, odnosno Teorema 8.38 + sekcija 6.5)

U Dedekindovim domenima su svi nenula prosti ideali:
 : maksimalni (obrnuto, svi maksimalni su nek prosti, Alg 2)

Zato je za svaki prost ideal $\mathfrak{p} \subseteq \mathbb{Z}[i]$
 $\mathbb{Z}[i]/\mathfrak{p}$ jedno polje (konačno! - dobivate direktno)

$$\begin{aligned} \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} &\hookrightarrow \mathbb{Z}[i]/\mathfrak{p} && \text{stopene polja} \\ n+p\mathbb{Z} &\longmapsto n+\mathfrak{p} && (\text{tj. } \mathbb{Z}[i]/\mathfrak{p} \text{ je raširenje polja } \mathbb{F}_p) \end{aligned}$$

② Ako je $\mathfrak{p}$ prost ideal potena $\mathbb{Z}[i]$ koji 'leži iznad' $p\mathbb{Z}$ (tj. $\mathfrak{p} \supseteq p \cdot \mathbb{Z}[i] \Leftrightarrow \mathfrak{p} | \langle p \rangle = p \cdot \mathbb{Z}[i]$) ^{za deljivost ideala videti: (TB, T. 6.45)}
 onda definišemo stepen ideala $\mathfrak{p}$ sa

$$\deg \mathfrak{p} := [\mathbb{Z}[i]/\mathfrak{p} : \mathbb{F}_p] - \text{stepen raširenja polja}$$

$$(\quad = f(\mathfrak{p} | p\mathbb{Z}) = \text{stepen inercije ideala } \mathfrak{p} \text{ nad idealom } p\mathbb{Z})$$

(TB. sekaja 10.1 i videti npr. Tvđenje 10.10)

Primer. Ako je $p \equiv 3 \pmod{4}$ i $\mathfrak{p} = \langle p \rangle$ onda je

$$\deg \mathfrak{p} = f(\mathfrak{p} | p\mathbb{Z}) = 2$$

$$\Leftrightarrow \mathbb{Z}[i]/\mathfrak{p} \cong \mathbb{F}_{p^2}$$

• Ako je $p \equiv 1 \pmod{4}$ i $\mathfrak{p} = \langle a+bi \rangle$, $a^2+b^2=p$,

$$\deg \mathfrak{p} = 1$$

- 2 -

Dokazali smo da je $z \in p \nmid 2n$

$$(1-T)(1-pT) Z(E_n/\mathbb{F}_p; T) = (1-\alpha T)(1-\bar{\alpha} T) = (*)$$

gde je $\alpha = \alpha_f = i\sqrt{p}$ ako je $p \equiv 3(4)$

$\alpha = \alpha_f = a+bi \equiv \left(\frac{n}{p}\right) \pmod{2+2i}$ ako je $a^2+b^2=p \equiv 1(4)$

$\alpha_f = 0$ ako $f \mid 2n\mathbb{Z}[i]$ tj. $p \mid 2n$
(videti 5. domaći)

(*) možemo uniformno zapisati kao

$$(*) = \prod_{f \mid \langle p \rangle} \left(1 - (\alpha_f T)^{\deg f} \right)$$

$$= \begin{cases} 1 - \alpha_f^2 T^2, & p \equiv 3(4) \\ (1 - \alpha_f T)(1 - \bar{\alpha}_f T), & p \equiv 1(4) \end{cases}$$

(u 2. slučaju α_f je jedinstven generator ideala f kongruentan $\left(\frac{n}{p}\right) \pmod{2+2i}$; isto važi i za ideal $\bar{f}$)

② Za svaki nenula ideal α prstena $\mathbb{Z}[i]$ definišemo njegovu normu sa

$$N(\alpha) := [\mathbb{Z}[i] : \alpha] = \text{indeks Abelovih grupa}$$

(TB, Posledica 8.36)

Može se pokazati da je svaki α ranga 2 tj. izomorfan sa $\mathbb{Z}^2$
pa iz Alg 1 znamo da je $[\mathbb{Z}[i] : \alpha] < \infty$

• Ako je ideal $\alpha = \langle \alpha \rangle$ glavi (u $\mathbb{Z}[i]$ su svi glavi)
onda je

$$N(\alpha) = N(\langle \alpha \rangle) = |N(\alpha)| = \left| \prod_{\sigma \in \text{Gal}} \sigma(\alpha) \right| \quad \text{TB, Teorema 9.20}$$

• Norma ideala je multiplikativna

$$N(\alpha \cdot b) = N(\alpha) N(b)$$

TB, Teorema 9.21

• Za proste ideale $\mathfrak{p} \subseteq \mathbb{Z}[i]$ je

$$N(\mathfrak{p}) = [\mathbb{Z}[i] : \mathfrak{p}] = |\mathbb{Z}[i]/\mathfrak{p}| = p^{\deg \mathfrak{p}}$$

