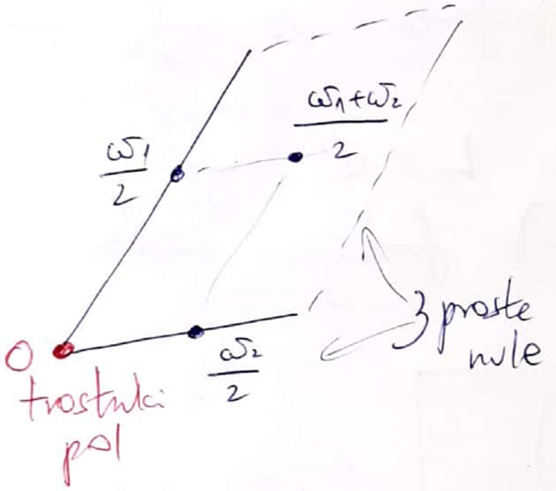
Eliptičke krive u Weierstrass-ovom obliku

1

$$\wp'(z) = -2\sum_{\ell\in L}\frac{1}{(z-\ell)^3} = -\frac{2}{z^3} - 2\underbrace{\sum_{\ell\in L\setminus\{0\}}\frac{1}{(z-\ell)^3}}_{\text{apsolutno konvergira}}$$

pa $\wp'(z)$ ima trostruki pol (=reda 3) u $z=0$ i tri proste nule u Π' (nema drugih zbog L3) u točkama $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$, $\frac{\omega_1+\omega_2}{2}$:



- Eliptička funkcija $\wp'(z)^2$ je parna, $\in \mathcal{E}_L^+$, pa je prema T6 jednaka nekoj racionalnoj fji po $\wp(z)$.
- Ali dokaz T6 je konstruktivan, i kako $\wp'(z)^2$ ima 3 ~~proste~~ dvostruke nule u $(\Pi'\setminus\{0\})\cap\frac{1}{2}L$ i nema polova u ..., slijedi da je $a_1 = \frac{\omega_1}{2}$, $a_2 = \frac{\omega_2}{2}$, $a_3 = \frac{\omega_1+\omega_2}{2}$, a b_j-ova nema, tj. fja $g(z)$ je polinom po $\wp(z)$.
- Kako $\wp'(z)^2$ ima u 0 pol reda 6, jasno je da je taj polinom kubni.

• Dakle, kao direktnu posledicu (T6) dobijamo da $\exists C \in \mathbb{C}$ takvo da je

$$\wp'(z)^2 = C\left(\wp(z) - \wp\left(\tfrac{\omega_1}{2}\right)\right)\left(\wp(z) - \wp\left(\tfrac{\omega_2}{2}\right)\right)\left(\wp(z) - \wp\left(\tfrac{\omega_1+\omega_2}{2}\right)\right)$$
$$= C\left(\wp(z) - e_1\right)\left(\wp(z) - e_2\right)\left(\wp(z) - e_3\right)$$

• Kako je $\wp'(z) = -\frac{2}{z^3} + \dots$, a $\wp(z) = \frac{1}{z^2} + \dots$ u okolini nule, poredeći koeficijente uz $\frac{1}{z^6}$ $\rightarrow C = 4$

Posledica 8 Za svaku rešetku $L \leq \mathbb{C}$ njena Weierstrass-ova $\wp(z) = \wp(z; L)$ funkcija zadovoljava diferencijalnu jednačinu

