ELIPTIČNE FUNKCIJE

IZAK JENKO

Fakulteta za matematiko in fiziko
Univerza v Ljubljani

V članku je obravnanvana osnovna teorija eliptičnih funkcij, ki so dvojno periodične meromorfne funkcije na kompleksni ravnini. Konstruira se nekaj primerov eliptičnih funkcij, nato pa se osredotoči na Weierstrassovo eliptično funkcijo $\wp$. V članku se izpelje njen Laurentov razvoj okoli izhodišča in vpelje Eisensteinove vrste. Nazadnje se pokazaže, kako $\wp$ in njen odvod parametrizirata določeno eliptično krivuljo nad poljem kompleksnih števil.

ELLIPTIC FUNCTIONS

This paper discusses the basic theory of elliptic functions, which are doubly periodic meromorphic functions on the complex plane. A few examples of elliptic functions are constructed and afterwards focus shifts to the Weierstrass elliptic function $\wp$. Laurent expansion of $\wp$ around the origin is derived, where Eisenstein series are also introduced. Lastly it is shown, that $\wp$ along with its derivative parametrizes a certain elliptic curve over the field of complex numbers.

1. Uvod

Dobro poznamo enojno periodične fukcije, kot sta na primer funkciji sinus in kosinus. Poleg njunih analitičnih lastnosti sta zanimivi tudi iz algebraičnega vidika. Zadoščata namreč zvezi

$$\cos^2(z) + \sin^2(z) = 1,$$

ki velja za vse $z \in \mathbb{C}$, kar pomeni, da predpis $z \mapsto (\cos(z), \sin(z))$ podaja dobro definirano funkcijo, ki slika v krivuljo, podano z enačbo $x^2 + y^2 = 1$. Če gledamo rešitve te enačbe v prostoru $\mathbb{C}^2$, te tvorijo podmnožico $C \subseteq \mathbb{C}^2$, tovrstne množice rešitev polinomskih enačb v dveh spremenljivkah pa splošno imenujemo afine algebraične krivulje nad poljem kompleksnih števil $\mathbb{C}$. V nadaljevanju bo za nas pomembna projektivna različica krivulj, zato najprej vpeljemo *kompleksno projektivno ravnino*. To je prostor

$$\mathbb{P}^2_{\mathbb{C}} = (\mathbb{C}^3 \setminus \{0\})/\langle v \sim \lambda v; \lambda \in \mathbb{C}^* \rangle,$$

opremljen s kvocientno topologijo, ki je največja topologija na tej množici, za katero je kvocientna projekcija $\mathbb{C}^3 \setminus \{0\} \to \mathbb{P}^2_{\mathbb{C}}$ zvezna. Pri tem $\mathbb{C}^*$ označuje multiplikativno grupo kompleksnih števil. Na projektivni ravnini imamo tudi t. i. *homogene koordinate* in sicer ekvivalenčni razred predstavnika točke $(x, y, z) \in \mathbb{C}^3 \setminus \{0\}$ označimo s $[x : y : z]$. Za homogene koordinate tedaj jasno velja zveza $[\lambda x : \lambda y : \lambda z] = [x : y : z]$ za vse $\lambda \in \mathbb{C}^*$.

Osredotočili se bomo na posebne projektivne algebraične krivulje tretjega reda − *eliptične krivulje*. Eliptična krivulja E je množica točk $[x : y : z] \in \mathbb{P}^2_{\mathbb{C}}$, ki zadošča Weierstrassovi enačbi

$$E : \quad y^2 z = 4x^3 - axz^2 - bz^3, \tag{1}$$

kjer je $a^3 - 27b^2 \neq 0$. Pogoj o koeficientih a in b nam zagotavlja, da je ta krivulja nesingularna.

Opomnimo, zakaj je ta definicija smiselna. Naj bo $F(x, y, z) = y^2 z - 4x^3 + axz^2 + bz^3$ polinom, ki izhaja iz enačbe (1). Opazimo, da je F homogen in zanj velja $F(\lambda x, \lambda y, \lambda z) = \lambda^3 F(x, y, z)$ za vse $\lambda \in \mathbb{C}^*$. Pogoj $F(x, y, z) = 0$ je tako neodvisen od izbire homogenih koordinat točke $[x : y : z] \in \mathbb{P}^2_{\mathbb{C}}$, torej je eliptična krivulja E dobro definirana podmnožica projektivne ravnine $\mathbb{P}^2_{\mathbb{C}}$. Za uvod v teorijo algebraičnih krivulj se skličemo na [1]. Eliptično krivuljo opremimo še s topologijo podprostora, ki jo podeduje iz $\mathbb{P}^2_{\mathbb{C}}$.

V nadaljevanju bomo obravnavali Weierstrassovo eliptično funkcijo $\wp$, ki bo skupaj s svojim odvodom za eliptično krivuljo E imela podobno vlogo, kot jo imata funkciji sinus in kosinus za krivuljo C, podano z enačbo $x^2 + y^2 = 1$. Weierstrassova eliptična funkcija $\wp$ bo osrednja tema tega članka.

2. Eliptične funkcije

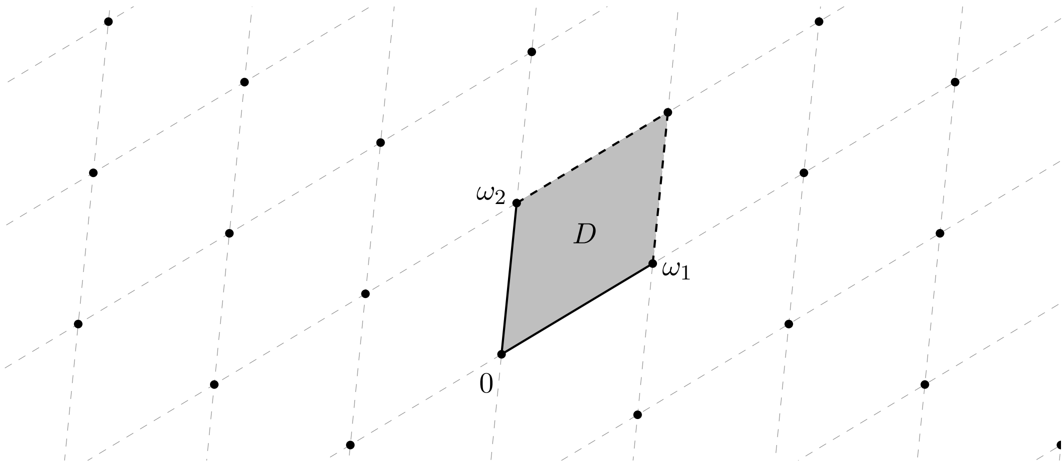
Eliptične funkcije so meromorfne funkcije na kompleksni ravnini, periodične v dveh realno linearno neodvisnih smereh. Da jih zares vpeljemo, pa najprej potrebujemo nekaj novih pojmov.

Definicija 1. Aditivna podgrupa kompleksnih števil $\mathbb{C}$ izomorfna abelovi grupi $\mathbb{Z}^2$ se imenuje *mreža*.

Ekvivalentno je mreža prosta abelova grupa na dveh generatorjih $\omega_1, \omega_2 \in \mathbb{C}^*$, ki jima pravimo *osnovni periodi*, za kateri velja $\operatorname{Im} \frac{\omega_1}{\omega_2} \neq 0$, kar pomeni, da sta realno linearno neodvisni. Splošnemu elementu $\omega \in \Lambda$ pravimo *perioda*. Eksplicitno si mrežo predstavljamo kot množico točk v kompleksni ravnini

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{k_1\omega_1 + k_2\omega_2 \mid k_1, k_2 \in \mathbb{Z}\},$$

kot kaže slika 1.



Slika 1. Mreža Λ in fundamentalni paralelogram D.

Na kompleksno ravnino $\mathbb{C}$ vpeljimo relacijo

$$z \sim w \iff z - w \in \Lambda \quad \text{za vsaka } z, w \in \mathbb{C}.$$

To pomeni, da identificiramo vsaki dve točki, ki se razlikujeta kvečjemu za prišteto periodo $\omega \in \Lambda$. Brez težav se lahko prepričamo, da je to ekvivalenčna relacija na $\mathbb{C}$. Tako lahko tvorimo kvocientno množico $\mathbb{C}/_\sim$, katere ekvivalenčne razrede bomo označevali z $z + \Lambda$ in jih imenovali *translati*, saj si jih lahko predstavljamo kot za vektor z translirano mrežo Λ. Pripadajoča kvocientna projekcija bo $\pi : \mathbb{C} \to \mathbb{C}/_\sim$. Kvocient $\mathbb{C}/_\sim$ bomo od tod dalje rajši označevali s $\mathbb{C}/\Lambda$. To množico lahko opremimo še s kvocientno topologijo, od koder je razvidno, da je kvocientni prostor $\mathbb{C}/\Lambda$ v resnici homeomorfen torusu.

