UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO

Matematika – 1. stopnja

Izak Jenko

**Eliptične krivulje in kompleksni torusi**

Delo diplomskega seminarja

Mentor: izr. prof. dr. Sašo Strle

Ljubljana, 2022

## Kazalo

**Eliptične krivulje in kompleksni torusi**


Povzetek

*Eliptična krivulja* nad poljem kompleksnih števil $\mathbb{C}$ je nesingularna projektivna kubika, podana z Weierstrassovo enačbo. S pomočjo izreka o implicitni funkciji pokažemo, da ta dopušča kompleksno sturkturo, kar pomeni, da postane Riemannova ploskev. Po drugi strani vsak torus, predstavljen kot kvocient $\mathbb{C}$ po mreži $\Lambda$ – diskretni podgrupi $\mathbb{C}$ izomorfni $\mathbb{Z}^2$, podeduje kompleksno strukturo preko kvocientne preslikave in tako pojasni imenovanje *kompleksni torus*. Izkaže se, da ti dve, bistveno različni konstrukciji, presenetljivo porodita enaka oz. izomorfna matematična objekta. To vez razložimo preko teorije dvojno periodičnih funkcij, imenovanih eliptične funkcije, in modularnih funkcij z mnogo simetrije, povezane z modularno grupo $\mathrm{SL}_2(\mathbb{Z})$. Obravnavamo njihove osnovne lastnosti in razvijemo teorijo Weierstrassove funkcije $\wp$, ki nam nazadnje omogoči eksplicitno podati omenjeni izomorfizem in dokazati uniformizacijski izrek, ki združuje oba objekta.


**Elliptic curves and complex tori**


Abstract

An *elliptic curve* over the field of complex numbers $\mathbb{C}$ is a nonsingular projective cubic, given by the Weierstrass equation. Using the implicit function theorem we show, that it admits a complex structure, which makes it a Riemann surface. On the other hand every torus, which we view as a quotient of $\mathbb{C}$ modulo a lattice $\Lambda$ – a discrete subgroup of $\mathbb{C}$ isomorphic to $\mathbb{Z}^2$, inherits a complex structure via its quotient map, which justifies us naming it *complex torus*. These two, vastly different constructions, remarkably turn out to yield the same i.e. isomorphic mathematical objects. This link is explained using the theory of doubly periodic functions, also called elliptic functions, and modular functions, which are meromorphic functions on the upper half plane enjoying many symmetries involving the modular group $\mathrm{SL}_2(\mathbb{Z})$. We discuss their basic properties and develop the necessary theory of the Weierstrass $\wp$-function, alowing us to explicitly construct the aforementioned isomorphism and prove the uniformizaton theorem, unifying both objects of study.



**Math. Subj. Class. (2020):** 11F03, 11G05, 14H52, 14H55

**Ključne besede:** eliptična krivulja, eliptična funkcija, kompleksni torus, Weierstrassova funkcija $\wp$, $j$-invarianta, modularna funkcija

**Keywords:** elliptic curve, elliptic function, complex torus, Weierstrass $\wp$-function, $j$-invariant, modular function

# 1. Uvod

Matematike pogosto zanimajo rešitve različnih enačb. Obstoj rešitev, kakšne lastnosti imajo in kako se obnašajo pod raznimi transformacijami. Osrednja tema moje naloge bo preučiti in ustvariti geometrijsko predstavo množice ničel kompleksnega polinoma tretje stopnje posebne oblike. To množico ničel si lahko predstavljamo kot realno ploskev in ji pravimo eliptična krivulja. Zgodovinsko je eliptična krivulja množica ničel enačbe

$$y^2 = x^3 + ax + b.$$

V tem delu pa se bomo ukvarjali z nekoliko prilagojeno – projektivno – obliko te enačbe. Množicam ničel polinomov več spremenljivk pravimo *algebraične krivulje* in z njimi bomo začeli v poglavju 2.

Pri iskanju rešitev polinomskih enačb se razmeroma hitro porodi vprašanje, iz katerega ambientnega prostora sploh sprejemamo veljavne rešitve. Spomnimo se fundametalnega izreka algebre, ki pravi, da ima vsak nekonstanten polinom s kompleksnimi koeficienti ničlo v polju kompleksnih števil, med tem ko brez težav poiščemo realne polinome, ki realnih ničel nimajo. Podobno situacijo imamo tukaj. Eliptične krivulje se namreč da študirati nad mnogo različnimi polji. Nad končnimi polji igrajo eliptične kriulje pomembno vlogo v kriptografiji, nad poljem racionalnih števil in njihovimi končnimi razširitvami – številskimi polji – pridejo do izraza v algebraični teoriji števil, mi pa jih bomo v tem delu gledali nad poljem kompleksnih števil.

V primeru obravnave nad poljem kompleksnih števil eliptične krivulje naravno pridobijo dodatno kompleksno stukturo in na ta način postanejo t. i. *Riemannove ploskve*. Ta struktura nam omogoči analizo holomorfnih funkcij na prostorih, ki niso nujno domene v kompleksni ravnini in jo bomo bolj podrobno raziskali v poglavju 4. Po drugi strani bomo toruse vpeljali kot kvocientne prostore kompleksne ravnine $\mathbb{C}$ po delovanju diskretne grupe izomorfne $\mathbb{Z}^2$. To delovanje bo na nek način dovolj regularno, da bo tako konstruirani kvocientni prostor prevzel ključne lokalne lastnosti kompleksne ravnine in nam tako olajšal definicijo kompleksne strukture in interpretacije holomorfnih funkcij na njem. Skupaj s to strukturo bomo ta kvocientni prostor imenovali kompleksni torus in izkazal se bo za najbolj primerno domeno t. i. *eliptičnih funkcij*. V osnovi so eliptične oz. dvojno periodične funkcije meromorfne funkcije z dvema periodama – v dveh realno linearno neodvisnih smereh v kompleksni ravnini. Njihove lastnosti in obnašanje si bomo ogledali v poglavju 3, ključno vlogo pa bo igrala prav posebna Weierstrassova eliptična funkcija $\wp$. Skupaj s svojim kompleksnim odvodom Weierstrassova funkcija $\wp$ zadošča enačbi

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3,$$

ki je po obliki presenetljivo podobna enačbi eliptične krivulje. Idejo, da je domena eliptične funkcije lahko kompleksni torus, na tem primeru interpretiramo kot dejstvo, da kompleksni torus in par funkcij $(\wp, \wp')$ parametrizira eliptično krivuljo podano z enačbo $y^2 = 4x^3 - g_2x - g_3$. Ta zveza nam bo nazadnje v poglavju 5 omogočila konstrukcijo preslikave, ki bo pokazala, da sta kompleksni torus in eliptična krivulja v nekem smislu enaka matematična objekta. Vsakemu kompleksnemu torusu bo tako pripadala neka eliptična krivulja, s pomočjo *modularnih funkcij* pa bomo pokazali še obrat, kako iz eliptične krivulje priti nazaj do kompleksnega torusa.

Vredno je še opomniti, da eliptične krivulje in področja, v katerih se uporabljajo, nimajo več vsebinsko praktično nič opravka z elipsami. Izkazalo se je, da so inverzi funkcij, s katermi računamo dolžine lokov elips, dvojno periodični, če jih gledamo kot funkcije kompleksne spremenljivke in od tod pride ime eliptičnih funkcij. V teh izračunih namreč integriramo izraze oblike $R(t, \sqrt{f(t)})$, kjer je $R \in \mathbb{C}(x, y)$ neka racionalna funkcija in $f$ polinom tretje ali četrte stopnje brez kvadratnih faktorjev. Ravno polinom $f$ pa se pod ustrezno uvedbo nove spremenljivke da transformirati v desno stran enačbe, ki podaja eliptično krivuljo.

## 2. Algebraične krivulje

Algebraične krivulje so množice ničel polinomov nad različnimi polji. V tem poglavju bomo začeli z afinimi algebraičnimi krivuljami, ki jih v nadaljevanju sicer ne bomo direktno potrebovali, bodo pa igrale pomembno vlogo pri razumevanju projektivnih algebraičnih krivulj, ki jih bomo vpeljali takoj za tem. Zaradi namenov tega dela, algebraičnih krivulj ne bomo obravnavali nad povsem splošnimi polji, pač pa se bomo omejili na polje kompleksnih števil, ki ga bomo označevali s $\mathbb{C}$. V smislu enodimenzionalnega kompleksnega prostora bomo množici kompleksnih števil pravili tudi kompleksna premica.

2.1. **Afine algebraične krivulje.** Naj $\mathbb{C}[x_1, \ldots, x_n]$ označuje kolobar polinomov $n$ spremenljivk s kompleksnimi koeficienti. Množica ničel poljubnega polinoma $f \in \mathbb{C}[x_1, \ldots, x_n]$ je

$$V(f) = \{p \in \mathbb{C}^n \mid f(p) = 0\} \subseteq \mathbb{C}^n.$$

**Definicija 2.1.** Množica $C \subseteq \mathbb{C}^2$ je *afina algebraična krivulja*, če obstaja tak nekonstanten polinom $f \in \mathbb{C}[x, y]$, da je

$$C = V(f).$$

Afine algebraične krivulje si lahko predstavljamo, kot nekaj podobnega ploskvam v prostoru $\mathbb{R}^4$, če naredimo identifikacijo $\mathbb{C} \equiv \mathbb{R}^2$. Dve kompleksni spremenljivki polinoma lahko zamenjamo s štirimi realnimi, prav tako pa tedaj tudi polinomska enačba $f(x, y) = 0$ razpade na dve realni. To sta

$$\operatorname{Re} f(x_1 + ix_2, y_1 + iy_2) = 0 \quad \text{in} \quad \operatorname{Im} f(x_1 + ix_2, y_1 + iy_2) = 0,$$

kjer so $x_1, x_2, y_1, y_2 \in \mathbb{R}$ realne spremenljivke. Pogoji, ki jim zadoščajo točke na afini algebraični krivulji $C \subseteq \mathbb{R}^4$, so zelo podobni tistim, ki definirajo gladke podmnogoterosti z glavno razliko, da gradienti teh definicijskih funkcij niso nujno (realno) linearno neodvisni. To bi bilo na $C$ razvidno kot samopresečišča ali osti, ki pa jih podmnogoterosti seveda nimajo.

V ta namen bi radi definirali singularne točke na afini algebraični krivulji $C = V(f)$ kot rešitve sistema enačb

$$\frac{\partial f}{\partial x}(x_0, y_0) = 0, \quad \frac{\partial f}{\partial y}(x_0, y_0) = 0, \quad f(x_0, y_0) = 0.$$

Toda ta definicija zaenkrat ni dobra, saj polinom $f \in \mathbb{C}[x, y]$ ni enolično določen s krivuljo $C$. Zato uvedemo pojem minimalnega polinoma krivulje $C$.

**Definicija 2.2.** Naj bo $C$ afina algebraična krivulja. *Minimalni polinom* krivulje $C$ je polinom $f \in C[x, y]$ najmanjše stopnje, za katerega velja $V(f) = C$.

**Opomba 2.3.** Če je $f$ minimalni polinom krivulje $C$, je to tudi $\alpha f$ za $\alpha \in \mathbb{C}^*$, saj je $V(f) = V(\alpha f)$. Minimalni polinomi afine algebraične krivulje se tako lahko razlikujejo za neničelno konstanto.

S pomočjo minimalnega polinoma krivulje, lahko sedaj definiramo singularne in regularne točke na njej.

**Definicija 2.4.** Naj bo $C$ afina algebraična krivulja in $f \in \mathbb{C}[x, y]$ njen minimalni polinom. Točka $(x_0, y_0) \in C$ je *regularna*, če velja

$$\frac{\partial f}{\partial x}(x_0, y_0) \neq 0 \quad \text{ali} \quad \frac{\partial f}{\partial y}(x_0, y_0) \neq 0,$$

in *singularna* sicer. Pravimo, da je afina algebraična krivulja *singularna*, če vsebuje kakšno singularno točko, in je *nesingularna* sicer.