$$\boxed{\wp'(z)^2 = f(\wp(z))}$$

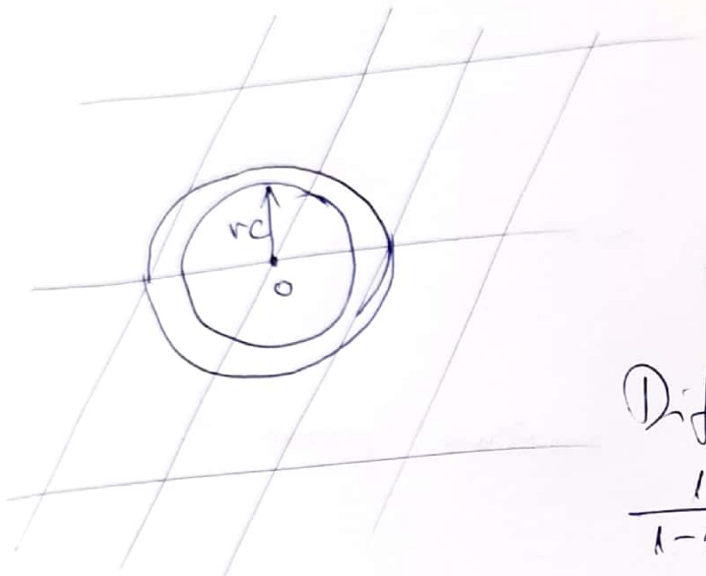
gde je $\boxed{f(x) = 4(x-e_1)(x-e_2)(x-e_3)} \in \mathbb{C}[x]$ kubni polinom sa 3 različita korena.

[2] Isti zaključak – eksplicitnim računom:

$$\wp'(z)^2 = \underbrace{\frac{4}{z^6} + \frac{b_{-4}}{z^4} + \frac{b_{-2}}{z^2}} + b_0 + b_2 z^2 + \dots$$

Ideja je da nađemo kubni polinom $f(x) = ax^3 + bx^2 + cx$ tako da $f(\wp(z))$ ima isti "polarni deo" kao $\wp'(z)^2$.

Onda će se u razlici $\wp'(z)^2 - f(\wp(z))$ tj polarni deo "pokratiti" tj. ova razlika će biti holomorfna u $z=0$. Kako $\wp(z)$ i $\wp'(z)$ nemaju polove van tačaka rešetke, ova razlika nigde neće imati pol, pa je prema (L.1), jednaka nekoj konstanti $d \in \mathbb{C}$.



$c = \min\{|\ell| : \ell \in L \setminus \{0\}\}$

$r < 1$

$z \in \Delta(0, rc)$

Diferenciranjem geometrijskog reda

$$\frac{1}{1-x} = 1 + x + x^2 + \dots$$

(stavimo $x = \frac{z}{\ell}$, $|x| \leq \frac{|z|}{|\ell|} < \frac{rc}{c} = r < 1$):
za $\ell \neq 0$

$$\frac{1}{\left(1-\frac{z}{\ell}\right)^2} = 1 + 2\frac{z}{\ell} + 3\frac{z^2}{\ell^2} + 4\frac{z^3}{\ell^3} + \dots$$

pa je

$$\wp(z) = \frac{1}{z^2} + \sum_{\ell \in L \setminus \{0\}} \left(\frac{1}{(z-\ell)^2} - \frac{1}{\ell^2} \right) \qquad (3)$$

$$= \frac{1}{z^2} + \sum_{\ell \in L \setminus \{0\}} \left(\frac{2}{\ell^3} z + \frac{3}{\ell^4} z^2 + \frac{4}{\ell^5} z^3 + \dots + \frac{k-1}{\ell^k} z^{k-2} + \dots \right)$$

Ovaj dvostruki red konvergira apsolutno u disku $|z| < rc$:

za fiksirano $\ell \in L \setminus \{0\}$ apsolutna vrednost unutrašnje sume je ograničena sa

$$\frac{2|z|}{|\ell|^3}\left(1+\frac{3}{2}\left|\frac{z}{\ell}\right|+\frac{4}{2}\left|\frac{z}{\ell}\right|^2+\frac{5}{2}\left|\frac{z}{\ell}\right|^3+\dots\right)$$

$$< \frac{2|z|}{|\ell|^3}\left(1+\frac{3}{2}r+\frac{4}{2}r^2+\frac{5}{2}r^3+\dots\right)$$

$$< \frac{2|z|}{(1-r)^2}\frac{1}{|\ell|^3}$$

a znamo da red $\sum_{\ell \in L\setminus\{0\}} \frac{1}{|\ell|^3} < \infty$.