Definicija 2. *Fundamentalni paralelogram* za mrežo $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ je

$$D_\alpha = \{\alpha + t_1\omega_1 + t_2\omega_2 \mid t_1, t_2 \in [0, 1)\}.$$

Zaprtje fundamentalnega paralelograma D_α v $\mathbb{C}$ bomo označili z $\overline{D}_\alpha$.

Opomba 1. Kadar bomo govorili o fundamentalnih paralelogramih pogosto izbira izhodišča α ne bo pomembna, zato ga bomo tedaj izpustili in pisali samo D. V tem primeru lahko privzamemo, da je s tem mišljen D_0.

Naslednja lema pove, da je preslikava $D_\alpha \to \mathbb{C}/\Lambda$ bijekcija med možicama.

Lema 1. *Poljuben translat $z + \Lambda$ mreže $\Lambda \subseteq \mathbb{C}$ ima natanko enega predstavnika v fundamentalnem paralelogramu D_α.*

Dokaz. Ker sta osnovni periodi ω_1, ω_2 $\mathbb{R}$-linearno neodvisni, tvorita bazo za $\mathbb{C}$ gledano kot realen vektorski prostor. Tako lahko zapišemo $z - \alpha = a_1\omega_1 + a_2\omega_2$, kjer sta $a_1, a_2 \in \mathbb{R}$. Tedaj za

$$t_i = a_i - \lfloor a_i \rfloor \in [0, 1) \quad \text{za } i \in \{1, 2\},$$

kjer $\lfloor x \rfloor$ označuje največje celo število, ki ni večje od x, velja $\alpha + t_1\omega_1 + t_2\omega_2 = z - \lfloor a_1 \rfloor \omega_1 - \lfloor a_2 \rfloor \omega_2 \in D_\alpha \cap (z + \Lambda)$. ∎

Spomnimo se, da so *holomorfne* funkcije na neki odprti domeni $D \subseteq \mathbb{C}$ tiste, ki jih je mogoče odvajati v kompleksnem smislu povsod na D. Kolobar holomorfnih funkcij na D označimo z $\mathcal{O}(D)$. Če je funkcija holomorfna na celotnem $\mathbb{C}$, pravimo, da je *cela holomorfna* funkcija. Množico teh označimo z $\mathcal{O}(\mathbb{C})$.

Če je $S \subseteq D$ diskretna množica brez stekališč v D, potem funkcijam, ki so holomorfne na $D \setminus S$, v točkah iz S pa imajo pole, pravimo *meromorfne* funkcije, točkam iz S pa *singularnosti.* Vsako meromorfno funkcijo f na $D \subseteq \mathbb{C}$ lahko vidimo tudi kot preslikavo $D \to \widehat{\mathbb{C}}$ v Riemannovo sfero $\widehat{\mathbb{C}}$, kjer dodatno definiramo

$$f(w) = \infty \quad \text{za vsak } w \in S.$$

Definicija 3. Naj bo f meromorfna funkcija na $\mathbb{C}$ in $\Lambda \subseteq \mathbb{C}$ mreža. Če za f velja

$$f(z + \omega) = f(z) \quad \text{za vse } \omega \in \Lambda \text{ in } z \in \mathbb{C},$$

potem pravimo, da je f *eliptična* oziroma *dvojno periodična* funkcija. Kadar želimo poudariti, da je f eliptična glede na mrežo Λ, pravimo, da je Λ-*periodična.*

3. Lastnosti eliptičnih funkcij

Sedaj si bomo pogledali nekaj izrekov, ki opisujejo naravo eliptičnih funkcij in jih lahko povečini pripišemo Liouvillu. Prvi je direktna posledica njegovega slavnega izreka iz kompleksne analize, ki pove, da razen konstant celih omejenih holomorfnih funkcij ni. Dokaz tega izreka lahko najdemo v [2, izrek 59].

Izrek 2. *Naj bo f cela eliptična funkcija. Tedaj je f konstantna.*

Dokaz. Ker je f konstantna na ekvivalenčnih razredih množice $\mathbb{C}/\Lambda$, tj. translatih oblike $z + \Lambda$, je enolično določena že z vrednostjo na enem od predstavnikov vsakega translata. Po lemi 1 vidimo, da lahko predstavnika poljubnega translata najdemo v fundametnalnem paralelogramu D, zato bo

$$\sup_{z \in \mathbb{C}} |f(z)| = \sup_{z \in \overline{D}} |f(z)|.$$

Ker je f holomorfna na celotnem $\mathbb{C}$, je tam seveda zvezna in je zato zvezna tudi na zaprtju fundamentalnega paralelograma $\overline{D}$. To je zaprta in omejena množica v $\mathbb{C}$ in je tako kompaktna [3, trditev 2.22]. Zvezna funkcija f je na kompaktu $\overline{D}$ omejena, kot eliptična funkcija pa je tako omejena na celotnem $\mathbb{C}$ [3, posledica 2.28]. Funkcija f je torej omejena in cela holomorfna, zato je po Liouvillovem izreku konstantna. ∎

Opomba 2. Enako lahko sklepamo tudi, če f nima ničel. Tedaj je $1/f$ cela eliptična funkcija, ko jo v polih f razširimo z 0.

Lema 3. *Naj bo f eliptična funkcija. Tedaj je tudi njen odvod f' eliptična funkcija.*

Dokaz. Recimo, da je $z \in \mathbb{C}$ točka, kjer f nima pola, zato je v njeni okolici holomorfna in jo lahko odvajamo v kompleksnem smislu. Z odvajanjem osnovnega pogoja za eliptične funkcije dobimo

$$f'(z+\omega) = f'(z) \quad \text{za vsak } \omega \in \Lambda.$$

Če pa je v točki $z \in \mathbb{C}$ pol funkcije f, ima tudi f' v tej točki pol, torej pogoj za eliptičnost velja povsod na $\mathbb{C}$. ∎

Vpeljimo nekaj notacije, ki jo bomo potrebovali v naslednjih izrekih. Če je f meromorfna funkcija na odprti domeni $D \subseteq \mathbb{C}$, pravimo, da ima f *red* $m \in \mathbb{Z}$ v točki $z_0 \in D$, če obstaja okolica $U \subseteq D$ točke z_0 in holomorfna funkcija $g \in \mathcal{O}(U)$, ki je neničelna povsod na U, da velja

$$f(z) = (z - z_0)^m g(z) \quad \text{za vse } z \in U.$$

Tedaj označimo $\operatorname{ord}_{z_0}(f) = m$. Če je $m > 0$, ima f v z_0 *ničlo* reda m, če pa je $m < 0$, ima f v z_0 *pol* reda $-m$.

Residuum ali *ostanek* funkcije f pri točki $z_0 \in D$ je koeficient pred potenco $(z - z_0)^{-1}$ v Laurentovi vrsti za f okrog z_0. Označimo ga z $\operatorname{res}_{z_0}(f)$.

Izrek 4. *Naj bo f eliptična funkcija in D fundamentalni paralelogram glede na mrežo Λ, katerega rob ∂D ne vsebuje polov ali ničel f. Tedaj velja*

$$(i) \quad \sum_{w \in D} \operatorname{res}_w(f) = 0 \tag{2}$$

$$(ii) \quad \sum_{w \in D} \operatorname{ord}_w(f) = 0 \tag{3}$$

$$(iii) \quad \sum_{w \in D} \operatorname{ord}_w(f) \cdot w \in \Lambda. \tag{4}$$

Dokaz. (i) Uporabimo izrek o ostankih [2, izrek 71], ki pove

$$\sum_{w \in D} \operatorname{res}_w(f) = \frac{1}{2\pi i} \int_{\partial D} f(z) dz.$$

Razdelimo rob fundametalnega paralelograma $\partial D = \sigma_1 \cup \sigma_2 \cup \sigma_3 \cup \sigma_4$ na štiri daljice, ki ga omejujejo, kot prikazuje slika 2. Pri tem opomnimo, da so daljice $\sigma_1, \ldots, \sigma_4$ orienirane skladno s pozitivno orientacijo roba paralelograma D.

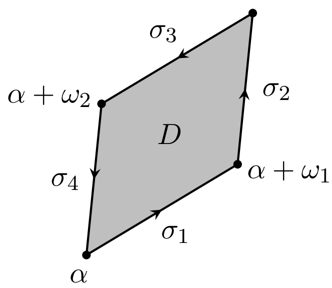
Jasno tedaj velja

$$\int_{\partial D} f(z) dz = \int_{\sigma_1} f(z) dz + \int_{\sigma_2} f(z) dz + \int_{\sigma_3} f(z) dz + \int_{\sigma_4} f(z) dz.$$

Z menjavo spremenljivk $w = z + \omega_2$ v prvem in $w = z + \omega_1$ v četrtem integralu je zaradi Λ-periodičnosti f in orientacije obeh parov nasprotnih stranic (σ_1 in σ_3 ter σ_2 in σ_4) razvidno, da se integrala po parih nasproti ležečih stranic izničita, kar nam da želeni rezultat 0.