$\uparrow$
index
Ab. grupe

$\uparrow$
kardinalnost
polja

(TB, vrh str. 233)

$$(1-T)(1-pT) Z(E_n/\mathbb{F}_p; T) = \prod_{\mathfrak{p} | \langle p \rangle} (1 - (\alpha_{\mathfrak{p}} T)^{\deg \mathfrak{p}})$$

Smena promenljivih: $T = p^{-s}$, $s \in \mathbb{C}$

$$(1-p^{-s})(1-p^{-(s-1)}) Z(E_n/\mathbb{F}_p; p^{-s}) \quad (1)$$

$$= 1 - 2 a_{E_n, p} p^{-s} + p^{1-2s} = \prod_{\mathfrak{p} | \langle p \rangle} \left(1 - \frac{\alpha_{\mathfrak{p}}^{\deg \mathfrak{p}}}{N(\mathfrak{p})^s} \right)$$

setite se: $\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}}$, (za $\Re s > 1$)

Kad pomnožimo (1) sa sv praste brojeve p i uzmemo recipročnu vrednost (još ne diskutujemo konvergenciju !):

$$\frac{\zeta(s) \zeta(s-1)}{\prod_p Z(E_n/\mathbb{F}_p; p^{-s})} = \prod_{p \nmid 2n} \frac{1}{1 - 2a_{E_n, p} p^{-s} + p^{1-2s}}$$

proizvod po
svim prastim elementima
(idealama) $p \in \mathbb{Z}$

$$= \prod_{\mathfrak{p} \nmid 2n} \frac{1}{1 - \frac{\alpha_{\mathfrak{p}}^{\deg \mathfrak{p}}}{(N\mathfrak{p})^s}} \stackrel{\textcircled{2}}{=} L(E_n, s) \quad (2)$$

proizvod po svim
prastim idealima $\in \mathbb{Z}[i]$

$$(\mathfrak{p} \nmid 2n \Leftrightarrow \mathfrak{p} \nmid \langle 2n \rangle \Leftrightarrow \mathfrak{p} \neq \langle 2n \rangle)$$

Hasse-Weil-ova
L-funkcija
priključena eliptičkoj
krivoj E_n

Kao što je

$$\zeta(s) = \underbrace{\prod_p \frac{1}{1 - \frac{1}{p^s}}}_{\text{Euler-ov proizvod}} = \underbrace{\sum_{m \geq 1} \frac{1}{m^s}}_{\text{Dirichlet-ov red}}$$

tako: Euler-ov proizvod iz definicije (2) možemo raspisati u Dirichlet-ov red:

$$L(E_n, s) = \prod_{\mathfrak{p} \nmid 2n} \frac{1}{1 - \frac{\alpha_{\mathfrak{p}}^{\deg \mathfrak{p}}}{(N\mathfrak{p})^s}} = \sum_{m \geq 1} \frac{b_m(E_n)}{m^s} ,$$

za neke kompleksne koeficijente $b_m(E_n) =: b_{m,n}$

konistićemo
ovu bravu oznaku

Primer: $E_1: y^2 = x^3 - x$

- ako $p \equiv 3(4)$, onda je $a_{E_1,p} = 0$

- ako $p \equiv 1(4)$, onda je $a_{E_1,p} = a$

(ili $2a = p + 1 - N_1$, $N_1 = \text{broj tačaka na } E_1/\mathbb{F}_p$)

$$\boxed{\begin{array}{l} a^2 + b^2 = p \\ a + bi \equiv 1 \pmod{2+2i} \end{array}}$$

Prvih nekoliko faktora Euler-ovog proizvoda
i prvih nekoliko sabiraka Dirichlet-ovog reda su:

$$L(E_1, s) = \frac{1}{1 + \frac{3}{9^s}} \cdot \frac{1}{1 + \frac{2}{5^s} + \frac{5}{25^s}} \cdot \frac{1}{1 + \frac{7}{49^s}} \cdot \frac{1}{1 + \frac{11}{121^s}} \\ \cdot \frac{1}{1 - \frac{6}{13^s} + \frac{13}{169^s}} \cdot \frac{1}{1 - \frac{2}{17^s} + \frac{17}{289^s}} \cdot \dots$$

$$= 1 - \frac{2}{5^s} - \frac{3}{9^s} + \frac{6}{13^s} + \frac{2}{17^s} + \sum_{m \geq 25} \frac{b_{m,1}}{m^s}$$