**Primer 2.5.** Naj bo $f = x^2 + y^2 - 1$ in $g = (x^2 + y^2 - 1)^2$. Jasno je $V(f) = V(g)$, kar pomeni, da $f$ in $g$ določata isto algebraično krivuljo. Toda sistem

$$\frac{\partial f}{\partial x}(x, y) = 2x = 0, \quad \frac{\partial f}{\partial y}(x, y) = 2y = 0, \quad f(x, y) = 0 \tag{2.1}$$

nima nobene rešitve, sistem

$$\begin{aligned} \frac{\partial g}{\partial x}(x, y) &= 4x(x^2 + y^2 - 1) = 0, \\ \frac{\partial g}{\partial y}(x, y) &= 4y(x^2 + y^2 - 1) = 0, \\ g(x, y) &= 0 \end{aligned} \tag{2.2}$$

pa jih ima veliko. Namreč vsaka rešitev enačbe $f(x, y) = x^2 + y^2 - 1 = 0$ reši sistem (2.2), od koder bi lahko napačno sklepali, da je vsaka točka krivulje $V(f)$ singularna. Minimalni polinom opazovane krivulje je $f$ in iz sistema (2.1) vidimo, da singularnih točk nimamo, torej je krivulja nesingularna.

Definicija 2.4 nam omogoči formulirati prvo opazko.

**Trditev 2.6.** *Vsaka nesingularna afina algebraična krivulja $C \subseteq \mathbb{C}^2$ je z identifikacijo $\mathbb{C}^2 \equiv \mathbb{R}^4$ gladka 2-podmnogoterost oz. ploskev.*

*Dokaz.* Najprej se spomnimo definicije podmnogoterosti. Neprazna podmnožica $X \subseteq \mathbb{R}^{n+k}$ je *$n$-podmnogoterost* razreda gladkosti $\mathcal{C}^r$, za $r \in \{0, 1, \ldots, \infty, \omega\}$, če za vsako točko $x_0 \in X$ obstaja okolica $U \subseteq \mathbb{R}^{n+k}$ točke $x_0$ in t. i. definicijska funkcija $F : U \subseteq \mathbb{R}^{n+k} \to \mathbb{R}^k$ razreda $\mathcal{C}^r$ na $U$, da velja

(1) $X \cap U = F^{-1}(\{0\}) = \{x \in U \mid F(x) = 0\}$ in
(2) Jacobijeva matrika definicijske funkcije $F$ ima poln rang povsod na $X \cap U$, tj. $\operatorname{rang} JF(x) = k$ za vsak $x \in X \cap U$.

Številu $n$ pravimo *dimenzija* podmnogoterosti $X$, številu $k$ pa *kodimenzija.*

Sedaj poglejmo, da je pri nesingularnih afinih krivuljah tej definiciji zadoščeno. Definicijsko funkcijo imamo tokrat podano kar globalno na celotnem $\mathbb{R}^4$. Njeno vlogo igra minimalni polinom $f \in \mathbb{C}[x, y]$, ki podaja krivuljo $C = V(f)$. Polinom $f$ namesto kot funkcijo dveh kompleksnih spremenljivk interpretiramo kot funkcijo štirih realnih spremenljivk, njeno kodomeno, ki je $\mathbb{C}$, pa identificiramo z $\mathbb{R}^2$, tako da ločimo realni in imaginarni del funkcije $f(x_1+ix_2, y_1+iy_2) = u(x_1,x_2,y_1,y_2) + iv(x_1,x_2,y_1,y_2)$. Naj bo torej $g : \mathbb{R}^4 \to \mathbb{R}^2$ podana s predpisom

$$g(x_1,x_2,y_1,y_2) = (u(x_1,x_2,y_1,y_2), v(x_1,x_2,y_1,y_2)).$$

Jacobijeva matrika te preslikave je

$$Jg = \begin{pmatrix} u_{x_1} & u_{x_2} & u_{y_1} & u_{y_2} \\ v_{x_1} & v_{x_2} & v_{y_1} & v_{y_2} \end{pmatrix} = \begin{pmatrix} u_{x_1} & -v_{x_1} & u_{y_1} & -v_{y_1} \\ v_{x_1} & u_{x_1} & v_{y_1} & u_{y_1} \end{pmatrix},$$

kjer smo v drugi enakosti po $2 \times 2$ blokih upoštevali Cauchy-Riemannov sistem enačb, saj imamo opravka s polinomi, ki so kot funkcije holomorfni v obeh svojih kompleksnih spremenljivkah. Izračun

$$\frac{\partial f}{\partial x} = \frac{1}{2}\left(\frac{\partial f}{\partial x_1} - i\frac{\partial f}{\partial x_2}\right) = \frac{1}{2}(u_{x_1} + iv_{x_1} - iu_{x_2} + v_{x_2}) = u_{x_1} + iv_{x_1},$$

skupaj z analognim računom za $\frac{\partial f}{\partial y} = u_{y_1} + iv_{y_1}$, in predpostavko o nesingularnosti krivulje nam zagotovita, da je v vsaki točki na $C$ vsaj eno od števil $u_{x_1} + iv_{x_1}$ in $u_{y_1} + iv_{y_1}$ neničelno. Normi teh dveh števil sta ravno determinanti skrajnega levega oz. desnega $2 \times 2$ bloka matrike $Jg$, ki ima zato v vsaki točki iz $C$ poln rang. □

Ta trditev pove, katere od afinih algebraičnih krivulj ne le lokalno v okolici regularnih točk izgledajo kot ploskve, temveč tudi so zares ploskve.

Na tem mestu se pojavi manjša nejasnost, zakaj afine algebraične krivulje poimenovati ravno *krivulje*. V kontekstu realnih podmnogoterosti se sprva to poimenovanje res zdi malce neusklajeno, toda v okviru kompleksnih dimenzij ta terminologija postane smiselna. Če v definiciji podmnogoterosti namreč zgolj zamenjamo polje realnih števil s $\mathbb{C}$, se povedano bistveno ne spremeni. Še vedno ohranimo dejstvo, da število "linearno neodvisnih" enačb ustreza kodimenziji podmnogoterosti in analogno tudi dimenzija podmnogoterosti ustreza razliki (kompleksne) dimenzije ambientnega prostora in kodimenzije. V tem smislu so potem ti objekti, ki jih realno vidimo kot ploskve, zares tudi kompleksne 1-podmnogoterosti oziroma krivulje.

2.2. **Projektivne algebraične krivulje.** V tem razdelku bomo algebraične krivulje obravnavali še v projektivnem smislu. Definirali bomo kompleksno projektivno ravnino in krivulje v njej. Vpeljavo projektivne ravnine opravičujemo z mnogimi lepimi lastnostmi v povezavi s presečišči krivulj v njej, pa tudi z raznimi bolj topološkimi razlogi, kot so na primer kompaktnost algebraičnih krivulj.

Najprej bomo obravnavali kompleksno projektivno ravnino in njene lastnosti.

**Definicija 2.7.** *Kompleksen projektivni prostor* dimenzije $n$ je

$$\mathbb{P}^n_{\mathbb{C}} = (\mathbb{C}^{n+1} \setminus \{0\})/\langle v \sim \lambda v; \lambda \in \mathbb{C}^*\rangle.$$

Tukaj $\mathbb{C}^*$ označuje multiplikativno grupo kompleksnih števil oz. $\mathbb{C} \setminus \{0\}$. Pri tem bomo $\mathbb{P}^2_{\mathbb{C}}$ – kot projektiven prostor dimenzije 2 – imenovali *kompleksna projektivna ravnina*. Pridevnik kompleksna bomo v nadaljevanju pogosto izpustili.

**Primer 2.8.** Kompleksen projektiven prostor dimenzije 1 smo že srečali. To je *Riemannova sfera* $\widehat{\mathbb{C}} \equiv \mathbb{P}^1_{\mathbb{C}}$. Včasih jo bomo imenovali tudi (kompleksna) projektivna premica. Riemannova sfera ima sicer še nekoliko več strukture, ki smo jo zaenkrat pri projektivnih prostorih izpustili, a se bomo k njej vrnili v 4. poglavju o Riemannovih ploskvah.

Projektivni prostor si lahko predstavljamo kot množico vseh enodimenzionalnih vektorskih podprostorov v $\mathbb{C}^{n+1}$. Ti so v našem primeru vse kompleksne premice, ki potekajo skozi izhodišče. Vse točke na posamezni kompleksni premici brez izhodišča identificiramo, ta ekvivalenčni razred pa potem tvori eno samo točko projektivnega prostora. Vsak tak ekvivalenčni razred oz. točko v projektivnem prostoru predstavimo s t. i. homogenimi koordinatami. Poljuben $x = (x_0, \ldots, x_n) \in \mathbb{C}^{n+1} \setminus \{0\}$ je predstavnik ekvivalenčnega razreda $[x]_\sim = \{(\lambda x_0, \ldots, \lambda x_n) \in \mathbb{C}^{n+1} \mid \lambda \in \mathbb{C}^*\} \in \mathbb{P}^n_\mathbb{C}$, kar v homogenih koordinatah zapišemo z

$$[x]_\sim = [x_0 : \ldots : x_n]$$

in zanje velja

$$[x_0 : \ldots : x_n] = [\lambda x_0 : \ldots : \lambda x_n]$$

za poljuben $\lambda \in \mathbb{C}^*$.

**Opomba 2.9.** Projektivne prostore lahko opremimo tudi s topologijo, ki nam bo omogočila govoriti o zveznosti kvocientne projekcije

$$q : \mathbb{C}^{n+1} \setminus \{0\} \to \mathbb{P}^n_\mathbb{C}, \quad (x_0, \ldots, x_n) \mapsto [x_0 : \ldots : x_n]\,.$$

In sicer vzamemo za odprte množice v $\mathbb{P}^n_\mathbb{C}$ *natanko* tiste podmnožice $U \subseteq \mathbb{P}^n_\mathbb{C}$, za katere je $q^{-1}(U)$ odprta v $\mathbb{C}^{n+1} \setminus \{0\}$. Hkrati je to tudi največja topologija na $\mathbb{P}^n_\mathbb{C}$, za katero je projekcija $q$ še vedno zvezna. Tej topologiji pravimo *kvocientna topologija* in o njej lahko več izvemo v [7, poglavje 3.2].

*Komentar.* Projektivne prostore lahko ekvivalentno definiramo tudi kot prostore orbit (desnega) delovanja krožnice $S^1 \subseteq \mathbb{C}$ s skalarnim množenjem na kompleksni enotski sferi

$$S(\mathbb{C}^{n+1}) = \{v \in \mathbb{C}^{n+1} \mid \|v\| = 1\}.$$

Tedaj je

$$\mathbb{P}^n_\mathbb{C} \equiv S(\mathbb{C}^{n+1})/S^1.$$

Ker je kompleksna enotska sfera $S(\mathbb{C}^{n+1})$ kompakten 2-števen Hausdorffov prostor, je zaradi delovanja kompaktne krožnice $S^1$, tudi projektiven prostor $\mathbb{P}^n_\mathbb{C}$ kompakten 2-števen in Hausdorffov. Podrobnosti o tem lahko bralec najde v [7, zgled 3.43].