(ii) Po lemi 3 je f' eliptičen, zato je tudi kvocient f'/f eliptičen. Tedaj velja

$$\sum_{w \in D} \operatorname{ord}_w(f) = \frac{1}{2\pi i} \int_{\partial D} \frac{f'(z)}{f(z)} dz = 0,$$



Slika 2. Fundamentalni paralelogram.

kjer smo v prvi enakosti uporabili princip argumenta [2, izrek 72], druga enakost pa je identiteta (2), ki velja zaradi eliptičnosti kvocienta f'/f.

(iii) Oglejmo si funkcijo $z \mapsto z\frac{f'(z)}{f(z)}$. Jasno je ta funkcija meromorfna na $\mathbb{C}$. Naj bo $z_0 \in \mathbb{C}$ poljuben. Tedaj obstaja $m \in \mathbb{Z}$, okolica $U \subseteq \mathbb{C}$ točke z_0 in holomorfna funkcija $g \in \mathcal{O}(U)$, ki je neničelna na U, da velja

$$f(z) = (z - z_0)^m g(z) \quad \text{za vsak } z \in U.$$

Z odvajanjem te enakosti dobimo

$$f'(z) = m(z - z_0)^{m-1} g(z) + (z - z_0)^m g'(z),$$

ki prav tako velja povsod na U. Skupaj tako dobimo, da za vsak $z \in U$ velja

$$z\frac{f'(z)}{f(z)} = \frac{mz}{z - z_0} + z\frac{g'(z)}{g(z)} = \frac{mz_0}{z - z_0} + \underbrace{m + z\frac{g'(z)}{g(z)}}_{\in\mathcal{O}(U)}.$$

Ker sta zadnja dva člena holomorfna na U, edino člen $\frac{mz_0}{z-z_0}$ prispeva h glavnemu delu Laurentovega razvoja funkcije $z \mapsto z\frac{f'(z)}{f(z)}$ okrog z_0. Zato je

$$\operatorname{res}_{z_0}\left(z\frac{f'(z)}{f(z)}\right) = mz_0 = \operatorname{ord}_{z_0}(f) z_0.$$

Tako dobimo

$$\sum_{w\in D} \operatorname{ord}_w(f) \cdot w = \sum_{w\in D} \operatorname{res}_w \left(z\frac{f'(z)}{f(z)}\right) = \frac{1}{2\pi i}\int_{\partial D} z\frac{f'(z)}{f(z)} dz.$$

Poglejmo si sedaj zadnji integral, ki ga podobno kot pri dokazu formule (2) razbijemo na vsoto integralov po štirih stranicah. Argument o odštevanju integralov po nasprotnih stranicah paralelograma pa tokrat zaradi neperiodičnosti funkcije $z \mapsto z\frac{f'(z)}{f(z)}$ v splošnem ne bo deloval. Z uvedbo nove spremenljivke $w = z + \omega_2$ v integral po stranici σ_1 vidimo

$$\begin{aligned}\int_{\sigma_1} z\frac{f'(z)}{f(z)} dz &= \int_{\sigma_1} z\frac{f'(z+\omega_2)}{f(z+\omega_2)} dz \\ &= -\int_{\sigma_3} (w - \omega_2)\frac{f'(w)}{f(w)} dw = -\int_{\sigma_3} z\frac{f'(z)}{f(z)} dz + \omega_2 \int_{\sigma_3} \frac{f'(z)}{f(z)} dz.\end{aligned}$$

Podobno z uvedbo nove spremenljivke $w = z+\omega_1$ storimo z integralom po stranici σ_4 in tako dobimo

$$\int_{\partial D} z\frac{f'(z)}{f(z)} dz = \omega_1 \int_{\sigma_4} \frac{f'(z)}{f(z)} dz + \omega_2 \int_{\sigma_3} \frac{f'(z)}{f(z)} dz.$$

Za poljubno sklenjeno in odsekoma gladko krivuljo $\gamma : [0,1] \to \mathbb{C}$, tj. $\gamma(0) = \gamma(1)$, ki ne poteka skozi izhodišče $0 \in \mathbb{C}$, je

$$\frac{1}{2\pi i} \int_\gamma \frac{dz}{z} \in \mathbb{Z}$$

ovojno število krivulje γ okoli 0 in nam pove, kolikokrat se krivulja γ ovije okoli izhodišča. Podrobnosti o tem lahko bralec najde v [4, 4.2.1].

Osredotočimo se sedaj samo na prvi integral, premislek za drugega je analogen. Opazimo, da je zaradi eliptičnosti f krivulja $f(\sigma_4)$ sklenjena, saj sta krajišči daljice σ_4 točki α in $\alpha + \omega_2$, v katerih ima f enaki vrednosti. Pot $\gamma : [0,1] \to f(\sigma_4)$, ki predstavlja to sklenjeno krivuljo, je podana s predpisom $t \mapsto f(\alpha + t\omega_2)$. Tedaj lahko zapišemo

$$2\pi i k_1 = \int_\gamma \frac{dz}{z} = \int_0^1 \frac{\gamma'(t)}{\gamma(t)} dt = \int_0^1 \frac{f'(\alpha + t\omega_2)}{f(\alpha + t\omega_2)} \omega_2 dt = \int_{\sigma_4} \frac{f'(z)}{f(z)} dz$$

za neki $k_1 \in \mathbb{Z}$. Podobno je tako tudi

$$2\pi i k_2 = \int_{\sigma_3} \frac{f'(z)}{f(z)} dz,$$

za neki $k_2 \in \mathbb{Z}$. Skupaj je torej

$$\sum_{w \in D} \operatorname{ord}_w(f) \cdot w = \frac{1}{2\pi i} \int_{\partial D} z \frac{f'(z)}{f(z)} dz = k_1\omega_1 + k_2\omega_2 \in \Lambda. \qquad \blacksquare$$

Opomba 3. (i) V vseh treh točkah seštevamo po neštevnem fundamentalnem paralelogramu D, toda vse tri vsote vsebujejo zgolj končno mnogo neničelnih členov. Residuum in red funkcije f sta lahko različna od nič samo v ničlah ali polih f, teh pa je v kompaktu $\overline{D}$ lahko le končno, saj bi sicer prišli v nasprotje s principom identičnosti. Ta pravi, da se meromorfni funkciji, definirani na neki odprti domeni Ω, ki se ujemata na množici s stekališčem v Ω, ujemata povsod na Ω.

(ii) Kot nakazuje izrek, je izbira fundamentalnega paralelograma irelevantna, dokler ta izpolnjuje določene predpostavke o robu. Kljub temu pa se prepričajmo, da lahko vselej izberemo fundamentalni paralelogram, katerega rob ne vsebuje polov ali ničel f.

Denimo, da to ni mogoče, torej da ima vsak fundamentalni paralelogram na svojem robu vsaj en pol eliptične funkcije f. S translacijami

$$\tau_n : z \mapsto z + \frac{1}{n}(\omega_1 + \omega_2); \quad n \in \mathbb{N}$$

delujemo na rob fundamentalnega paralelograma ∂D in tako dobimo števno mnogo različnih polov za f. To zaporedje polov leži v uniji $\bigcup_{n\in\mathbb{N}} \tau_n(\partial D)$, ki jo lahko zapremo v dovolj velik zaprt disk. Na ta način dobimo zaporedje polov v kompaktu, ki ima po Bolzano-Weierstrassovem izreku stekališče, kar pa je v nasprotju s tem, da je množica polov meromorfne funkcije diskretna v $\mathbb{C}$.

Podobno lahko hkrati sklepamo še za ničle funkcije f in s pomočjo principa identičnosti pridemo v nasprotje z diskretnostjo množice ničel meromorfne funkcije f.

(iii) Formula (3) pove, da ima eliptična funkcija na fundamentalnem paralelogramu enako število ničel in polov štetih z večkratnostjo.

Definicija 4. *Red* eliptične funkcije je število polov šteto z večkratnostjo v zaprtju poljubnega fundamentalnega paralelograma.