- Zbog apsolutne konvergencije možemo promeniti redosled sumacije u (3):

(4)

$$\boxed{\wp(z) = \frac{1}{z^2} + 3G_4 \cdot z^2 + 5G_6 z^4 + 7G_8 z^6 + \dots}$$

gde je za se $k > 2$ označeno

$$G_k := G_k(L) = G_k(\omega_1, \omega_2) := \sum_{\ell \in L\setminus\{0\}} \frac{1}{\ell^k} = \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{1}{(m\omega_1+n\omega_2)^k}$$

Za neparne k je $G_k = 0$, jer se $\frac{1}{\ell^k}$ i $\frac{1}{(-\ell)^k}$ potrate (L je grupa!), a to se i slaže jer znamo da je $\wp(z)$ parna f-ja.

Diferencirajući (4) direktno dobijamo (da u istom disku važi)

$$\wp'(z) = -\frac{2}{z^3} + 6G_4 z + 20 G_6 z^3 + 42 G_8 z^5 + \dots$$

pa dalje

$$\wp'(z)^2 = \frac{4}{z^6} - 24 G_4 \frac{1}{z^2} - 80 G_6 + (36 G_4^2 - 168 G_8) z^2 + \dots$$

$$\wp(z)^2 = \frac{1}{z^4} + 6 G_4 + 10 G_6 z^2 + \dots$$

$$\wp(z)^3 = \frac{1}{z^6} + 9 G_4 \frac{1}{z^2} + 15 G_6 + (21 G_8 + 27 G_4^2) z^2 + \dots$$

Tražimo nepoznate $a, b, c, d \in \mathbb{C}$ t.d.

$$\wp'(z)^2 = a \cdot \wp(z)^3 + b \wp(z)^2 + c \cdot \wp(z) + d$$

Izjednačavanjem koef. uz $\frac{1}{z^6}, \frac{1}{z^4}, \frac{1}{z^2}$ i 1 dobijamo:

$$a = 4, \quad b = 0, \quad c = -60 G_4, \quad d = -140 G_6$$

- Tradicionalne oznake:

$$g_2 = g_2(L) := 60 G_4 = 60 \sum_{l \in L \setminus \{0\}} \frac{1}{l^4}$$

$$g_3 = g_3(L) := 140 G_6 = 140 \sum_{l \in L \setminus \{0\}} \frac{1}{l^6}$$

Posledica 8' Za svaku rešetku $L \leq \mathbb{C}$ važi

$$\wp'(z)^2 = f(\wp(z))$$

gde je $f(x) \in \mathbb{C}[x]$ sledeći kubni polinom:

$$\boxed{f(x) = 4x^3 - g_2 x - g_3} \quad (5)$$

$\boxed{3}$ Teorema 9 $L \leq \mathbb{C}$ rešetka. Preslikavanje

$$(6)\ \begin{cases} \mathbb{C}/L \longrightarrow \mathbb{P}^2_{\mathbb{C}} \\ z \longmapsto (\wp(z), \wp'(z), 1), \quad \text{za } z \neq 0 \\ 0 \longmapsto (0, 1, 0) \quad \text{- "tačka u beskonačnosti"} \end{cases}$$

je analitička 1-1 korespondencija između torusa $\mathbb{C}/L$ i eliptičke krive $\boxed{y^2 = 4x^3 - g_2(L)x - g_3(L)}$ (7)

(tj. njene homogenizacije u $\mathbb{P}^2_{\mathbb{C}}$)

▼ Za svako $z \neq 0$, slika preslikavanjem (6) pripada eliptičkoj krivi (7) na osnovu Posl. 8', dok $z = 0$ presl. (6) šalje u tačku u beskonačnost projektivizacije krive (7):

$$Zy^2 = 4x^3 - g_2(L)xZ^2 - g_3(L)Z^3$$

• Preslikavanje (6) je '1-1' i 'na':

- U tačku u ∞ se slika samo $z=0$
- Neka je sada tačka $(x, y, 1)$ proizvoljna tačka na eliptičkoj krivoj (7).