Za definicijo projektivnih algebraičnih krivulj potrebujemo polinome, ki so usklajeni s homogenostjo koordinat na $\mathbb{P}^2_\mathbb{C}$. To so t. i. *homogeni polinomi.* Polinom $F \in \mathbb{C}[x, y, z]$ stopnje $d = \deg F$ je *homogen*, če so vsi njegovi monomi stopnje $d$ oz. ekvivalentno, če za vsak $\lambda \in \mathbb{C}^*$ in vsak $(x, y, z) \in \mathbb{C}^3$ velja

$$F(\lambda x, \lambda y, \lambda z) = \lambda^d F(x, y, z).$$

Od tod opazimo tudi, da je zaradi tega pogoj $F(x, y, z) = 0$ neodvisen od izbire homogenih koordinat točke $[x : y : z]$, ki so zgolj neničelni skalarni večkratniki nekega predstavnika tega ekvivalenčnega razreda.

Zdaj lahko definiramo projektivne algebraične krivulje. Definicija se pričakovano ne bo drastično razlikovala od definicije afinih algebraičnih krivulj.

**Definicija 2.10.** Množica $C \subseteq \mathbb{P}^2_\mathbb{C}$ je *projektivna algebraična krivulja*, če obstaja tak nekonstanten homogen polinom $F \in \mathbb{C}[x, y, z]$, da je

$$C = V(F) = \{[x : y : z] \in \mathbb{P}^2_\mathbb{C} \mid F(x, y, z) = 0\}.$$

*Afini del* projektivne algebraične krivulje $C$ je afina algebraična krivulja, ki je množica ničel *dehomogeniziranega* polinoma $f = F(x, y, 1) \in \mathbb{C}[x, y]$, torej $V(f) \subseteq \mathbb{C}^2$.

Podobno kot v afinem primeru, želimo tudi tukaj govoriti o singularnih točkah na projektivnih krivuljah. Naj bo od tod dalje $F \in \mathbb{C}[x, y, z]$ homogeni polinom najnižje stopnje, da velja $V(F) = C$.

**Definicija 2.11.** Naj bo $C = V(F) \subseteq \mathbb{P}^2_{\mathbb{C}}$ projektivna algebraična krivulja. Točka $[x_0 : y_0 : z_0] \in C$ je *singularna*, če velja

$$\frac{\partial F}{\partial x}(x_0, y_0, z_0) = \frac{\partial F}{\partial y}(x_0, y_0, z_0) = \frac{\partial F}{\partial z}(x_0, y_0, z_0) = 0$$

in je *regularna* sicer. Projektivna algebraična krivulja je *singularna*, če vsebuje kakšno singularno točko, in je *nesingularna* sicer.

Najprej se prepičamo, da so vsi parcialni odvodi homogenega polinoma spet homogeni polinomi. Res, odvod poljubnega monoma po kateri koli spremenljivki, je bodisi 0 ali pa spet monom ene stopnje nižje. To nam zagotovi, da je definicija dobra.

Vidimo torej, da so singularne točke ravno rešitve sistema $F = \frac{\partial F}{\partial x} = \frac{\partial F}{\partial y} = \frac{\partial F}{\partial z} = 0$. Izkaže se, da je ena enačba tukaj odveč. To pove naslednja trditev, imenovana *Eulerjeva identiteta*.

**Trditev 2.12.** *Naj bo $F \in \mathbb{C}[x, y, z]$ homogen polinom stopnje $d$. Tedaj velja*

$$\frac{\partial F}{\partial x}(x, y, z)x + \frac{\partial F}{\partial y}(x, y, z)y + \frac{\partial F}{\partial z}(x, y, z)z = d \cdot F(x, y, z).$$

*Dokaz.* Ker je polinom $F$ homogen, velja

$$F(\lambda x, \lambda y, \lambda z) = \lambda^d F(x, y, z).$$

Če to enakost odvajamo po $\lambda$, dobimo

$$\frac{\partial F}{\partial x}(\lambda x, \lambda y, \lambda z)x + \frac{\partial F}{\partial y}(\lambda x, \lambda y, \lambda z)y + \frac{\partial F}{\partial z}(\lambda x, \lambda y, \lambda z)z = d\lambda^{d-1} F(x, y, z).$$

Nazadnje vstavimo $\lambda = 1$ in trditev sledi. □

Sedaj bi radi razvili način, kako malce bolj splošno ločiti projektivne krivulje. Razlikovanje vseh krivulj želimo reducirati zgolj na različne geometrijske karakteristike in nekaj parametrov. Projektivne krivulje bomo tako razlikovali do *projektivne ekvivalence* natančno. To nam bo v nadaljevanju omogočilo omejitev obravnave nesingularnih kubik na takšne, ki so podane s preprostejšimi polinomskimi enačbami. V ta namen najprej poglejmo, kaj so projektivne transformacije, ki nam bodo pri tem pomagale.

**Definicija 2.13.** Naj bo $(a_{ij}) = A \in \mathrm{GL}_3(\mathbb{C})$ obrnljiva kompleksna $3 \times 3$ matrika. *Projektivna transformacija* ali *projektivnost* je preslikava

$$\Phi : \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}},$$
$$[x : y : z] \mapsto [a_{11}x + a_{12}y + a_{13}z : a_{21}x + a_{22}y + a_{23}z : a_{31}x + a_{32}y + a_{33}z].$$

Projektivnost $\Phi$ je pravzaprav določena z linearno preslikavo $\mathcal{A}_\Phi : \mathbb{C}^3 \to \mathbb{C}^3$, ki predstavlja množenje z matriko $A$.

Nekoliko manj formalno projektivnost podamo tudi kot uvedbo novih spremenljivk

$$x = a_{11}X + a_{12}Y + a_{13}Z, \quad y = a_{21}X + a_{22}Y + a_{23}Z, \quad z = a_{31}X + a_{32}Y + a_{33}Z.$$

**Opomba 2.14.** (1) Analogno lahko definiramo projektivne transformacije tudi na več razsežnih projektivnih prostorih.

(2) S preslikavami te oblike na projektivni premici oz. Riemannovi sferi, smo se že srečali. Te so natanko *Möbiusove* ali *lomljene linearne preslikave*, ki tvorijo grupo (kompleksnih) avtomorfizmov Riemannove sfere.

$$\mathrm{Aut}(\widehat{\mathbb{C}}) = \left\{ z \mapsto \frac{az+b}{cz+d} \middle| a,b,c,d \in \mathbb{C} \text{ in } ad-bc \neq 0 \right\}.$$

Preslikavo $z \mapsto \frac{az+b}{cx+d}$ lahko namreč identificiramo s preslikavo

$$[x:y] \mapsto [ax+by : cx+dy]\,,$$

kjer ima vlogo točke $\infty \in \widehat{\mathbb{C}}$ projektivna točka $[0:1]$.

(3) Če definiramo kvocientno projekcijo $\pi : \mathbb{C}^3 \setminus \{0\} \to \mathbb{P}^2_{\mathbb{C}}$, ki točki $(x,y,z)$ priredi projektivno točko $[x:y:z]$, potem velja

$$\pi \circ \mathcal{A}_\Phi = \Phi \circ \pi.$$

Projektivne transformacije tvorijo grupo za kompozitum, ki je izomorfna grupi $\mathrm{PGL}_3(\mathbb{C}) = \mathrm{GL}_3(\mathbb{C})/\mathbb{C}^*$, posebej je $\mathrm{Aut}(\widehat{\mathbb{C}}) \cong \mathrm{PGL}_2(\mathbb{C})$. Več o tem lahko najdemo v [4, poglavje 11].

**Definicija 2.15.** Homogena polinoma $F, G \in \mathbb{C}[x,y,z]$ sta *projektivno ekvivalentna*, če obstajata taka projektivna transformacija $\Phi$ in $\lambda \in \mathbb{C}^*$, da velja

$$G = \lambda(F \circ \mathcal{A}_\Phi).$$

Če sta $F$ in $G$ minimalna polinoma projektivnih krivulj $C = V(F)$ in $C' = V(G)$, pravimo, da sta krivulji $C$ in $C'$ *projektivno ekvivalentni* ali *izomorfni kot projektivni algebraični krivulji*, kadar sta njuna minimalna polinoma projektivno ekvivalentna, tedaj označimo $C \cong C'$.

Projektivno ekvivalenco dveh krivulj lahko interpretiramo kot prehajanje med njunima minimalnima polinomoma z uvedbo novih spremenljivk.

**Zgled 2.16.** Naj bo $C = V(F)$ krivulja, podana s polinomom $F = y^2z - x^3 - x^2z$. Recimo, da bi se radi znebili kvadratnega člena $x^2z$ v polinomu $F$. Tedaj lahko vzamemo projektivnost

$$x = X - \frac{1}{3}Z, \quad y = Y, \quad z = Z,$$

ki krivuljo $C$ preslika na krivuljo $C' = V(G)$, podano s homogenim polinomom $G = Y^2Z - X^3 + \frac{1}{3}XZ^2 - \frac{2}{27}Z^3$.

**Trditev 2.17.** *Projektivna ekvivalenca je ekvivalenčna relacija na množici vseh projektivnih algebraičnih krivulj.*

*Dokaz.* Naj bodo $C, C', C'' \subseteq \mathbb{P}^2_{\mathbb{C}}$ projektivne algebraične krivulje in $F, G, H \in \mathbb{C}[x,y,z]$ njihovi minimalni polinomi.

Relacija je refleksivna. Za projektivnost vzamemo $\Phi = \mathrm{id}_{\mathbb{P}^2_{\mathbb{C}}}$ in konstanto $\lambda = 1$.

Denimo, da velja $C \cong C'$, torej je $G = \lambda(F \circ \mathcal{A}_\Phi)$ za neko projektivnost $\Phi$ in $\lambda \in \mathbb{C}^*$. Tedaj velja $F = \frac{1}{\lambda}(G \circ \mathcal{A}_\Phi^{-1})$. Ker je $\mathcal{A}_\Phi^{-1} = \mathcal{A}_{\Phi^{-1}}$, velja tudi $C' \cong C$, zato je relacija simetrična.

Denimo, da sta projektivno ekvivalentni krivulji $C$ in $C'$ ter $C'$ in $C''$. Tedaj imamo $G = \lambda(F \circ \mathcal{A}_\Phi)$ in $H = \mu(G \circ \mathcal{A}_\Psi)$. Od tod vidimo, da je $H = \mu\lambda(G \circ \mathcal{A}_\Phi \circ \mathcal{A}_\Psi)$.

Tako iz $\mathcal{A}_\Phi \circ \mathcal{A}_\Psi = \mathcal{A}_{\Phi\circ\Psi}$ sledi $C \cong C''$, torej je projektivna ekvivalenca tudi tranzitivna. □

Posebej bo za nas pomembno, da je projektivna ekvivalenca ekvivalenčna relacija na množici nesingularnih kubik, kot bomo videli v nadaljevanju.

**Trditev 2.18.** *Naj bosta $C, C' \subseteq \mathbb{P}^2_{\mathbb{C}}$ projektivno ekvivalentni krivulji. Tedaj je $C$ singularna natanko tedaj, ko je $C'$ singularna.*

*Dokaz.* Če sta $F$ in $G$ minimalna polinoma krivulj $C$ oz. $C'$, zaradi projektivne ekvivalence obstajata projektivnost $\Phi$ in $\lambda \in \mathbb{C}^*$, da je

$$G = \lambda(F \circ \mathcal{A}_\Phi). \tag{2.3}$$

Če je $C$ nesingularna, je $\left(\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}, \frac{\partial F}{\partial z}\right) \neq 0$ povsod na $\mathbb{C}^3 \setminus \{0\}$, torej z odvajanjem zveze 2.3 v točki $(x, y, z)$ in upoštevanjem Leibnitzovega pravila za odvajanje produkta dobimo

$$\left(\frac{\partial G}{\partial x}, \frac{\partial G}{\partial y}, \frac{\partial G}{\partial z}\right)_{(x,y,z)} = \lambda\left(\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}, \frac{\partial F}{\partial z}\right)_{\mathcal{A}_\Phi(x,y,z)} \cdot A,$$

produkt vrstice in matrike $A$, ki je konstantna Jacobijeva matrika linearne preslikave $\mathcal{A}_\Phi$. Vrstica $\left(\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}, \frac{\partial F}{\partial z}\right)_{\mathcal{A}_\Phi(x,y,z)}$ je po predpostavki neničelna, matrika $A$ pa obrnljiva, zato je njun produkt spet neničelna vrstica, torej je $\left(\frac{\partial G}{\partial x}, \frac{\partial G}{\partial y}, \frac{\partial G}{\partial z}\right)_{(x,y,z)} \neq 0$. □

Z drugimi besedami ta trditev pove, da projektivna ekvivalenca ohranja singularnost oz. nesingularnost krivulj. Izkaže se, da ohranja tudi mnoge druge pomembne geometrijske karakteristike, kot so tangente, prevoji, presečne večkratnosti, redi točk ipd., toda v tem delu o njih ne bomo podrobneje govorili. O tem lahko več izvemo v [4].