Tudi če pol z_0 Λ-periodične funkcije f leži na robu ∂D izbranega fundamentalnega paralelograma prirejenega mreži Λ, lahko govorimo o redu tega pola *znotraj* D. Če imamo recimo pol z_0, ki leži na eni od robnih stranic fundamentalnega paralalelograma in ni eno od oglišč, zaradi Λ-periodičnosti f na nasproti ležeči stranici najdemo pol z_1, za katerega je $z_1 - z_0 \in \Lambda$. Toda ta dva pola glede na fundamentalni paralelogram D smatramo za enakovredna, saj v $\mathbb{C}/\Lambda$ določata isti točki, poleg tega pa bi lahko z dovolj majhno perturbacijo $D \rightsquigarrow D'$ dosegli, da z_0 leži v notranjosti D', z_1 pa zunaj. Reda polov z_0 in z_1 znotraj D bi zato radi enakovredno porazelili, da bo njuna vsota enaka $\operatorname{ord}_{z_0}(f)$. Tako štejemo *red pola* $z_0 \in \partial D$ *znotraj* D kot $\frac{1}{2}\operatorname{ord}_{z_0}(f)$, če pol ni eno od štirih oglišč, oziroma v primeru, ko je pol z_0 oglišče paralelograma, vzamemo za njegov red vrednost

$$\frac{\ell(\partial\Delta(z_0, r) \cap D)}{2\pi r} \operatorname{ord}_{z_0}(f).$$

Ob tem ℓ opisuje dolžino danega krožnega loka, $r > 0$ pa je dovolj majhen, da je z_0 edino oglišče fundamentalnega paralelograma, vsebovano v odprtem disku $\Delta(z_0, r) = \{z \in \mathbb{C} \mid |z - z_0| < r\}$. Z drugimi besedami je ta količina normaliziran notranji kot fundamentalnega paralelograma pri oglišču z_0, pomnožen z $\operatorname{ord}_{z_0}(f)$.

Zgled 1. Naj bo $\rho = e^{2\pi i/3}$ in $\Lambda = \mathbb{Z} + \rho\mathbb{Z}$. Fundamentalni paralelogram D te mreže je torej romb v kompleksni ravnini z oglišči 0, 1, ρ in $1 + \rho$. Naj bo f eliptična funkcija s poli v mreži Λ. Tedaj bo red pola 0 za f v D enak

$$\frac{2\pi/3}{2\pi} \operatorname{ord}_0(f) = \frac{1}{3} \operatorname{ord}_0(f),$$

saj je notranji kot romba D v oglišču 0 enak $2\pi/3$, red pola ρ za f v D pa bo enak

$$\frac{\pi/3}{2\pi} \operatorname{ord}_\rho(f) = \frac{1}{6} \operatorname{ord}_\rho(f),$$

saj stranici, ki se srečata v ρ, skupaj oklepata kot velikosti $\pi/3$. Analogno sklepamo še, da je red pola 1 za f v D enak $\frac{1}{6}\operatorname{ord}_1(f)$, red pola $1 + \rho$ pa $\frac{1}{3}\operatorname{ord}_{1+\rho}(f)$. Zaradi Λ-periodičnosti funkcije f velja $\operatorname{ord}_0(f) = \operatorname{ord}_1(f) = \operatorname{ord}_\rho(f) = \operatorname{ord}_{1+\rho}(f)$, točke 0, 1, ρ in $1 + \rho$ pa se v $\mathbb{C}/\Lambda$ identificiarjo. Zato bo

$$\frac{1}{3} \operatorname{ord}_0(f) + \frac{1}{6} \operatorname{ord}_1(f) + \frac{1}{6} \operatorname{ord}_\rho(f) + \frac{1}{3} \operatorname{ord}_{1+\rho}(f) = \operatorname{ord}_0(f).$$

Opazimo, da desna stran enačbe opisuje natanko red pola 0 za f, če bi pol 0 ležal v notranjosti fundamentalnega paralalelograma.

Posledica 5. *Nekonstantna eliptična funkcija ima red vsaj* 2.

Dokaz. Brez škode za splošnost denimo, da je f nekonstantna eliptična funkcija z enim (enostavnim) polom z_0 v fundamentalni domeni D, saj po izreku 2 že vemo, da bi bila f konstantna, če bi bila brez polov. Predpostavimo lahko tudi, da pol leži v notranjosti D. Z integracijo po robu ∂D tako dobimo neničelni residuum

$$\frac{1}{2\pi i} \int_{\partial D} f(z) dz = \operatorname{res}_{z_0}(f) \neq 0.$$

To pa je v nasprotju s formulo (2) iz izreka 4, ki pove, da je ta residuum – kot edini člen v vsoti – enak nič. ∎

Posledica 6. *Nekonstantna eliptična funkcija* $f : \mathbb{C} \to \widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ *je surjektivna.*

Dokaz. Ker je f nekonstantna, ima po izreku 2 pol in zato tam doseže točko ∞. Naj bo sedaj $w \in \mathbb{C}$ poljubna točka in pokažimo, da obstaja $z \in \mathbb{C}$, da velja $f(z) = w$.

Definirajmo $g(z) := f(z) - w$. Funkcija g je prav tako eliptična in ima pol, saj je takšna f in prištevanje konstante na ti dve lastnosti nima vpliva. Po opombi 3 (iii) ima g ničlo v $\mathbb{C}$, kar pokaže želeno. ∎

4. Weierstrassova funkcija $\wp$

Osrednja tema tega članka, za katero je bilo potrebno razvijati teorijo v prejšnjem razdelku, bo najprej definicija in pregled lastnosti t. i. *Weierstrassove funkcije* $\wp$, nato pa si bomo ogledali, kako lahko s pomočjo $\wp$ in njenega odvoda parametriziramo določeno eliptično krivuljo.

Vseskozi naj bo Λ mreža v $\mathbb{C}$ in naj velja oznaka $\Lambda' = \Lambda \setminus \{0\}$.

Definicija 5. Za celo število $k > 2$ je *Eisensteinova vrsta reda* k podana kot

$$G_k(\Lambda) = \sum_{\omega \in \Lambda'} \frac{1}{\omega^k}.$$

Opomba 4. Opazimo, da za lihe k velja $G_k(\Lambda) = 0$, saj se člena pri ω in $-\omega$ v vsoti odštejeta.

Lema 7. *Za vsako celo število $k > 2$ je Eisensteinova vrsta reda k absolutno konvergentna.*

Dokaz. Za vsak $n \in \mathbb{N}$ definirajmo množice

$$C_n = \{k_1\omega_1 + k_2\omega_2 \in \Lambda \mid |k_1| + |k_2| = n\}.$$

Induktivni sklep pokaže, da je moč posamezne od teh množic C_n enaka $4n$. Vsak element $\omega \in C_n$ pa lahko po absolutni vrednosti ocenimo $|\omega| \geq \rho n$, kjer je $\rho > 0$ razdalja od izhodišča 0 do roba paralelograma z oglišči v točkah $\pm\omega_1, \pm\omega_2$. Tedaj velja ocena

$$\sum_{\omega \in \Lambda'} \frac{1}{|\omega^k|} = \sum_{n=1}^{\infty} \sum_{\omega \in C_n} \frac{1}{|\omega|^k} \leq \sum_{n=1}^{\infty} \sum_{\omega \in C_n} \frac{1}{(\rho n)^k} = \sum_{n=1}^{\infty} \frac{4n}{\rho^k n^k} = \frac{4}{\rho^k} \sum_{n=1}^{\infty} \frac{1}{n^{k-1}}.$$

Klasičen rezultat iz realne analize pove, da zadnja vrsta konvergira natanko tedaj, ko je $k - 1 > 1$ in tako po primerjalnem kriteriju dobimo absolutno kovergenco Eisensteinove vrste $\sum_{\omega \in \Lambda'} \omega^{-k}$. ■

Lema 8. *Za vsako celo število $k > 2$ vrsta*

$$\sum_{\omega \in \Lambda'} \frac{1}{(z - \omega)^k}$$

konvergira absolutno za poljuben $z \in \mathbb{C} \setminus \Lambda'$ in enakomerno po kompaktih na $\mathbb{C} \setminus \Lambda'$.

Dokaz. Glavna ideja dokaza bo s pomočjo nekaj ocen uporabiti Weierstrassov M-test. Naj bo $K \subseteq \mathbb{C}$ poljuben kompakt disjunkten z Λ'. Kot tak je omejen, zato je vsebovan v nekem disku $\Delta(0, r)$ z radijem $r > 0$. Razdelimo obravnavo period $\omega \in \Lambda'$ na tiste, ki ležijo v disku $\Delta(0, 2r)$, in na tiste, ki ne.