– Ako je $x \in \{e_1, e_2, e_3\}$ – jedan od korena

$$e_1 = \wp\left(\frac{\omega_1}{2}\right) \quad e_2 = \wp\left(\frac{\omega_2}{2}\right) \quad e_3 = \wp\left(\frac{\omega_1+\omega_2}{2}\right)$$

kubnog polinoma (5), na osnovu (L.7) znamo da jednačina $\wp(z) = x$ ima tačno jedno rešenje (u Π', odnosno na torusu $\mathbb{C}/L$)

U tim tačkama je $y^2 = f(x) = 0$ tj. $y = 0$

Ali takođe znamo da je $\wp'\left(\frac{\omega_1}{2}\right) = \wp'\left(\frac{\omega_2}{2}\right) = \wp'\left(\frac{\omega_1+\omega_2}{2}\right) = 0$

pa preslikavanje (6) šalje

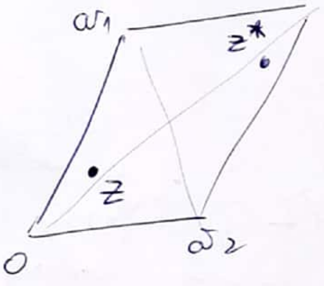
$$\frac{\omega_1}{2} \longmapsto (e_1, 0, 1)$$

$$\frac{\omega_2}{2} \longmapsto (e_2, 0, 1)$$

$$\frac{\omega_1+\omega_2}{2} \longmapsto (e_3, 0, 1)$$

Pokazali smo da su e_1, e_2, e_3 su međusobno različiti, pa je i ovde 'preslikavanje 1-1 i na'.

– Ako $x \notin \{e_1, e_2, e_3\}$. Onda (L7) garantuje da jednačina $\wp(z) = x$ ima dva različita i "simetrična" rešenja z i z^* na Π' (torusu).



Za ove vrednosti je

$$\wp'(z)^2 = f(\wp(z)) = f(x) \neq 0 \quad \left(\text{jer } x \text{ nije koren!}\right)$$

Posledica $\wp'$

$$\wp'(z^*)^2 = f(\wp(z^*)) = f(x) \neq 0$$

Međutim, $\wp'$ je <u>neparna</u> funkcija, pa iz toga i eliptičnosti sledi da je $\wp'(z^*) = -\wp'(z)$ tj. vrednosti $\wp'$ u ove dve tačke su različitog znaka.

Ovo daje da je preslikavanje (6) bijektivno i na

$$\Pi' \setminus \left\{ \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}, 0 \right\} \longleftrightarrow \left(\begin{array}{c} \text{projektivna eliptička kriva} \\ - \ 4 \text{ tačke} \end{array} \right)$$

- Na kraju preslikavanje (6) je analitičko: oko svake tačke na torusu $\mathbb{C}/L$ dato je trojkom analitičkih f-ja.

  - van tačke 0, tj. za tačke na $\mathbb{C}$ koje nisu tačke rešetke, definisano je sa

$$z \longmapsto (\wp(z), \wp'(z), 1)$$

analitičke (holomorfne) na $\mathbb{C} - L$

  - u okolini tačke 0, tj. za tačke na L, preslikavanje (6) je opet definisano sa

$$z \longmapsto \left(\frac{\wp(z)}{\wp'(z)}, 1, \frac{1}{\wp'(z)} \right)$$

opet analitičke f-je u proširenoj okolini 0

($\frac{\wp}{\wp'}$ je analitička jer brojioc ima pol reda 2, a imenilac pol reda 3)

P.S. Ja slobodno šetam sa $\mathbb{C}$ na $\mathbb{C}/L$, što odgovara u algebri radu sa predstavnicima koseta podgrupe, ili sa kosetima (tj. nema veze - jer su sve f-je L-periodične). Prelazak na $\mathbb{C}$ - je zgodan jer tu već imamo "kompleksnu kartu".