• Eksplisitno

$$b_m(E_n) = \sum_{\substack{\mathfrak{a} \leq \mathbb{Z}[i] \\ N(\mathfrak{a}) = m}} \alpha_{\mathfrak{p}_1}^{e_1 \deg \mathfrak{p}_1} \cdot \alpha_{\mathfrak{p}_2}^{e_2 \deg \mathfrak{p}_2} \cdot \dots \cdot \alpha_{\mathfrak{p}_r}^{e_r \deg \mathfrak{p}_r}$$

$$N(\mathfrak{a}) = m$$

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \dots \mathfrak{p}_r^{e_r}$$

(svaki ideal se
rastavlja na proizvod
prostih - T. 6.45)

Ideja: ako nađemo multiplikativnu funkciju $\tilde{\chi}_n$ na idealima prstena $\mathbb{Z}[i]$ koja zadovoljava

$$\tilde{\chi}_n(a \cdot b) = \tilde{\chi}_n(a) \cdot \tilde{\chi}_n(b)$$

i

$$\tilde{\chi}_n(\mathfrak{p}) = \alpha_{\mathfrak{p}}^{\deg \mathfrak{p}} \quad \text{na prostim idealima } \mathfrak{p} \nmid 2n$$

onda je

$$L(E_n, s) = \prod_{\mathfrak{p} \nmid 2n} \frac{1}{1 - \frac{\tilde{\chi}_n(\mathfrak{p})}{(N\mathfrak{p})^s}}$$

$$= \prod_{\mathfrak{p} \nmid 2n} \left(1 + \frac{\tilde{\chi}_n(\mathfrak{p})}{(N\mathfrak{p})^s} + \frac{\tilde{\chi}_n(\mathfrak{p}^2)}{(N\mathfrak{p})^{2s}} + \frac{\tilde{\chi}_n(\mathfrak{p}^3)}{(N\mathfrak{p})^{3s}} + \dots \right)$$

$$= \sum_{0 \neq a \in \mathbb{Z}[i]} \frac{\tilde{\chi}_n(a)}{(Na)^s} \quad (3)$$

- Dirichletov red po svim nenula idealima prstena $\mathbb{Z}[i]$

(zbog multiplikativnosti norme je

$$N(a) = N(\mathfrak{p}_1)^{e_1} N(\mathfrak{p}_2)^{e_2} \dots N(\mathfrak{p}_r)^{e_r}$$

$\parallel$
 $\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$

Ovde je kompleksna aps. vrednost za $\frac{\wp}{p\mathbb{Z}}$

$$|\tilde{\chi}_n(\wp)| = |\alpha_{\wp}|^{\deg \wp} = \sqrt{p}^{\deg \wp} = p^{\frac{1}{2} \deg \wp} = (N \wp)^{\frac{1}{2}}$$

pa ove vrednosti više nisu na jedinичnom krugu.

- Nulta vrednosti Dirihleovih karaktera na $\mathbb{Z}$ su na jedinичnom krugu, pa funkcija $\tilde{\chi}_n$ koji tražimo ne može biti (analog)

Dirihleov karakter na $\mathbb{Z}[i]$.

- Ovakvo uopštenje Dirihleovih karaktera na prstenima celih brojeva polja je dao E. Hecke i zovu se Hecke-ovi Gröpencharakter-i

- Dakle cilj je da konstruišemo (prepoznamo) Hecke-ov karakter $\tilde{\chi}_n$ za koji je

$$\tilde{\chi}_n(\wp) = \alpha_{\wp}^{\deg \wp}$$

- Hecke je dokazao analitičko proširenje i funkcionalnu jednačinu za rektore (3) pridružene Heckeovim Gröpencharakterima, pa će odatle slediti i svojstva za Hasse-Weil-ov L-fn $L(E_n, s)$!

Dakle, suština i ideja dokaza u jednoj rečenici je da ćemo (CM) eliptičkim krivama $E_n/\mathbb{Q}$ pridružiti Heckeove Gröpencharaktere $\tilde{\chi}_n/\mathbb{Q}(i)$:

"pridruživanje" = imamo iste L-fce:

$$\boxed{L(E_n, s) = L(\tilde{\chi}_n, s)}$$

↑
a analitička svojstva ovih znamo!

• Heckeov Gröpencharakter $\tilde{\chi}_n$ možemo videti (opet je) kao automorfnu formu na $GL_1(\mathbb{A}_{\mathbb{Q}(i)})$, pa je tu svega korespondencija (primer Langlands-ovih korespondencija) eliptička kriva $\longleftrightarrow$ automorfna forma.

• Ako E nije CM-kriva, Wiles-Taylor su dokazali da $\exists$ neka modularna forma f takve 2. vrste da je

$$\boxed{L(E, s) = L(f, s)}$$

a modularne forme su primeri automorfnih formi na $GL_2(\mathbb{A}_{\mathbb{Q}})$ (klasične)