(i) Zaradi kompaktnosti množice K za vse $\omega \in \Lambda' \cap \Delta(0, 2r)$ obstaja minimum

$$\min_{z \in K} |z - \omega| =: \epsilon_\omega > 0.$$

Ker pa je takšnih period, za katere je $|\omega| < 2r$, zgolj končno mnogo, denimo $n \in \mathbb{N}$, lahko za ϵ izberemo najmanjšega izmed ϵ_ω in tako velja

$$|z - \omega| \geq \epsilon \quad \text{za vse } z \in K \text{ in vse } 0 < |\omega| < 2r.$$

(ii) Za vse periode $|\omega| \geq 2r$ preko trikotniške neenakosti

$$|\omega| \leq |z - \omega| + |z| \quad \text{za vse } z \in K$$

vidimo, da velja

$$|z - \omega| \geq |\omega| - |z| \geq |\omega| - r \geq |\omega| - \frac{1}{2}|\omega| \geq \frac{1}{2}|\omega| \quad \text{za vse } z \in K.$$

Tako pridemo do ocene

$$\sum_{\omega\in\Lambda'}\frac{1}{|z-\omega|^k}=\sum_{\substack{\omega\in\Lambda'\\|\omega|<2r}}\frac{1}{|z-\omega|^k}+\sum_{\substack{\omega\in\Lambda'\\|\omega|\geq 2r}}\frac{1}{|z-\omega|^k}\leq\frac{n}{\epsilon^k}+\sum_{\substack{\omega\in\Lambda'\\|\omega|\geq 2r}}\frac{2^k}{|\omega|^k},$$

ki velja povsod na K. Ker je zadnja vsota del (po lemi 7) absolutno konvergentne Eisensteinove vrste reda k, nam Weierstrassov M-test zagotovi želeni rezultat. ■

V nadaljevanju bomo obravnavali različne funkcijske vrste holomorfnih (meromorfnih) funkcij, za katere bi se radi prepričali, da se tudi seštejejo v holomorfne funkcije. Naslednji izrek, ki ga samo navedemo, nam pove, da je zadosten pogoj za to zahtevo v bistvu samo njihova enakomerna konvergenca po komapktih.

Izrek 9 ([2, izrek 64]). *Naj bo $(f_n)_{n\in\mathbb{N}}$ zaporedje holomorfnih funkcij na odprti domeni $\Omega\subseteq\mathbb{C}$, ki enakomerno po kompaktih v Ω konvergira k limitni funkciji f. Tedaj je tudi f holomorfna na Ω in zaporedje odvodov $(f_n')_{n\in\mathbb{N}}$ konvergira enakomerno po kompaktih v Ω k odvodu limitne funkcije f'.*

Oglejmo si sedaj funkcijo $f:\mathbb{C}\setminus\Lambda\to\mathbb{C}$, podano s predpisom

$$f(z)=\sum_{\omega\in\Lambda}\frac{1}{(z-\omega)^k},\quad k>2.$$

Zaradi absolutne konvergence te vrste jo lahko seštevamo v poljubnem vrstnem redu. Če to storimo postopoma po diskih $\Delta(0,n)$ za $n\in\mathbb{N}$, dobimo zaporedje delnih vsot, ki so holomorfne na $\mathbb{C}\setminus\Lambda$ in konvergirajo k f. Poleg tega zaradi leme 8 že vemo, da ta vrsta konvergira tudi enakomerno po kompaktih v $\mathbb{C}\setminus\Lambda$, torej na tej domeni f določa holomorfno funkcijo po izreku 9. Dodatno ima f v vsakem $\omega_0\in\Lambda$ pol reda k in residuum 0, o čemer se lahko prepričamo, ko na neki dovolj majhni prebodeni okolici točke ω_0 zapišemo

$$f(z)=\frac{1}{(z-\omega_0)^k}+\sum_{\omega\in\Lambda\setminus\{\omega_0\}}\frac{1}{(z-\omega)^k}.$$

H glavnemu delu okrog ω_0 prispeva samo člen $(z-\omega_0)^{-k}$, vrsta, ki ostane, pa je zaradi leme 8 po podobnem razmisleku kot zgoraj holomorfna na tej prebodeni okolici in zato na glavni del nima vpliva. Tako je f meromorfna funkcija na $\mathbb{C}$.

Primer 1. Zgornje nam omogoča konstruirati prvi netrivialen primer eliptične funkcije, ki bo koristen tudi v nadaljevanju. Prepričajmo se, da je funkcija, podana s predpisom

$$f(z)=\sum_{\omega\in\Lambda}\frac{1}{(z-\omega)^3},$$

ne le meromorfna, ampak res tudi eliptična. Če je $z\in\mathbb{C}$ poljuben in $\omega_0\in\Lambda$ poljubna perioda, vidimo, da velja

$$f(z+\omega_0)=\sum_{\omega\in\Lambda}\frac{1}{(z+\omega_0-\omega)^3}=\sum_{\omega\in\Lambda}\frac{1}{(z-(\omega-\omega_0))^3}=\sum_{\omega\in\Lambda}\frac{1}{(z-\omega)^3}=f(z),$$

kjer smo v predzadnji enakosti upoštevali, da je translacija $\omega\mapsto\omega-\omega_0$ zgolj permutacija mreže Λ, ki samo premeša vrstni red seštevanja v zadnji (absolutno konvergentni) vrsti.

Funkcija iz primera 1 ima v vsaki periodi $\omega \in \Lambda$ pol stopnje 3 oziroma na fundamentalnem paralelogramu ima natanko pol stopnje 3, torej bi lahko rekli, da je eliptična funkcija reda 3. Posledica 5 nam zagotavlja, da je spodnja meja za red nekonstantne eliptične funkcije enaka 2, zato se je naravno vprašati, ali je ta meja kdaj dosežena. Poskusili bi lahko z vrsto $\sum_{\omega\in\Lambda}(z-\omega)^{-2}$, toda ta žal ne konvergira absolutno. Vseeno pa jo lahko nekoliko popravimo, kar nas privede do naslednje definicije.

Definicija 6. *Weierstrassova eliptična funkcija* $\wp$ glede na mrežo Λ je

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda'} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Kadar želimo poudariti, da je ta prirejena mreži Λ, pišemo tudi $\wp_\Lambda$.

Trditev 10. *Za Weierstrassovo funkcijo $\wp$ glede na mrežo Λ veljajo naslednje trditve.*

(*i*) *Vrsta, ki definira funkcijo $\wp$, konvergira absolutno in enakomerno po kompaktih v $\mathbb{C}\setminus\Lambda'$, zato je $\wp$ holomorfna funkcija na $\mathbb{C}\setminus\Lambda$.*

(*ii*) *$\wp$ je soda.*

(*iii*) *$\wp$ je Λ-periodična.*

(*iv*) *Točke iz mreže Λ so natanko poli Weierstrassove funkcije $\wp$. Vsi so stopnje 2, vsi residuumi v njih pa so enaki 0.*

Dokaz. (*i*) Naj bo $K \subseteq \mathbb{C}\setminus\Lambda$ kompakt in $r>0$, da disk $\Delta(0,r)$ omejuje kompakt K. Podobno kot v dokazu leme 8 bomo obravnavo razdelili na periode $\omega\in\Lambda$, ki ležijo znotraj diska $\Delta(0,2r)$, in na tiste, ki ležijo v njegovem komplementu. Na kompaktu K že vemo, da lahko omejimo izraz

$$\frac{1}{|z^2|} + \sum_{\substack{\omega\in\Lambda' \\ |\omega|<2r}} \left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| < M \quad \text{za vsak } z\in K,$$

kjer je $M\in\mathbb{R}$. Za periode $\omega\in\Lambda, |\omega|\geq 2r$ in $z\in K$, že poznamo oceno $|z-\omega| \geq |\omega| - |z| \geq \frac{1}{2}|\omega|$, izpeljemo pa še

$$|2\omega - z| \leq |2\omega| + |z| \leq 3|\omega|.$$

Tako velja

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| = \left| \frac{\omega^2-(z-\omega)^2}{\omega^2(z-\omega)^2} \right| = \left| \frac{z(2\omega-z)}{\omega^2(z-\omega)^2} \right| \leq \frac{r\cdot 3|\omega|}{|\omega|^2(\frac{1}{2}|\omega|)^2} = \frac{12r}{|\omega|^3},$$

kar pomeni, da lahko del vsote, ki teče po $\omega\in\Lambda', |\omega|\geq 2r$, navzgor omejimo s konstanto $12r$ pomnoženim (po lemi 7) konvergentnim delom vrste $\sum_{\omega\in\Lambda'}|\omega|^{-3}$.

Zaporedje holomorfnih delnih vsot je tako po Weierstrassovem M-testu absolutno in po kompaktih enakomerno konvergentno na $\mathbb{C}\setminus\Lambda$. Izrek 9 nam tedaj zagotavlja, da je limitna funkcija zaporedja – tj. Weierstrassova funkcija $\wp$ – holomorfna na $\mathbb{C}\setminus\Lambda$.

(*ii*) Z računom se prepričamo

$$\begin{aligned}\wp(-z) &= \frac{1}{(-z)^2} + \sum_{\omega\in\Lambda'} \left(\frac{1}{(-z-\omega)^2} - \frac{1}{\omega^2} \right) \\ &= \frac{1}{z^2} + \sum_{\omega\in\Lambda'} \left(\frac{1}{(z+\omega)^2} - \frac{1}{(-\omega)^2} \right) = \frac{1}{z^2} + \sum_{\omega\in\Lambda'} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) = \wp(z),\end{aligned}$$

kjer smo za predzadnji enačaj upoštevali, da transformacija $\omega \mapsto -\omega$ samo premeša vrstni red seštevanja v absolutno konvergentni vrsti.