2.3. **Nesingularne kubike.** Začnimo z definicijo projektivne kubike.

**Definicija 2.19.** *Projektivna kubika* je projektivna algebraična krivulja v $\mathbb{P}^2_{\mathbb{C}}$, katere minimalni polinom je tretje stopnje. V splošnem je podana z enačbo

$$C: \quad ax^3 + by^3 + cz^3 + dx^2y + exy^2 + fx^2z + gy^2z + hxyz + ixz^2 + jyz^2 = 0$$

Pri izbirnem predmetu Algebraične krivulje smo spoznali popolno klasifikacijo projektivnih kubik do projektivne ekvivalence natančno. Najprej jih delimo na nesingularne in singularne, te pa dalje na nerazcepne in razcepne. Podrobneje se v to klasifikacijo ne bomo spuščali, bralec pa si lahko več o tem prebere v [4, poglavje 15]. Za nas bodo posebej zanimive nesingularne projektivne kubike, saj bomo te lahko preko projektivnosti zapisali v lepši obliki, ki jo bo lažje analizirati. Tej klasični obliki pravimo *Weierstrassova normalna forma* in v njej se enačba kubike glasi

$$y^2z = x^3 + \alpha xz^2 + \beta z^3. \tag{2.4}$$

Izkaže se, da ni vsaka kubika te oblike vedno tudi nesingularna. Za koeficienta $\alpha, \beta \in \mathbb{C}$ mora veljati posebna zveza, kar pove naslednja trditev.

**Trditev 2.20.** *Projektivna kubika $C \subseteq \mathbb{P}^2_{\mathbb{C}}$ podana v Weierstrassovi normalni formi*

$$C: \quad y^2z = x^3 + \alpha xz^2 + \beta z^3$$

*je nesingularna natanko tedaj, ko velja $4\alpha^3+27\beta^2 \neq 0$. Tedaj to krivuljo imenujemo* Weierstrassova kubika.

**Opomba 2.21.** Vrednost $-4\alpha^3 - 27\beta^2$ je med drugim diskriminanta kubičnega polinoma $x^3 + \alpha x + \beta$, ki nam pove, kako je z večkratnostjo njegovih ničel. Njena vrednost je enaka 0 natanko tedaj, ko ima ta polinom kakšno večkratno ničlo. To ime prevzamemo tudi v kontekstu kubik, kjer *diskriminanto Weierstrassove kubike* vpeljemo kot

$$\Delta = -16(4\alpha^3 + 27\beta^2).$$

Izkaže se, da je faktor 16 ugodno dodati za lepšo obliko računov v nadaljevanju.

*Dokaz.* Naj bo $F = y^2z - x^3 - \alpha xz^2 - \beta z^3$. Pokažimo, da obstaja singularna točka na $C$ natanko tedaj, ko je $4\alpha^3 + 27\beta^2 = 0$. To se bo zgodilo natanko tedaj, ko bo sistem

$$\begin{aligned} 0 &= \frac{\partial F}{\partial x}(x,y,z) = -3x^2 - \alpha z^2 \\ 0 &= \frac{\partial F}{\partial y}(x,y,z) = 2yz \\ 0 &= \frac{\partial F}{\partial z}(x,y,z) = y^2 - 2\alpha xz - 3\beta z^2 \end{aligned}$$

imel netrivialno rešitev. Če je $z = 0$, dobimo iz prve enačbe $x = 0$ in iz tretje $y = 0$. To niso koordinate nobene projektivne točke, zato lahko privzamemo $z \neq 0$. Druga enačba tedaj implicira $y = 0$, tretjo lahko zaradi $z \neq 0$ delimo z $z$ in tako skupaj dobimo

$$3x^2 + \alpha z^2 = 0 \quad \text{in} \quad 2\alpha x - 3\beta z = 0.$$

Za netrivialno rešitev tega sistema zadošča poiskati že netrivialno rešitev sistema

$$3x^2 + \alpha z^2 = 0 \quad \text{in} \quad (2\alpha x)^2 = (3\beta z)^2.$$

Ta sistem se v matrični obliki glasi

$$\begin{pmatrix} 3 & \alpha \\ 4\alpha^2 & -9\beta^2 \end{pmatrix} \begin{pmatrix} x^2 \\ z^2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

in ima netrivialno rešitev natanko tedaj, ko je determinanta sistema $-4\alpha^3 - 27\beta^2$ enaka 0. □

Naslednji rezultat – katerega dokaz sicer ni zahteven, a uporablja nekatere pojme, ki jih za nadaljevanje ne bomo potrebovali – bomo samo navedli brez dokaza. Zagotavlja nam, da se lahko brez škode za splošnost pri obravnavi nesingularnih kubik omejimo samo na tiste v Weierstrassovi normalni formi.

**Trditev 2.22** ([4, lemma 15.2]). *Vsaka nesingularna projektivna kubika je projektivno ekvivalentna neki nesingularni Weierstrassovi kubiki.*

Ob tej trditvi pa se porodi vprašanje, kako prosto izbiro imamo s koeficientoma $\alpha$ in $\beta$ iz $\mathbb{C}$, ali je ta izbira lahko enolična? Za odgovor na to vprašanje najprej opazimo, da sta Weierstrassovi kubiki

$$C: \quad y^2z = x^3 + \alpha xz^2 + \beta z^3 \quad \text{in} \quad C': \quad Y^2Z = X^3 + \alpha' XZ^2 + \beta' Z^3.$$

projektivno ekvivalentni, če velja, na primer $u^4\alpha' = \alpha$ in $u^6\beta' = \beta$ za neki $u \in \mathbb{C}^*$. Takrat imamo namreč projektivnost

$$\Phi : C \to C', \quad [x:y:z] \mapsto \left[u^2x : u^3y : z\right],$$

krajše zapisano

$$x = u^2 X, \quad y = u^3 Y, \quad z = Z,$$

ki identificira eno krivuljo z drugo. Ob tem se transformira tudi diskriminanta $u^{12}\Delta' = \Delta$. Naslednja lema pove, da je takšne oblike tudi vsaka projektivnost med dvema projektivno ekvivalentnima Weierstrassovima kubikama.

**Lema 2.23.** *Naj bosta $C, C'$ projektivno ekvivalentni Weierstrassovi kubiki kot zgoraj in $\Phi : C \to C'$ poljubna projektivnost med njima. Tedaj $\Phi$ fiksira točko $[0:1:0]$ in je oblike*

$$x = u^2 X, \quad y = u^3 Y, \quad z = Z, \tag{2.5}$$

*za neki $u \in \mathbb{C}^*$. Opazovane količine se tedaj transformirajo*

$$u^4 \alpha' = \alpha, \quad u^6 \beta' = \beta \quad \textit{in} \quad u^{12}\Delta' = \Delta. \tag{2.6}$$

*Dokaz.* Naj bosta $F = y^2z - x^3 - \alpha xz^2 - \beta z^3$ in $G = y^2z - x^3 - \alpha' xz^2 - \beta' z^3$ homogena polinoma, s katerima sta podani projektivno ekvivalentni krivulji $C$ in $C'$. Tedaj vemo, da je $G = \lambda(F \circ \mathcal{A}_\Phi)$ in naj bo $A$ matrika linearne preslikave $\mathcal{A}_\Phi$.

Najprej pokažimo, da projektivnost $\Phi$ fiksira točko $[0:1:0]$. Za elemente v matriki $A = (a_{ij})$ moramo torej pokazati $a_{12} = a_{32} = 0$ in $a_{22} \neq 0$.

- Če je $a_{12} \neq 0$, v polinomu $F(\mathcal{A}_\Phi(x,y,z))$ nastopa člen $x^2z$, ki ga na levi strani pri $G$ ni,
- podobno, če je $a_{32} \neq 0$, imamo v polinomu $F(\mathcal{A}_\Phi(x,y,z))$ člen $yz^2$, ki ga prav tako ni pri $G$.

Ker sta $a_{12}$, $a_{32} = 0$, mora biti $a_{22} \neq 0$, sicer bi v $A$ imeli stolpec poln ničel, kar bi bilo v nasprotju z obrnljivostjo $A$.

Sedaj v enačbo za $C$ oziroma polinom $\lambda F(x,y,z)$ vstavimo

$$x = a_{11}X + a_{13}Z, \quad y = a_{21}X + a_{22}Y + a_{23}Z, \quad z = a_{31}X + a_{33}Z$$

in primerjamo koeficiente pri istoležnih členih polinoma $G$. Dobimo sistem enačb.

$$\begin{aligned}
x^3: \quad -1 &= \lambda(-a_{11}^3 + a_{21}^2 a_{31} - a_{11}a_{31}^2\alpha - a_{31}^3\beta) \\
x^2y: \quad 0 &= \lambda(2a_{21}a_{22}a_{31}) \\
xy^2: \quad 0 &= \lambda(a_{22}^2 a_{31}) \\
x^2z: \quad 0 &= \lambda(3a_{11}^2 a_{31} + 2a_{21}a_{23}a_{31} + a_{21}^2 a_{33} - a_{31}^3\alpha - 2a_{11}a_{31}a_{33}\alpha - 3a_{31}^2 a_{33}\beta) \\
xyz: \quad 0 &= \lambda(2a_{22}a_{23}a_{31} + 2a_{21}a_{22}a_{33}) \\
y^2z: \quad 1 &= \lambda(a_{22}^2 a_{33}) \\
xz^2: \quad -\alpha' &= \lambda(a_{23}^2 a_{31} - 3a_{11}a_{31}^2 + 2a_{21}a_{23}a_{33} - 2a_{31}^2 a_{33}\alpha - a_{11}a_{33}^2\alpha - 3a_{31}a_{33}^2\beta) \\
yz^2: \quad 0 &= \lambda(2a_{22}a_{23}a_{33}) \\
z^3: \quad -\beta' &= \lambda(-a_{31}^3 + a_{23}^2 a_{33} - a_{31}a_{33}^2\alpha - a_{33}^3\beta)
\end{aligned}$$

Od tod sledi $a_{13}, a_{21}, a_{23}, a_{31} = 0$ in $a_{11}, a_{33} \neq 0$. Ob tem pa dobimo še zveze

$$a_{11}^3 = a_{33}a_{22}^2 = \lambda^{-1}, \quad \alpha' = \lambda a_{11}a_{33}^2\alpha, \quad \beta' = \lambda a_{33}^3\beta.$$

Ker vsi neničelni skalarni večkratniki matrike $A$ določajo isto projektivnost, lahko brez izgube splošnosti privzamemo $a_{33} = 1$. Če vzamemo $t \in \mathbb{C}^*$ poljuben, da velja $t^6 = \lambda^{-1}$, bo $a_{22}$ enak bodisi $t^3$, bodisi $-t^3$. Po potrebi lahko z menjavo $t \mapsto -t$ vedno dosežemo, da velja $a_{22} = t^3$. Iz zveze $a_{11}^3 = t^6$ pa sledi ena od naslednjih treh možnosti.