(*iii*) Vemo že, da je $\wp$ holomorfna funkcija, podana z vrsto, ki konvergira enakomerno po kompaktih v $\mathbb{C} \setminus \Lambda$ in katere členi so holomorfne funkcije na tem območju. Vrsto, ki definira $\wp$, lahko torej členoma odvajamo, kar pomeni, da je odvod funkcije $\wp$ enak

$$\wp'(z) = \sum_{\omega \in \Lambda} \frac{-2}{(z-\omega)^3}.$$

Naj bo sedaj $\omega \in \Lambda$ poljubna perioda. Kot smo se prepričali v primeru 1, je $\wp'$ eliptična funkcija glede na Λ, zato je $\wp'(z+\omega) - \wp'(z) = 0$, kar pomeni, da se funkciji $\wp(z+\omega)$ in $\wp(z)$ razlikujeta zgolj za prišteto konstanto. Če vstavimo $z = -\frac{\omega}{2}$ in upoštevamo sodost funkcije $\wp$, vidimo, da je ta konstanta enaka 0, kar pokaže želeno.

(*iv*) Zaradi Λ-periodičnosti funkcije $\wp$ po točki (iii) je dovolj primer obravnavati samo okoli točke $0 \in \Lambda$. Podobno kot smo sklepali o polih funkcije $\sum_{\omega \in \Lambda'} (z-\omega)^{-k}$, tudi tukaj vidimo, da na neki prebodeni okolici točke 0 h glavnemu delu Laurentove vrste za $\wp$ okoli 0 prispeva le člen z^{-2}, ki nam da pol reda 2 z ostankom 0, preostanek vrste pa po dokazu točke (i) na tej prebodeni okolici definira holomorfno funkcijo, ki na glavni del nima vpliva. ∎

Naše zanimanje za Weierstrassovo eliptično funkcijo se skriva v dejstvu, da ta funkcija zadošča posebni diferencialni enačbi oblike $\wp'(z)^2 = f(\wp(z))$, kjer je $f \in \mathbb{C}[x]$ kubični polinom, ki je v tesni povezavi z Weierstrassovo enačbo eliptične krivulje. Da bo ta povezava jasneje razvidna, si poglejmo Laurentov razvoj $\wp$ okoli izhodišča 0.

Lema 11. *Naj bo $\wp$ Weierstrassova eliptična funkcija glede na mrežo Λ. Njen Laurentov razvoj okoli točke 0 je*

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2}(\Lambda) z^{2k}, \tag{5}$$

kjer $G_{2k}(\Lambda)$ označuje Eisensteinovo vrsto reda $2k$.

Dokaz. Najprej z odvajanjem geometrijske vrste za $(1-x)^{-1}$ pri $x \in \mathbb{C}$, $|x| < 1$ ugotovimo, da je

$$\frac{1}{(1-x)^2} = \sum_{n=0}^{\infty} (n+1) x^n$$

in ta konvergenca je enakomerna in absolutna na kompaktih v disku $x \in \Delta(0,1)$. To uporabimo v izrazu

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\left(\frac{1}{(1-\frac{z}{\omega})^2} - 1\right) = \frac{1}{\omega^2} \sum_{n=1}^{\infty} (n+1) \frac{z^n}{\omega^n} = \sum_{n=1}^{\infty} (n+1) \frac{z^n}{\omega^{n+2}},$$

ki velja za vse $\omega \in \Lambda'$ in $|z| < |\omega|$. Tako imamo

$$\begin{aligned}
\wp(z) &= \frac{1}{z^2} + \sum_{\omega\in\Lambda'} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) \\
&= \frac{1}{z^2} + \sum_{\omega\in\Lambda'} \sum_{n=1}^{\infty} (n+1) \frac{z^n}{\omega^{n+2}} \\
&= \frac{1}{z^2} + \sum_{n=1}^{\infty} \left(\sum_{\omega\in\Lambda'} \frac{1}{\omega^{n+2}} \right) (n+1) z^n \\
&= \frac{1}{z^2} + \sum_{n=1}^{\infty} (n+1) G_{n+2}(\Lambda) z^n \\
&= \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2}(\Lambda) z^{2k}
\end{aligned}$$

za vse $|z| < \min_{\omega\in\Lambda'} |\omega|$. V tretjem enačaju smo zamenjali vrstni red seštevanja, kar nam omogoča absolutna konvergenca obeh vrst, v zadnjem enačaju pa smo preindeksirali vsoto na sode $n \in \mathbb{N}$, saj so vse Eisensteinove vrste lihega reda enake 0. ■

Izrek 12. *Weierstrassova eliptična funkcija $\wp$ glede na mrežo Λ zadošča diferencialni enačbi*

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda), \tag{6}$$

kjer je sta $g_2(\Lambda) = 60G_4(\Lambda)$ in $g_3(\Lambda) = 140G_6(\Lambda)$.

Dokaz. Definirajmo funkcijo $\psi : \mathbb{C} \setminus \Lambda \to \mathbb{C}$ s predpisom

$$\psi(z) = \wp'(z)^2 - 4\wp(z)^3 + g_2(\Lambda)\wp(z) + g_3(\Lambda).$$

Kot vsota samih meromorfnih Λ-periodičnih funkcij je ψ meromorfna Λ-periodična funkcija na $\mathbb{C}$. Zato jo na neki prebodeni okolici $U \subseteq \mathbb{C}$ točke 0 lahko razvijemo v konvergentno Laurentovo vrsto. Najprej izračunajmo prvih nekaj členov Laurentovih vrst naslednjih funkcij.

$$\begin{aligned}
\wp'(z)^2 &= \frac{4}{z^6} - 24G_4(\Lambda)\frac{1}{z^2} - 80G_6(\Lambda) + 36G_4(\Lambda)^2 z^2 + \cdots \\
-4\wp(z)^3 &= -\frac{4}{z^6} - 36G_4(\Lambda)\frac{1}{z^2} - 60G_6(\Lambda) - 84G_8(\Lambda) z^2 + \cdots \\
60G_4(\Lambda)\wp(z) &= 60G_4(\Lambda)\frac{1}{z^2} + 180G_4(\Lambda)^2 z^2 + \cdots
\end{aligned}$$

Vidimo, da vsaka od njih nastopa v definiciji funkcije ψ, zato bo njen Laurentov razvoj okoli 0 enak

$$\psi(z) = 0 \cdot \frac{1}{z^6} + 0 \cdot \frac{1}{z^2} + 0 + (216G_4(\Lambda)^2 - 84G_8(\Lambda))z^2 + \cdots . \tag{7}$$

Funkcija ψ tako nima glavnega dela pri 0 in je zato na okolici U holomorfna. Zaradi Λ-periodičnosti je holomorfna tudi na okolici poljubne periode $\omega \in \Lambda$. Ker je ψ meromorfna na $\mathbb{C}$ in brez polov, je v resnici cela eliptična funkcija, kot takšna pa je po izreku 2 konstantna. Preostane le še ugotoviti kateri konstanti je enaka. Iz razvoja (7) takoj sledi, da je ta konstanta 0, ko vanjo vstavimo vrednost 0, to pa tudi zaključi dokaz izreka. ■

Izrek 12 namiguje, da lahko s poljubno mrežo Λ definiramo eliptično krivuljo

$$E_\Lambda : \quad y^2 z = 4x^3 - g_2(\Lambda)xz^2 - g_3(\Lambda)z^3. \tag{8}$$

Če vanjo vstavimo $z = 1$ ter $x = \wp$ in $y = \wp'$, dobimo natanko formulo iz izreka. Preostane se le še prepričati, da ta enačba res podaja eliptično krivuljo – preveriti je treba pogoj o nesingularnosti, torej da velja $g_2(\Lambda)^3 - 27g_3(\Lambda)^2 \neq 0$. V ta namen dokažimo naslednji dve lemi.

Lema 13. *Točka $z \in \mathbb{C} \setminus \Lambda$ je ničla za $\wp'$ natanko tedaj, ko je $2z \in \Lambda$.*

Dokaz. Najprej se lotimo implikacije iz desne v levo. Ker je $\wp$ soda po trditvi 10 (ii), vemo, da je njen odvod $\wp'$ liha funkcija. Tako lahko za $2z \in \Lambda$ z upoštevanjem Λ-periodičnosti $\wp'$ zapišemo

$$\wp'(z) = \wp'(z - 2z) = \wp'(-z) = -\wp'(z).$$

Od tod sledi, da je $\wp'(z) = 0$.