(i) Če je $a_{11} = t^2$, vzamimo $u = t$ in takrat je $a_{11} = u^2$ in $a_{22} = u^3$.
(ii) Če je $a_{11} = \rho t^2$, kjer je $\rho = e^{2\pi i/3}$ tretji primitivni koren enote, vzamemo $u = \rho^2 t$ in dobimo $a_{11} = u^2$ in $a_{22} = u^3$.
(iii) Če je $a_{11} = \rho^2 t^2$, vzamemo $u = \rho t$ in ob tem dobimo $a_{11} = u^2$ ter $a_{22} = u^3$.

Vedno lahko torej izberemo tak $u \in \mathbb{C}^*$, za katerega je $u^6 = \lambda^{-1}$, da velja

$$a_{11} = u^2, \quad a_{22} = u^3, \quad u^4\alpha' = \alpha, \quad u^6\beta' = \beta \quad \text{in} \quad u^{12}\Delta' = \Delta.$$

Projektivnost $\Phi$ je tedaj oblike

$$x = u^2 X, \quad y = u^3 Y, \quad z = Z. \qquad \square$$

Ugotovili smo, da lahko dva različna para koeficientov $\alpha, \beta \in \mathbb{C}$ podata projektivno ekvivalentni Weierstrassovi kubiki. Obstaja pa količina, ki se pri tovrstnih transformacijah ne spreminja – ostaja invariantna. Tej količini pravimo *$j$-invarianta* Weierstrassove kubike, oziroma pozneje, eliptične krivulje. Podana je kot

$$j = -1728(4\alpha)^3/\Delta = 1728\frac{4\alpha^3}{4\alpha^3 + 27\beta^2}.$$

Jasno je, da se pri transformaciji (2.5) iz prejšnje leme $j$-invarianta ohranja. To pokaže krajši račun

$$j = -1728(4\alpha)^3/\Delta = -1728(4u^4\alpha')^3/(u^{12}\Delta') = -1728(4\alpha')^3/\Delta' = j'.$$

Pozneje bomo videli, kako lahko $j$-invarianto gledamo tudi kot funkcijo kompleksne spremenljivke in tako malce pokomentirali izbiro faktorja 1728 pred celotno formulo.

Pomembna ugotovitev, ki je med drugim posledica algebraične zaprtosti polja kompleksnih števil, je naslednja.

**Trditev 2.24.** *Nesingularni projektivni Weierstrassovi kubiki sta projektivno ekvivalentni natanko tedaj, ko imata enaki $j$-invarianti.*

*Dokaz.* Implikacija v desno je jasna iz zgornjega premisleka in leme 2.23, preostane nam pokazati še implikacijo v levo.

Denimo, da imata Weierstrassovi kubiki

$$C: \quad y^2 z = x^3 + \alpha x z^2 + \beta z^3 \quad \text{in} \quad C': \quad Y^2 Z = X^3 + \alpha' X Z^2 + \beta' Z^3$$

enaki $j$-invarianti, torej, da velja

$$\frac{(4\alpha)^3}{4\alpha^3 + 27\beta^2} = \frac{(4\alpha')^3}{4\alpha'^3 + 27\beta'^2}.$$

To nam da

$$\alpha^3 \beta'^2 = \alpha'^3 \beta^2. \tag{2.7}$$

Sedaj iščemo projektivnost oblike $x = u^2 X$, $y = u^3 Y$, $z = Z$ za neki $u \in \mathbb{C}^*$. Ločimo tri primere.

(i) $\alpha = 0$. Tedaj mora biti $\beta \neq 0$, saj bi sicer $C$ bila singularna po trditvi 2.20. Od tod iz enačbe (2.7) sledi, da je $\alpha' = 0$ in zato je tudi $\beta' \neq 0$, sicer bi bila $C'$ singularna. Zadošča vzeti $u \in \mathbb{C}^*$, za katerega je $u^6 = \beta/\beta'$.
(ii) $\beta = 0$. Tedaj iz podobnih razlogov kot pri (i) dobimo $\alpha \neq 0$, $\beta' = 0$ in $\alpha' \neq 0$. Za $u \in \mathbb{C}^*$ zadošča vzeti rešitev enačbe $u^4 = \alpha/\alpha'$.

(iii) $\alpha\beta \neq 0$. Tedaj je tudi $\alpha'\beta' \neq 0$, namreč če bi eden od $\alpha'$, $\beta'$ bil ničeln, bi zaradi zveze (2.7) bil tudi drugi, kar bi bilo v nasprotju z nesingularnostjo krivulje $C'$. Opazimo, da takrat velja

$$\left(\frac{\alpha}{\alpha'}\right)^3 = \left(\frac{\beta}{\beta'}\right)^2$$

in za $u \in \mathbb{C}^*$ zadošča vzeti rešitev enačbe $u^{12} = (\alpha/\alpha')^3 = (\beta/\beta')^2$. □

Poleg tega pa $j$-invarianta v celoti popiše vse neizomorfne Weierstrassove kubike. Za poljuben $j_0 \in \mathbb{C}$ obstaja Weierstrassova kubika, ki ima $j_0$ za svojo $j$-invarianto. Če je $j_0 \neq 0, 1728$, želimo iz enačbe

$$j_0 = 1728 \frac{4\alpha^3}{4\alpha^3 + 27\beta^2}$$

izraziti koeficient $\alpha$, pri tem pa imamo svobodo zahtevati $\alpha = \beta$. Tedaj bo $\alpha = 27j_0/4(j_0 - 1728)$ in kubika podana z enačbo

$$y^2z = x^3 + \frac{27j_0}{4(j_0 - 1728)}xz^2 + \frac{27j_0}{4(j_0 - 1728)}z^3$$

ima $j$-invarianto enako $j_0$. V robnih primerih imamo

- pri $j_0 = 0$ kubiko z enačbo

$$y^2z = x^3 + z^3$$

- in pri $j_0 = 1728$ kubiko z enačbo

$$y^2z = x^3 + xz^2.$$

Koncept $j$-invariante lahko razširimo tudi do poljubne nesingularne projektivne kubike. Pripišemo ji $j$-invarianto njej projektivno ekvivalentne Weierstrassove kubike, ki nam jo zagotovi trditev 2.22. Tako prostor vseh nesingularnih kubik razpade na izomorfnostne razrede (glede na izomorfnost projektivnih algebraičnih krivulj oz. projektivno ekvivalenco), kjer je favorizirani predstavnik vsakega razreda neka nesingularna Weierstrassova kubika. Glede na to razširitev $j$-invariante na vse nesingularne projektivne kubike je jasno, da je $j$-invariantna kot funkcija nesingularnih projektivnih kubik na izomorfnostnih razredih konstantna. V tem smislu vidimo $j$-invarianto kot funkcijo

$$j : \{\text{nesingularne projektivne kubike}\} /_{\cong} \to \mathbb{C},$$

kjer $\cong$ označuje projektivno ekvivalenco projektivnih kubik. V tem smislu bomo z $j_C$ ali $j(C)$ označevali $j$-invarianto nesingularne projektivne kubike $C$ oz. $j$-invarianto njenega izomorfnostnega razreda.

Za konec tega poglavja bomo podali še definicijo eliptične krivulje nad $\mathbb{C}$. Ta se za naše namene praktično ne bo razlikovala od običajne nesingularne Weierstrassove kubike, ki smo jo obravnavali v tem razdelku 2.3. Zaradi večje abstraktnosti standardne definicije eliptične krivulje, kot jo podaja Silverman [9, III. §3], in naših potreb v nadaljevanju, eliptične kriulje vpeljemo nekoliko enostavnje. Presenetljivo pa je naša definicija ekvivalenta standardni, le da za to potrebujemo Riemann–Rochov izrek, ki je izven dosega tega dela.

**Definicija 2.25.** Nesingularna projektivna kubika $E(\mathbb{C})$ ali samo $E$ skupaj s t. i. *izhodiščem* $O \in E(\mathbb{C})$ na njej, ki ga pogosto eksplicitno ne omenjamo, se imenuje *eliptična krivulja* nad poljem $\mathbb{C}$.

**Opomba 2.26.** (1) Ker nas bodo v nadaljevanju eliptične krivulje zanimale zgolj do projektivne ekvivalence natančno, bomo lahko brez škode za splošnost po trditvi 2.22 zahtevali, da je eliptična krivulja podana z enačbo v Weierstrassovi obliki

$$E: \quad y^2z = x^3 + \alpha xz^2 + \beta z^3, \quad \text{kjer je} \quad 4\alpha^3 + 27\beta^2 \neq 0.$$

(2) Zaradi kompletnosti smo v definicijo eliptične krivulje vključili še izbiro izhodišča, ki igra vlogo neutralnega elementa, potem ko eliptično krivuljo opremimo z grupno strukturo. Za lažje računanje se za izhodišče izbere enega od devetih prevojev, ki je najpogosteje točka v neskončnosti $[0 : 1 : 0]$.

(3) Morda smo nekoliko nepotrebno poudarjali, da je naša eliptična krivulja definirana nad poljem kompleksnih števil. Oznaka $E(\mathbb{C})$ pove, da opazujemo točke na krivulji s koordinatami iz $\mathbb{C}$, lahko pa bi se recimo omejili samo na tiste, ki v homogenih koordinatah premorejo predstavnika s samimi racionalnimi komponentami, in takrat pisali $E(\mathbb{Q})$. V splošnem se eliptične krivulje obravnava nad poljubnim poljem, kjer pride do izraza njegova karakterisika, ali je algebraično zaprto ipd. V našem primeru nad $\mathbb{C}$ takšnih skrbi ne bomo imeli.

V nadaljevanju bo ugodneje namesto *klasične* Weierstrassove oblike nesingularne kubike (2.4) obravnavati malenkost prilagojeno – še vedno pa projektivno ekvivalentno obliko

$$y^2z = 4x^3 - axz^2 - bz^3.$$

Med to in klasično različico enostavno prehajamo preko projektivnosti

$$x = tX, \quad y = Y, \quad z = Z, \qquad \text{kjer za } t \in \mathbb{C}^* \text{ velja } t^3 = 4.$$

Osnovne količine se tedaj povežejo preko enakosti

$$a = -t\alpha, \quad b = -\beta,$$

diskriminanta in $j$-invarianta pa se v koeficientih $a$ in $b$ izražata kot

$$\Delta = 16(a^3 - 27b^2) \quad \text{in} \quad j = 1728\frac{a^3}{a^3 - 27b^2}. \tag{2.8}$$

## 3. Eliptične funkcije

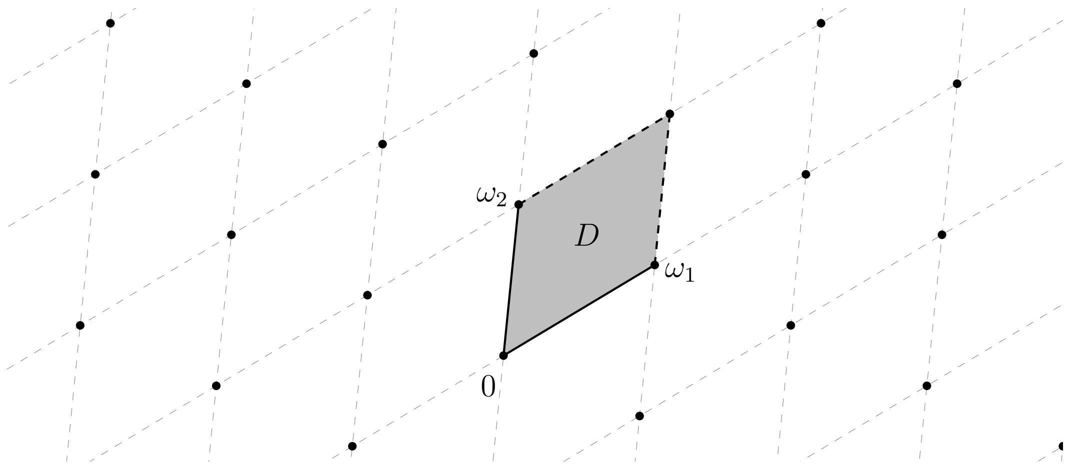
Glavna vez med eliptičnimi krivuljami in kompleksnimi torusi so t. i. *eliptične funkcije*. Da jih vpeljemo, najprej potrebujemo nekaj novih pojmov.

**Definicija 3.1.** 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 $\mathbb{R}$-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 $\Lambda$ 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 $\Lambda$. Pripadajoča kvocientna projekcija bo $\pi : \mathbb{C} \to \mathbb{C}/_\sim$. Kvocient $\mathbb{C}/_\sim$ bomo od tod dalje rajši označevali s $\mathbb{C}/\Lambda$.

Zaenkrat bomo $\mathbb{C}/\Lambda$ razumeli zgolj kot kvocientno množico, kasneje pa ga bomo opremili s topologijo, ki nam bo razkrila, da je ta prostor v resnici homeomorfen torusu. Za tem bomo definirali še kompleksno strukturo, ki nam bo na njem omogočila definirati holomorfne preslikave.

**Definicija 3.2.** *Fundamentalni paralelogram* za mrežo $\Lambda = \langle \omega_1, \omega_2 \rangle$ je

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

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

**Opomba 3.3.** Kadar bomo govorili o fundamentalnih paralelogramih pogosto, izbira izhodišča $\alpha$ 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 3.4.** *Poljuben translat $z + \Lambda$ mreže $\Lambda \subseteq \mathbb{C}$ ima natanko enega predstavnika v fundamentalnem paralelogramu $D_\alpha$.*

*Dokaz.* Ker sta osnovni periodi $\omega_1, \omega_2$ $\mathbb{R}$-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

$$t_i = a_i - \lfloor a_i \rfloor \in [0, 1),$$

za $i \in \{1, 2\}$, kjer $\lfloor x \rfloor$ označuje največje celo število, ki ni večje od $x$, velja $\alpha + t_1\omega_1 + t_2\omega_2 = z - \lfloor a_1 \rfloor\omega_1 - \lfloor a_2 \rfloor\omega_2 \in D_\alpha \cap (z + \Lambda)$. $\square$

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

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

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

**Definicija 3.5.** 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 $\Lambda$, pravimo, da je $\Lambda$-*periodična*. Polje $\Lambda$-periodičnih funkcij označimo s $\mathbb{C}(\Lambda)$.

3.1. **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 [5, izrek 59].

**Izrek 3.6.** *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 3.4 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 [7, trditev 2.22]. Zvezna funkcija $f$ je na kompaktu $\overline{D}$ omejena, kot eliptična funkcija pa je tako omejena na celotnem $\mathbb{C}$ [7, posledica 2.28]. Funkcija $f$ je torej omejena in cela holomorfna, zato je po Liouvillovem izreku konstantna. □

**Opomba 3.7.** Enako lahko sklepamo tudi, če $f$ nima ničel. Tedaj je $1/f$ cela eliptična funkcija, ko jo v polih $f$ razširimo z 0.

**Lema 3.8.** *Naj bo $f \in \mathbb{C}(\Lambda)$ eliptična funkcija. Tedaj je tudi njen odvod $f' \in \mathbb{C}(\Lambda)$ 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 je v točki $z \in \mathbb{C}$ pol, pa ima tudi $f'$ v tej točki pol, torej pogoj za eliptičnost velja povsod na $\mathbb{C}$ in tako je $f' \in \mathbb{C}(\Lambda)$. □

Vpeljimo nekaj notacije, ki jo bomo potrebovali v naslednjih izrekih. Če je $f$ meromorfna funkcija na odprti domeni $\Omega \subseteq \mathbb{C}$, pravimo, da ima $f$ *red* $m \in \mathbb{Z}$ v točki $z_0 \in \Omega$, če obstaja okolica $U \subseteq \Omega$ 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 $z_0 \in \Omega$, 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 3.9.** *Naj bo $f \in \mathbb{C}(\Lambda)$ eliptična funkcija in $D$ fundamentalni paralelogram glede na mrežo $\Lambda$, katerega rob $\partial D$ ne vsebuje polov ali ničel $f$. Tedaj velja*

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

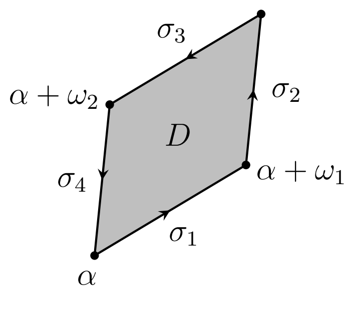
(*ii*)
$$\sum_{w \in D} \operatorname{ord}_w(f) = 0$$

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

*Dokaz.* (*i*) Uporabimo izrek o ostankih [5, 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.




Slika 2. Fundamentalni paralelogram.

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 periodičnosti $f$ in orientacije obeh parov nasprotnih stranic ($\sigma_1$ in $\sigma_3$ ter $\sigma_2$ in $\sigma_4$) razvidno, da se integrala po parih nasproti ležečih stranic izničita, kar nam da želeni rezultat 0.

(*ii*) Po lemi 3.8 je $f' \in \mathbb{C}(\Lambda)$, zato je tudi kvocient $f'/f$ eliptičen. Tedaj velja

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

kjer smo v prvi enakosti uporabili princip argumenta [5, izrek 72], druga enakost pa je identiteta $(i)$, 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 $(i)$ 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 $\sigma_1$ vidimo

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

Podobno z uvedbo nove spremenljivke $w = z + \omega_1$ storimo z integralom po stranici $\sigma_4$ 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 $\gamma$ okoli 0 in nam pove, kolikokrat se krivulja $\gamma$ ovije okoli izhodišča. Podrobnosti o tem lahko bralec najde v [1, 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

$\sigma_4$ točki $\alpha$ 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 $t \mapsto f(\alpha + t\omega_2)$. Opomnimo še, da to ni nujno parametrizacija krivulje v običajnem smislu, saj je lahko neinjektivna.

Zapišemo lahko

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

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

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

**Opomba 3.10.** (1) 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 $\Omega$, ki se ujemata na množici s stekališčem v $\Omega$, ujemata povsod na $\Omega$.

(2) Kot nakazuje izrek, je izbira fundamentalnega paralelograma irelevantna, dokler ta izpolnjuje določene predpostavke o robu. Kljub temu pa se prepričajmo, da lahko vselej takšen fundamentalni paralelogram vedno izberemo.

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 $\partial D$ 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 $f$.

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

**Definicija 3.11.** *Red* eliptične funkcije je število polov šteto z večkratnostjo v zaprtju fundamentalnega paralelograma.

Tudi če pol $z_0$ leži na robu $\partial D$ izbranega fundamentalnega paralelograma, lahko govorimo o redu tega pola v $D$. Takrat štejemo *red pola $z_0$ v $D$* kot $\frac{1}{2}\mathrm{ord}_{z_0}(f)$, če pol ni eno od štirih oglišč, oziroma, v primeru, ko je pol $z_0$ oglišče paralelograma, vzamemo za njegov red vrednost

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

Ob tem $\ell$ 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 $\mathrm{ord}_{z_0}(f)$.

**Zgled 3.12.** 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, $\rho$ in $1+\rho$. Naj bo $f$ eliptična funkcija s poli v mreži $\Lambda$. Tedaj bo red pola 0 za $f$ v $D$ enak

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

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

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

saj stranici, ki se srečata v $\rho$, skupaj oklepata kot velikosti $\pi/3$.

**Posledica 3.13.** *Nekonstantna eliptična funkcija ima red vsaj* 2.

*Dokaz.* Brez škode za splošnost denimo, da je $f \in \mathbb{C}(\Lambda)$ nekonstantna eliptična funkcija z enim (enostavnim) polom $z_0$ na fundamentalni domeni $D$, saj po izreku 3.6 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 $\partial D$ tako dobimo neničelni residuum

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

To pa je v nasprotju s formulo $(i)$ iz izreka 3.9, ki pove, da je ta residuum – kot edini člen v vsoti – enak nič. □

**Posledica 3.14.** *Nekonstantna eliptična funkcija* $f : \mathbb{C} \to \widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ *je surjektivna.*

*Dokaz.* Ker je $f \in \mathbb{C}(\Lambda)$ nekonstantna, ima po izreku 3.6 pol in lahko zato rečemo, da tam doseže točko $\infty$. 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 že $f$ in prištevanje konstante na ti dve lastnosti nima vpliva. Po opombi 3.10 (3) ima $g$ ničlo v $\mathbb{C}$, kar pokaže željeno. □

3.2. **Weierstrassova funkcija $\wp$.** Osrednja tema tega poglavja, ki bo povezala eliptične krivulje s kompleksnimi torusi in za katero je bilo potrebno razvijati teorijo v prejšnjem razdelku, bo najprej definicija nato pa pregled lastnosti t. i. *Weierstrassove funkcije* $\wp$.

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

**Definicija 3.15.** Za naravno število $k > 2$ je *Eisensteinova vrsta reda* $k$ podana kot

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

**Opomba 3.16.** Opazimo, da za lihe $k$ velja $G_k(\Lambda) = 0$, saj se člena pri $\omega$ in $-\omega$ v vsoti odštejeta.

**Lema 3.17.** *Za vsako naravno 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 3.18.** *Za vsako naravno 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 $\Lambda'$. 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 $\epsilon$ izberemo najmanjšega izmed $\epsilon_\omega$ 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 3.17) 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 kompaktih.

**Izrek 3.19** ([5, 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 $\Omega$ konvergira k limitni funkciji $f$. Tedaj je tudi $f$ holomorfna na $\Omega$ in zaporedje odvodov $(f_n')_{n\in\mathbb{N}}$ konvergira enakomerno po kompaktih v $\Omega$ 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 3.18 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 3.19. 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 $\omega_0$ 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 $\omega_0$ prispeva samo člen $(z-\omega_0)^{-k}$, vrsta, ki ostane, pa je zaradi leme 3.18 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 3.20.** 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 $\Lambda$, ki samo premeša vrstni red seštevanja v zadnji (absolutno konvergentni) vrsti.

Funkcija iz primera 3.20 ima v vsaki periodi $\omega \in \Lambda$ pol stopnje 3 oziroma na fundamentalnem paralelogramu ima natanko pol stopnje 3, torej lahko rečemo, da je eliptična funkcija reda 3. Posledica 3.13 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 3.21.** *Weierstrassova eliptična funkcija* $\wp$ glede na mrežo $\Lambda$ 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 $\Lambda$, pišemo tudi $\wp_\Lambda$.

**Trditev 3.22.** *Za Weierstrassovo funkcijo $\wp$ glede na mrežo $\Lambda$ veljajo naslednje trditve.*

*(i) Vrsta, ki predstavlja 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 $\Lambda$-periodična.*

*(iv) točke iz mreže $\Lambda$ 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 3.18 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 3.17) 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 $\mathbb{C} \setminus \Lambda$. Po izreku 3.19 je limitna funkcija zaporedja – tj. Weierstrassova funkcija $\wp$ – holomorfna na $\mathbb{C} \setminus \Lambda$, vrsto pa lahko odvajamo členoma, kar pomeni, da je odvod funkcije $\wp$ enak

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

(*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*) Naj bo $\omega \in \Lambda$ poljuben. Kot smo se prepričali v primeru 3.20, je $\wp'$ eliptična funkcija, 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 v obe vstavimo $z = -\frac{\omega}{2}$ in upoštevamo sodost funkcije $\wp$, vidimo, da je ta konstanta enaka 0, kar pokaže želeno.