Obratno, recimo, da sta $\omega_1, \omega_2 \in \Lambda$ osnovni periodi. Tedaj so edine točke v fundamentalnem paralelogramu D_0, za katere velja $z \in \mathbb{C} \setminus \Lambda$ in $2z \in \Lambda$, ravno *polperiode*

$$\frac{\omega_1}{2}, \quad \frac{\omega_2}{2}, \quad \frac{\omega_1 + \omega_2}{2}$$

in vse tri so po zgornjem ničle $\wp'$. Kot smo se prepričali v primeru 1, je $\wp'$ eliptična funkcija reda 3, zato razen treh naštetih polperiod, ki predstavljajo enostavne ničle, po izreku 4 (ii) drugih ničel na fundamentalnem paralelogramu ni. ■

Lema 14. *Za poljubno mrežo $\Lambda \subseteq \mathbb{C}$ velja $g_2(\Lambda)^3 - 27g_3(\Lambda)^2 \neq 0$.*

Dokaz. Najprej se spomnimo, da je diskriminanta kubičnega polinoma $f(x) = 4x^3 - g_2x - g_3$ enaka $16(g_2^3 - 27g_3^2)$ in da nam ta pove, kdaj ima polinom f kakšno večkratno ničlo. Pokazali bomo, da ima za poljubno mrežo Λ polinom $4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ same različne ničle, saj je natanko takrat njegova diskriminanta neničelna.

Naj bosta $\omega_1, \omega_2 \in \Lambda$ osnovni periodi in označimo tri polperiode $r_1 = \frac{\omega_1}{2}$, $r_2 = \frac{\omega_2}{2}$, $r_3 = \frac{\omega_1+\omega_2}{2}$. Vse tri so po lemi 13 ničle za $\wp'$. Poleg tega pa so vse tri vrednosti $\wp(r_i)$ za $i \in \{1, 2, 3\}$ ničle polinoma $4x^3 - g_2(\Lambda)x - g_3(\Lambda)$, kar je razvidno takoj, ko v identiteto (6) vstavimo osnovne tri polperiode r_1, r_2, r_3.

Vemo tudi, da diskriminanto in produkt poljubnih dveh različnih ničel povezuje enakost

$$16(g_2(\Lambda)^3 - 27g_3(\Lambda)^2) = 256 \prod_{1 \leq i < j \leq 3} (\wp(r_i) - \wp(r_j))^2,$$

zato bo zadoščalo pokazati, da so vse $\wp(r_i)$ različne.

Naj bo $h_i(z) = \wp(z) - \wp(r_i)$. Funkcija h_i je eliptična funkcija reda 2 s poli v mreži Λ. Očitno je r_i njena ničla, ki pa mora biti reda 2, saj je tudi ničla odvoda $h_i' = \wp'$ po lemi 13. To pomeni, da na fundamentalnem paralelogramu drugih ničel nima. Od tod sledi, da je $\wp(r_i) \neq \wp(r_j)$ za vsaka $i \neq j$, kar pokaže, da je diskriminanta neničelna oziroma, da je $g_2(\Lambda)^3 - 27g_3(\Lambda)^2 \neq 0$. Za rezulate o diskriminanti v tem dokazu se skličemo na [5]. ■

Zaključimo lahko, da je krivulja podana z enačbo (8) res eliptična krivulja. Nazadnje pa si še poglejmo, kako preko funkcije $\wp$ definiramo preslikavo iz torusa $\mathbb{C}/\Lambda$ v eliptično krivuljo E_Λ, ki to krivuljo parametrizira.

Izrek 15. *Naj bo $\Lambda \subseteq \mathbb{C}$ mreža, $\wp$ Weierstrassova eliptična funkcija glede na mrežo Λ in naj bo $E_\Lambda \subseteq \mathbb{P}^2_{\mathbb{C}}$ eliptična krivulja podana z enačbo*

$$E_\Lambda : \quad y^2z = 4x^3 - g_2(\Lambda)xz^2 - g_3(\Lambda)z^3.$$

Tedaj je preslikava $\phi : \mathbb{C}/\Lambda \to E_\Lambda$, podana s predpisom,

$$z + \Lambda \mapsto \begin{cases} [\wp(z) : \wp'(z) : 1]\,; & z \notin \Lambda \\ [0 : 1 : 0]\,; & z \in \Lambda \end{cases}$$

dobro definiran homeomorfizem.

Dokaz. Razdelimo dokaz izreka na naslednje tri dele: dobro definiranost, zveznost in bijektivnost preslikave ϕ.

Dobra definiranost. Po izreku 12 za poljuben $z \in \mathbb{C} \setminus \Lambda$ velja $[\wp(z) : \wp'(z) : 1] \in E_\Lambda$ in posebej je tudi $[0 : 1 : 0] \in E_\Lambda$, torej bo slika preslikave ϕ res vsebovana v eliptični kriulji E_Λ.

Predpis za ϕ je podan na kvocientu $\mathbb{C}/\Lambda$, torej se moramo prepričati še o neodivisnosti le tega od izbire predstavnikov ekvivalenčnih razredov. Če sta $z, w \in \mathbb{C}$ predstavnika istega ekvivalenčnega razreda, velja $z - w \in \Lambda$ oz. $w = z + \omega$, za neki $\omega \in \Lambda$. V primeru, ko je $z \notin \Lambda$, je tudi $w \notin \Lambda$, in tedaj zaradi Λ-periodičnosti funkcije $\wp$ velja

$$\big[\wp(w) : \wp'(w) : 1\big] = \big[\wp(z+\omega) : \wp'(z+\omega) : 1\big] = \big[\wp(z) : \wp'(z) : 1\big]\,.$$

Kadar pa sta $z, w \in \Lambda$, je že sam predpis ϕ neodvisen od izbire predstavnika, torej je celoten predpis ϕ res dobro definiran na točkah kvocienta $\mathbb{C}/\Lambda$.

Zveznost. Prepričajmo se, da je preslikava $\phi : \mathbb{C}/\Lambda \to E_\Lambda$ zvezna. Za nadaljevanje bo koristno poznati limiti

$$\lim_{z\to 0} \frac{\wp(z)}{\wp'(z)} = 0 \quad \text{in} \quad \lim_{z\to 0} \frac{1}{\wp'(z)} = 0,$$

zato ju izračunajmo. Spomnimo se obnašanja $\wp$ oz. $\wp'$ okoli svojih polov. Po trditvi 10 ima $\wp$ v točki 0 pol druge stopnje, zato obstajata takšni holomorfni funkciji $g, h \in \mathcal{O}(U)$, definirani na neki dovolj majhni odprti okolici $U \subseteq \mathbb{C}$ točke 0, ki sta na U neničelni, da velja $\wp(z) = \frac{g(z)}{z^2}$ in $\wp'(z) = \frac{h(z)}{z^3}$ za vse $z \in U$. Tedaj izračunamo

$$\lim_{z\to 0} \frac{\wp(z)}{\wp'(z)} = \lim_{z\to 0} \frac{g(z)z^3}{h(z)z^2} = \frac{g(0)}{h(0)} \cdot \lim_{z\to 0} \frac{z^3}{z^2} = 0$$

ter

$$\lim_{z\to 0} \frac{1}{\wp'(z)} = \lim_{z\to 0} \frac{z^3}{h(z)} = \frac{1}{h(0)} \cdot \lim_{z\to 0} z^3 = 0.$$

Zaradi Λ-periodičnosti dobimo tudi $\lim_{z\to\omega} \frac{\wp(z)}{\wp'(z)} = 0$ in $\lim_{z\to\omega} \frac{1}{\wp'(z)} = 0$ za vsak $\omega \in \Lambda$. Vidimo torej, da imata funkciji $\frac{\wp}{\wp'}$ in $\frac{1}{\wp'}$ zgolj odpravljivi singularnosti v točkah iz Λ, kar pomeni, da ju lahko z vrednostjo 0 v teh točkah holomorfno razširimo. Z manjšo zlorabo oznak bomo ti dve razšitivi spet označili kar s $\frac{\wp}{\wp'}$ oziroma $\frac{1}{\wp'}$ in razumeli $\frac{\wp(\omega)}{\wp'(\omega)} = 0$ ter $\frac{1}{\wp'(\omega)} = 0$ za $\omega \in \Lambda$.

Po lemi 13 vemo, da ima $\wp'$ po tri enostavne ničle na fundamentalnem paralelogramu v polperiodah mreže Λ, tj. v množici $\frac{1}{2}\Lambda = \{\frac{\omega}{2} \in \mathbb{C} \mid \omega \in \Lambda\}$. Natančneje je množica ničel funkcije $\wp'$ natanko $\frac{1}{2}\Lambda \setminus \Lambda$. Polperiode iz mreže Λ smo izvzeli, saj ima v vsaki izmed njih $\wp'$ pol tretje stopnje. Funkciji $\frac{\wp}{\wp'}$ in $\frac{1}{\wp'}$ sta tako dobro definirani holomorfni Λ-periodični funkciji na odprti domeni $\mathbb{C} \setminus (\frac{1}{2}\Lambda \setminus \Lambda)$.

Naj $\pi : \mathbb{C} \to \mathbb{C}/\Lambda$ označuje kvocientno projekcijo. Opazimo, da je ϕ natanko preslikava, ki jo inducira preslikava

$$\Phi : \mathbb{C} \to E_\Lambda, \quad z \mapsto \begin{cases} [\wp(z) : \wp'(z) : 1]\,; & z \notin \Lambda \\ [0 : 1 : 0]\,; & z \in \Lambda \end{cases},$$

zato bo zaradi trditve [3, trditev 3.22] dovolj preveriti zveznost Φ, ker je π kvocientna. Podali bomo dva predpisa za Φ, definirana na odprtih podmnožicah v $\mathbb{C}$, katerih unija bo pokrila $\mathbb{C}$, in oba predpisa se bosta na njunem preseku ujemala.