(*iv*) Zaradi $\Lambda$-periodičnosti funkcije $\wp$ po trditvi (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 $z^{-2}$. Ta nam da pol reda 2 z residuujem 0, preostanek vrste pa po dokazu trditve (i) na tej prebodeni okolici definira holomorfno funkcijo, ki na glavni del nima vpliva. $\square$

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

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}(\Lambda)z^{2k}, \tag{3.1}$$

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

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

$$\frac{1}{(1-x)^2} = \sum_{n=0}^{\infty}(n+1)x^n \quad \text{za } |x| < 1$$

in ta konvergenca je enakomerna in absolutna na kompaktih v disku $\Delta(0,1)$. 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 ničelne. $\square$

**Izrek 3.24.** *Weierstrassova eliptična funkcija $\wp$ glede na mrežo $\Lambda$ zadošča enačbi*

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda), \tag{3.2}$$

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

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

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

$$\psi(z) = 0 \cdot \frac{1}{z^6} + 0 \cdot \frac{1}{z^2} + 0 + (216G_4(\Lambda)^2 - 84G_8(\Lambda))z^2 + \cdots . \tag{3.3}$$

Funkcija $\psi$ tako nima glavnega dela pri 0 in je zato na okolici $U$ holomorfna. Zaradi $\Lambda$-periodičnosti je holomorfna tudi na okolici poljubne periode $\omega \in \Lambda$. Ker je $\psi$ meromorfna na $\mathbb{C}$ in brez polov, je v resnici cela eliptična funkcija, kot takšna pa je po izreku 3.6 konstantna. Preostane le še ugotoviti, kateri konstanti je enaka. Iz razvoja (3.3) takoj sledi, da je ta konstanta 0, ko vanjo vstavimo vrednost 0, to pa tudi zaključi dokaz izreka. □

Izrek 3.24 namiguje, da lahko s poljubno mrežo $\Lambda$ definiramo eliptično krivuljo

$$E_\Lambda : \quad y^2z = 4x^3 - g_2(\Lambda)xz^2 - g_3(\Lambda)z^3. \tag{3.4}$$

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. V ta namen dokažimo naslednji dve lemi.

**Lema 3.25.** *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 3.22 (ii), vemo, da je njen odvod $\wp'$ liha funkcija. Tako lahko za $2z \in \Lambda$ upoštevajoč $\Lambda$-periodičnost funkcije $\wp'$ 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 3.20, je $\wp'$ eliptična funkcija reda 3, zato razen treh naštetih polperiod, ki predstavljajo enostavne ničle, po izreku 3.9 (ii) drugih ničel na fundamentalnem paralelogramu ni. □

**Lema 3.26.** *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 $f = 4x^3 - g_2x - g_3$ 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 $\Lambda$ 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 3.25 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 (3.2) vstavimo osnovne tri polperiode $r_1$, $r_2$ in $r_3$.

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

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

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 $\Lambda$. Očitno je $r_i$ njena ničla, ki pa mora biti reda 2, saj je tudi ničla odvoda $h_i' = \wp'$ po lemi 3.25. To pomeni, da na fundamentalnem paralelogramu drugih ničel nima. Od to 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 [2]. □

Poljubni mreži $\Lambda \subseteq \mathbb{C}$ lahko torej priredimo eliptično krivuljo $E_\Lambda$, podano z enačbo (3.4). Tako smo pokazali pomemben del sklepnega izreka te naloge. To razmišljanje bomo nadaljevali v poglavju 5, kjer se bomo lotili še obrata – kako iz eliptične krivulje priti do mreže in vse skupaj povzeli v uniformizacijskem izreku.

## 4. Kompleksna struktura in holomorfne preslikave

Pri kompleksni analizi smo spoznali načine, kako definirati kompleksni logaritem in kompleksni koren dane funkcije, pri tem pa je bilo ključno predpostaviti, da delamo na zvezdastem območju (splošneje *enostavno povezanem*[1]), na katerem funkcija nima ničel. Oglejmo si primer kvadratnega korena.

Kvadratni koren kompleksnega števila $z$ vedno obstaja in sta običajno dva (razen, ko je $z = 0$). To sta ravno ničli polinoma $w^2 - z \in \mathbb{C}[w]$, ki se razlikujeta natanko za predznak, in vedno obstajata po osnovnem izreku algebre. Vsakemu $z \in \mathbb{C}$ lahko torej priredimo enega od teh korenov. Vprašanje, ki se porodi, pa je: ali lahko to storimo zvezno? Izkaže se, da je lokalno to mogoče globalno, na celotnem $\mathbb{C}$, pa ni. Če bi namreč potovali vzdolž enotske krožnice v $\mathbb{C}$, bi po končanem obhodu ugotovili, da se vrednost, v kateri smo končali, od tiste, v kateri smo začeli, razlikuje natanko za predznak. To je razvidno takoj, ko opazimo, da kvadratni koren številu na enotski krožnici razpolovi argument. Edina možna maksimalna domena v $\mathbb{C}$, na kateri obstaja zvezen (holomorfen) kvadratni koren, je tako $\mathbb{C}$ brez nekega poltraka skozi izhodišče, kot je na primer $\mathbb{C} \setminus (-\infty, 0]$.

Popolnoma vzporedno bi lahko za kvadratni koren oklicali tudi z $-1$ pomnoženo prejšnjo funkcijo in tako dobili dve t. i. *veji* kvadratnega korena, ki sta popolnoma enakovredni in pogosto od nas zahtevata izbiro ene izmed njiju.

En način, kako bi se tej izbiri lahko izognili, je, da njuni domeni zamenjamo s krivuljo $X = \{(z, w) \in \mathbb{C}^2 \mid w^2 = z\}$, ki je v bistvu unija grafov obeh vej, kvadratni

[1]Enostavno povezana območja v ravnini si predstavljamo kot območja brez lukenj. Kolobar $\{z \in \mathbb{C} \mid r_1 < |z| < r_2\}$ in prebodena ravnina $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ nista enostavno povezana, enotski disk $\Delta$ pa je.

koren pa interpretiramo kot projekcijo iz $X$ na $w$-os, tj. $(z, w) \mapsto w$. Tako se izognemo tej nekanonični izbiri veje, a smo s tem zašli v nov problem. Izgubili smo poznano predstavo holomorfnih funkcij na tej domeni, ki sedaj ni več neka odprta množica v $\mathbb{C}$. Na srečo pa imamo še vedno upanje povrniti to informacijo, saj lahko množico $X$ lokalno sploščimo in identificiramo z neko odprto množico v $\mathbb{C}$. Če znamo takšne lokalne identifikacije najti na celotnem $X$ in to storimo na nekakšen usklajen način, bo nastala struktura dopuščala razviti definicijo, ki opredeljuje holomorfne funkcije na $X$ in nam omogoča prilagoditi določene izreke o odprtih domenah v $\mathbb{C}$ na te abstraktne objekte, ki jih imenujemo *Riemannove ploskve.*

Iz tega in podobnih principov se je razvila teorija Riemannovih ploskev. Osnovne ideje in rezultate povezane z njo si bomo s pogledom, usmerjenim na eliptične krivulje in toruse, ogledali v tem poglavju.

## 4.1. **Definicije in lastnosti.**

**Definicija 4.1.** *Riemannova ploskev* je povezan 2-števen Hausdorffov topološki prostor $X$, opremljen z družino *lokalnih kart* $((U_i, \varphi_i))_{i \in I}$, ki ji pravimo *kompleksni atlas*, kadar zanjo velja

(i) $(U_i)_{i \in I}$ je odprto pokritje za $X$.

(ii) Preslikava $\varphi_i : U_i \to U_i' \subseteq \mathbb{C}$ je homeomorfizem med okolico $U_i \subseteq X$ in neko odprto podmnožico $U_i' \subseteq \mathbb{C}$. Njenemu inverzu pravimo *lokalna parametrizacija.*

(iii) Za poljubna $i, j \in I$ je t. i. *prehodna preslikava*

$$\varphi_{ij} = \varphi_i \circ \varphi_j^{-1} : \varphi_j(U_i \cap U_j) \longrightarrow \varphi_i(U_i \cap U_j)$$

holomorfna na odprti množici $\varphi_j(U_i \cap U_j) \subseteq \mathbb{C}$. Temu pogoju pravimo *kompatibilnostni pogoj.*

**Opomba 4.2.** Za vsako lokalno karto $(U, \varphi)$ iz danega kompleksnega atlasa bo zožitev $\varphi|_V$ na poljubno manjšo odprto podmnožico $V \subseteq U$ še vedno lokalna karta, kompatibilna z vsemi drugimi iz danega kompleksnega atlasa. Zato lahko v nadaljevanju po potrebi izbiramo lokalne karte, definirane na poljubno majhnih odprtih množicah v $X$.

**Primer 4.3.** Kompleksna ravnina $\mathbb{C}$ je Riemannova ploskev, podana z eno samo lokalno karto $(\mathbb{C}, \mathrm{id}_{\mathbb{C}})$.

**Primer 4.4.** Poljubna odprta podmnožica $Y$ Riemannove ploskve $X$ je tudi Riemannova ploskev. Če je $((U_i, \varphi_i))_{i \in I}$ kompleksni atlas za $X$, potem vzamemo družino $((U_i \cap Y, \varphi_i|_{U_i \cap Y}))_{i \in I}$ za kompleksni atlas na $Y \subseteq X$. Res, $(U_i \cap Y)_{i \in I}$ je odprto pokritje za $Y$, zožitve $\varphi_i|_{U_i \cap Y}$ so še vedno homeomorfizmi, morda nekoliko manjših okolic, vse zožitve prehodnih preslikav pa so tudi same holomorfne, spet morda na kakšnih manjših odprtih okolicah.

**Primer 4.5.** Prvi nekoliko bolj zanimiv primer Riemannove ploskve je Riemannova sfera $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$. Topološko gledano je $\widehat{\mathbb{C}}$ kompaktifikacija z eno točko kompleksne ravnine $\mathbb{C}$, torej homeomorfna sferi $S^2$. Bazo odprtih okolic poljubne točke $z \in \mathbb{C} \subseteq \widehat{\mathbb{C}}$ tvorijo odprti diski oblike $\Delta(z, r)$ za $r > 0$, bazo odprtih okolic točke $\infty \in \widehat{\mathbb{C}}$ pa sestavljajo komplementi zaprtih diskov s središčem v izhodišču $\widehat{\mathbb{C}} \setminus \overline{\Delta(0, r)}$. Glede na to topologijo je preslikava

$$\varphi : \widehat{\mathbb{C}} \setminus \{0\} \to \mathbb{C}, \quad z \mapsto \frac{1}{z}$$

homeomorfizem, kjer ob tem razumemo $\frac{1}{\infty} = 0$. Res, okoli vsake točke iz $\mathbb{C}^*$ je $\varphi$ zvezna in ima inverz podan z istim predpisom, ki je tudi zvezen, pri točki $\infty$ pa $\varphi$ odprte bazne okolice $\widehat{\mathbb{C}} \setminus \overline{\Delta(0,r)}$ bijektivno slika ravno v odprte diske $\Delta(0, \frac{1}{r})$, torej je pri $\infty$ zvezna in odprta, kar pomeni, da je homeomorfizem med $\widehat{\mathbb{C}} \setminus \{0\}$ in $\mathbb{C}^*$.