Vzemimo odprti množici $U_0 = \mathbb{C} \setminus \Lambda$ in $U_1 = \mathbb{C} \setminus (\frac{1}{2}\Lambda \setminus \Lambda)$ in definirajmo preslikavi

$$\Phi_0 : U_0 \to E_\Lambda, \quad z \mapsto \big[\wp(z) : \wp'(z) : 1\big]\,,$$
$$\Phi_1 : U_1 \to E_\Lambda, \quad z \mapsto \left[\tfrac{\wp(z)}{\wp'(z)} : 1 : \tfrac{1}{\wp'(z)}\right].$$

Zaradi omenjenih lastnosti $\frac{\wp}{\wp'}$ in $\frac{1}{\wp'}$ sta Φ_0 in Φ_1 zvezni kot kompoziciji preslikav $\mathbb{C} \to \mathbb{C}^3 \setminus \{0\}$ in zvezne kvocientne projekcije $q : \mathbb{C}^3 \setminus \{0\} \to \mathbb{P}^2_{\mathbb{C}}$. Na preseku njunih domen $U_0 \cap U_1 = \mathbb{C} \setminus \frac{1}{2}\Lambda$ velja

$$\Phi_0(z) = \big[\wp(z) : \wp'(z) : 1\big] = \Big[\tfrac{\wp(z)}{\wp'(z)} : 1 : \tfrac{1}{\wp'(z)}\Big] = \Phi_1(z),$$

saj je $\wp'(z) \in \mathbb{C}^*$ za $z \in \mathbb{C} \setminus \frac{1}{2}\Lambda$. Ker preslikavi Φ_0 in Φ_1 skupaj določata ravno Φ, je slednja zvezna, od koder sledi, da je tudi ϕ zvezna.

Bijektivnost. Nazadnje pokažimo še, da je ϕ bijekcija. Začnimo s surjektivnostjo. Očitno je $\phi(0 + \Lambda) = [0 : 1 : 0]$, zato izberimo poljubno točko $[x_0 : y_0 : z_0] \in E_\Lambda \setminus \{[0 : 1 : 0]\}$. Opazimo, da je koordinata z_0 te točke neničelna, kajti v nasprotnem primeru iz enačbe (8) sledi še $x_0 = 0$, kar pomeni, da je $[x_0 : y_0 : z_0] = [0 : 1 : 0]$. Brez izgube splošnosti lahko še dodatno predpostavimo, da velja $z_0 = 1$, kar dosežemo, ko homogene koordinate točke $[x_0 : y_0 : z_0]$ delimo z z_0.

Ker je po trditvi 6 eliptična funkcija $\wp$ surjektivna, obstaja $z \in \mathbb{C} \setminus \Lambda$, da je $\wp(z) = x_0$. Iz identitete (6) sledi $\wp'(z)^2 = y_0^2$, torej sta $\wp'(z)$ in y_0 enaka do predznaka natančno. Ker pa je $\wp$ soda in $\wp'$ liha, lahko po potrebi zamenjamo $-z$ in z, da dobimo $\wp(z) = x_0$ in $\wp'(z) = y_0$ oziroma $\phi(z + \Lambda) = [x_0 : y_0 : 1]$.

Pokažimo še injektivnost ϕ. Omejili se bomo samo na injektivnost zožitve $\phi|_{\pi(\mathbb{C}\setminus\Lambda)}$, saj je $0 + \Lambda$ edina točka, ki se preslika v $[0 : 1 : 0]$, slike vseh ostalih točk imajo namreč tretjo projektivno koordinato neničelno. Naj bosta $z_1 + \Lambda, z_2 + \Lambda \in \pi(\mathbb{C} \setminus \Lambda)$ poljubni in denimo, da velja $\phi(z_1 + \Lambda) = \phi(z_2 + \Lambda)$. Zaradi redukcije na območje $\pi(\mathbb{C} \setminus \Lambda)$ imamo opravka samo z afinim delom krivulje E_Λ in se zato zgronji pogoj prevede v ekvivalentnega

$$(\wp(z_1), \wp'(z_1)) = (\wp(z_2), \wp'(z_2)). \tag{9}$$

Ločimo dve možnosti:

- Če je $2z_1 \in \Lambda$, je z_1 polperioda, torej je $\wp'(z_1) = 0$ po lemi 13. Posledično iz predpostavke (9) sledi $\wp'(z_2) = 0$, zato je tudi z_2 polperioda. Predstavnik točke $z_1 + \Lambda$ je tako do prištete periode iz Λ natanko ena od polperiod
$$\frac{\omega_1}{2}, \quad \frac{\omega_2}{2}, \quad \frac{\omega_1 + \omega_2}{2}.$$
Iz dokaza leme 14 vemo, da $\wp$ v vsaki od teh treh polperiod zavzame drugačno vrednost, torej iz $\wp(z_1) = \wp(z_2)$ sledi $z_1 + \Lambda = z_2 + \Lambda$.

- Če je $2z_1 \notin \Lambda$, potem z_1 ni ena od polperiod in je $\wp'(z_1) \neq 0$. Ker je $\wp$ reda 2, je takšna tudi $\wp - \wp(z_1)$, zato ima slednja natanko dve ničli na fundamentalnem paralelogramu oz. na $\mathbb{C}/\Lambda$, šteti z večkratnostmi. Ena je gotovo $z_1 + \Lambda$, druga pa je $-z_1 + \Lambda$, saj je $\wp$ soda. Ker z_1 ni polperioda, sta ti dve točki iz $\mathbb{C}/\Lambda$ res tudi različni. Tako iz $\wp(z_1) = \wp(z_2)$ sledi
$$z_1 \equiv \pm z_2 \mod \Lambda.$$
Zaradi lihosti $\wp'$ in ker velja $\wp'(z_1) \neq 0$, se lahko zgodi le $z_1 + \Lambda = z_2 + \Lambda$, kajti v nasprotnem primeru bi imeli $\wp'(z_2) = \wp'(-z_1) = -\wp'(z_1) \neq \wp'(z_1)$, kar je v nasprotju s pogojem (9).

Skupaj je tako ϕ res zvezna bijekcija. Ker pa poleg tega slika iz kompakta $\mathbb{C}/\Lambda$ v Hausdorffov prostor $E_\Lambda \subseteq \mathbb{P}^2_{\mathbb{C}}$, je ϕ tudi homeomorfizem. ■

5. Zaključek

Videli smo, kako lahko poljubni mreži $\Lambda \subseteq \mathbb{C}$ priredimo eliptično krivuljo E_Λ, podano z enačbo (8), ki jo parametrizirata Weierstrassova funkcija $\wp$, prirejena mreži Λ, in njen odvod $\wp'$. Omenimo še, da imamo tudi neke vrste inverz te prireditve. Če začnemo z eliptično krivuljo E, podano z enačbo

$$E: \quad y^2z = 4x^3 - axz^2 - bz^3,$$

kjer sta a in b poljubni kompleksni števili, za kateri velja $a^3 - 27b^2 \neq 0$, vedno obstaja mreža Λ in pripadajoča Weierstrassova eliptična funkcija $\wp_\Lambda$, da $\wp_\Lambda$ in $\wp'_\Lambda$ parametrizirata E. Dokaz tega se dotakne modularnih funkcij in j-invariante, o čemer lahko več izvemo v [6, §3] in [7].

LITERATURA

[1] C. G. Gibson, *Elementary geometry of algebraic curves: An undergraduate introduction*, Cambridge University Press, Cambridge, (1998).

[2] J. Globevnik in M. Brojan, *Analiza II*, (2010), `https://www.fmf.uni-lj.si/~globevnik/skriptaII.pdf`, [ogled 30. 5. 2022]

[3] J. Mrčun, *Topologija*, Izbrana poglavja iz matematike in računalništva **44**, DMFA – založništvo, Ljubljana, (2008).

[4] L. V. Ahlfors, *Complex analysis*, third edition, McGraw-Hill Education, New York, NY, 1979.

[5] A. E. Brouwer, *Resultant and discriminant*, `https://www.win.tue.nl/~aeb/2WF02/resultant.pdf`, [ogled 29. 5. 2022]

[6] P. Stevenhagen, *Complex elliptic curves*, (2013), `http://www.julianlyczak.nl/teaching/EC2015-files/ec.pdf`, [ogled 30. 5. 2022]

[7] I. Jenko, *Eliptične krivulje in kompleksni torusi: delo diplomskega seminarja*, (2022), `https://repozitorij.uni-lj.si/IzpisGradiva.php?id=139404&lang=slv`