Za atlas na $\widehat{\mathbb{C}}$ se nam tako ponujata dve karti $(\mathbb{C}, \mathrm{id}_{\mathbb{C}})$ in $(\widehat{\mathbb{C}} \setminus \{0\}, \varphi)$. Množici $\mathbb{C}$ in $\widehat{\mathbb{C}} \setminus \{0\}$ tvorita odprto pokritje za $\widehat{\mathbb{C}}$, preslikavi $\mathrm{id}_{\mathbb{C}}$ in $\varphi$ pa sta homeomorfizma, ki zadoščata kompatibilnostnemu pogoju, saj je na njunem preseku $\mathbb{C} \cap \widehat{\mathbb{C}} \setminus \{0\} = \mathbb{C}^*$ prehodna preslikava $\varphi \circ \mathrm{id}_{\mathbb{C}}^{-1} = \varphi|_{\mathbb{C}^*} : z \mapsto \frac{1}{z}$ holomorfna. Ta par lokalnih kart tako res tvori kompleksni atlas, kar pokaže, da je Riemannova sfera $\widehat{\mathbb{C}}$ Riemannova ploskev.

**Definicija 4.6.** Naj bosta $X$ in $Y$ Riemannovi ploskvi. Pravimo, da je zvezna preslikava $f : X \to Y$ *holomorfna* ali *analitična*, kadar za vsak $x \in X$ obstajata lokalna karta $(U, \varphi)$ iz kompleksnega atlasa $X$, da je $x \in U$, in lokalna karta $(V, \psi)$ iz kompleksnega atalasa $Y$, da je $f(x) \in V$, ter ob tem velja, da je preslikava

$$\psi \circ f \circ \varphi^{-1} : \varphi(U \cap f^{-1}(V)) \to \psi(V)$$

holomorfna na neki odprti okolici točke $\varphi(x) \in \mathbb{C}$ .

**Trditev 4.7.** *V posamezni točki $x \in X$ je definicija 4.6 (oziroma holomorfnost preslikave $\psi \circ f \circ \varphi^{-1}$) neodvisna od izbire lokalnih kart $(U, \varphi)$ in $(V, \psi)$.*

*Dokaz.* Naj bosta $(U', \varphi')$ in $(V', \psi')$ drugi lokalni karti (kompatibilni z $(U, \varphi)$ in $(V, \psi)$), da velja $x \in U'$ in $f(x) \in V'$. Tedaj bo na $\varphi'(U \cap U')$, ali po potrebi na manjši okolici točke $\varphi'(x)$, veljalo

$$\begin{aligned} \psi' \circ f \circ \varphi'^{-1} &= \psi' \circ (\psi^{-1} \circ \psi) \circ f \circ (\varphi^{-1} \circ \varphi) \circ \varphi'^{-1} \\ &= (\psi' \circ \psi^{-1}) \circ (\psi \circ f \circ \varphi^{-1}) \circ (\varphi \circ \varphi'^{-1}). \end{aligned}$$

Zaradi kompatibilnostnega pogoja sta $\varphi \circ \varphi'^{-1}$ in $\psi' \circ \psi^{-1}$ biholomorfizma med dvema okolicama točk $\varphi'(x)$ in $\varphi(x)$ ter $\psi(f(x))$ in $\psi'(f(x))$, zato bo $\psi' \circ f \circ \varphi'^{-1}$ holomorfna na okolici točke $\varphi'(x)$ natanko tedaj, ko bo $\psi \circ f \circ \varphi^{-1}$ holomorfna na neki okolici točke $\varphi(x)$. S tem je neodvisnost dokazana. □

**Zgled 4.8.** Oglejmo si, kako lahko meromorfne funkcije na domenah v $\mathbb{C}$, glede na definicijo 4.6, vidimo kot holomorfne funkcije, ki slikajo v Riemannovo sfero. Naj bo $f$ meromorfna funkcija na domeni $D \subseteq \mathbb{C}$ z diskretno množico polov $S \subseteq D$. Tedaj ima v vsakem polu $a \in S$ funkcija $\frac{1}{f}$ odpravljivo singularnost z limito $\lim_{z \to a} \frac{1}{f(z)} = 0$, kar pomeni, da jo lahko v točkah iz $S$ z vrednostjo 0 holomorfno razširimo. Ta opazka bo koristna pri preverjanju holomorfnosti v nadaljevanju.

Formalno imamo trenutno opravka s funkcijo $f : D \setminus S \to \mathbb{C}$, radi pa bi jo identificirali s holomorfno funkcijo $D \to \widehat{\mathbb{C}}$. Edini smiselni način, da sploh zagotovimo zveznost, je izbira funkcije $\overline{f} : D \to \widehat{\mathbb{C}}$, za katero velja $\overline{f}|_{D \setminus S} = f$ in

$$\overline{f}(a) = \infty \text{ za vse } a \in S.$$

Polejmo si, zakaj bi $\overline{f}$ bila tudi holomorfna. V ta namen si lokalno okoli poljubne točke iz $D$ oglejmo $\overline{f}$ v kartah, ob tem pa ločimo dve možnosti.

(i) Če je $z \in D \setminus S$, zaradi diskretnosti množice $S$ obstaja odprta okolica $U$ točke $z$, ki je disjunktna s $S$. Tedaj je funkcija

$$\mathrm{id}_{\mathbb{C}} \circ \overline{f} \circ \mathrm{id}_U^{-1} = f|_U$$

holomorfna na $U$, med lokalnima kartama $(U, \mathrm{id}_U)$ za $D$ ter $(\mathbb{C}, \mathrm{id}_{\mathbb{C}})$ za $\widehat{\mathbb{C}}$.

(ii) Če je $z \in S$, pa zaradi diskretnosti množice ničel holomorfne funkcije $f$ obstaja odprta okolica $U$ točke $z$, ki množice ničel ne seka. Tedaj je funkcija

$$\varphi \circ \bar{f} \circ \mathrm{id}_U^{-1} = \frac{1}{f|_U}$$

holomorfna po začetni opazki, saj se $\frac{1}{f}$ holomorfno razširi z vrednostjo 0 v polu $z \in S$. Tukaj smo uporabili lokalni karti $(U, \mathrm{id}_U)$ za $D$ in $(\widehat{\mathbb{C}} \setminus \{0\}, \varphi)$ za $\widehat{\mathbb{C}}$.

Zaključimo lahko, da je tako definirana razširitev meromorfne funkcije $f$ holomorfna preslikava $D \to \widehat{\mathbb{C}}$ med Riemannovima ploskvama.

Zelo pomemba trditev, ki razčisti vprašanje o holomorfnosti inverza holomorfne bijekcije, je naslednja.

**Trditev 4.9.** *Naj bosta $X$ in $Y$ Riemannovi ploskvi in naj bo $f : X \to Y$ holomorfna bijekcija med njima. Tedaj je tudi preslikava $f^{-1} : Y \to X$ holomorfna.*

**Opomba 4.10.** Takšni holomorfni preslikavi $f : X \to Y$, katere inverz je prav tako holomorfen, pravimo *biholomorfizem* in tedaj imamo Riemannovi ploskvi $X$ in $Y$ za *biholomorfni* oziroma *izomorfni* v smislu Riemannovih ploskev, kar označujemo z

$$X \cong Y.$$

*Dokaz.* Naj bosta $(U, \varphi)$ in $(V, \psi)$ lokalni karti iz kompleksnih atlasov za $X$ in $Y$. Ker je $f$ bijekcija, velja $f(U \cap f^{-1}(V)) = f(U) \cap V$ in preslikava

$$\psi \circ f \circ \varphi^{-1} : \varphi(U \cap f^{-1}(V)) \to \psi(f(U) \cap V)$$

je holomorfna bijekcija med dvema odprtima množicama v $\mathbb{C}$. Sedaj želimo pokazati, da je njen inverz $\varphi \circ f^{-1} \circ \psi^{-1}$ holomorfen na $\psi(f(U) \cap V) \subseteq \mathbb{C}$.

Naj bo $z_0 \in \varphi(U \cap f^{-1}(V))$ poljubna. Tedaj je $(\psi \circ f \circ \varphi^{-1})'(z_0) \neq 0$. V nasprotnem primeru bi sicer lahko na neki dovolj majhni okolici $W \subseteq \varphi(U \cap f^{-1}(V))$ točke $z_0$ zapisali

$$\psi(f(\varphi^{-1}(z))) - \psi(f(\varphi^{-1}(z_0))) = (z - z_0)^m g(z),$$

kjer je $m \geq 2$ in $g \in \mathcal{O}(W)$ brez ničle na $W$, kar bi bilo v nasprotju z injektivnostjo $\psi \circ f \circ \varphi^{-1}$. Tako dobimo po izreku o inverzni funkciji [5, izrek 67] holomorfen inverz, definiran na okolici točke $\psi(f(\varphi(z_0))) \in \psi(f(U) \cap V)$, katerega predpis se bo zaradi enoličnosti inverzov ujemal s $\varphi \circ f^{-1} \circ \psi^{-1}$ na ustrezni domeni. To lahko storimo za vsak $z_0 \in \varphi(U \cap f^{-1}(V))$, kar zagotovi holomorfnost preslikave $\varphi \circ f^{-1} \circ \psi^{-1}$ na celotnem $\psi(f(U) \cap V)$.

S tem smo pokazali holomorfnost preslikave $f^{-1}$ v vseh lokalnih kartah Riemannovih ploskev $X$ in $Y$, od koder sledi biholomorfnost preslikave $f$ in zaključi dokaz. □

**Izrek 4.11** (Izrek o implicitni preslikavi)**.** *Naj bo $\Omega \subseteq \mathbb{C}^2$ odprto območje in naj bo $f : \Omega \to \mathbb{C}$, $(z, w) \mapsto f(z, w)$ funkcija, ki je holomorfna v obeh spremenljivkah posebej. Denimo, da je $(\alpha, \beta) \in \Omega$ ničla za $f$ in da velja $f_w(\alpha, \beta) \neq 0$, kjer $f_w$ označuje kompleksni odvod po drugi spremenljivki. Tedaj obstajata dovolj majhni okolici $U \subseteq \mathbb{C}$ točke $\alpha$ in $V \subseteq \mathbb{C}$ točke $\beta$, za kateri je $U \times V \subseteq \Omega$, ter enolično določena holomorfna preslikava $\phi : U \to V$, ki izpolnjuje pogoj: za vse pare $(z, w) \in U \times V$ je $f(z, w) = 0$ natanko tedaj, ko je $w = \phi(z)$.*

*Komentar.* To je dobro poznani izrek o implicitni preslikavi, ki smo ga že srečali. Z drugimi besedami pravi, da lahko množico ničel gladke funkcije $f$ lokalno predstavimo kot graf neke gladke funkcije $\phi$ nad eno izmed spremenljivk. Za nas pa bo pomembno, da ta funkcija $\phi$ ni le gladka, ampak tudi holomorfna, če je le $f$ holomorfna.

*Dokaz.* Dokaz gladke verzije izreka bralec najde v [5, izrek 14], preostane nam le še obravnava holomorfnosti implicitne funkcije $\phi$.

Na zvezo $f(z, \phi(z)) = 0$, ki velja povsod na $z \in U \subseteq \mathbb{C}$, delujemo s Cauchy-Riemannovim operatorjem $\frac{\partial}{\partial \bar{z}}$ in tako dobimo

$$f_{\bar{z}}(z, \phi(z)) + f_w(z, \phi(z)) \frac{\partial \phi}{\partial \bar{z}}(z) = 0.$$

Ker je $f$ holomorfna v prvi spremenljivki, je $f_{\bar{z}}(z, \phi(z)) = 0$ za vse $z \in U$, po drugi strani pa zaradi zveznosti odvoda $f_w$ in $f_w(\alpha, \beta) \neq 0$ velja $f_w(z, \phi(z)) \neq 0$ na celotnem $U$, ki ga po potrebi lahko tudi zmanjšamo. Od tod sledi

$$\frac{\partial \phi}{\partial \bar{z}} = 0 \quad \text{povsod na } U,$$

kar je – pod predpostavko gladkosti funkcije $\phi$, ki drži – ekvivalentno holomorfnosti funkcije $\phi$ na $U$. $\square$

4.2. **Kompleksna struktura na eliptični krivulji.** V tem razdelku si bomo ogledali, kako eliptični krivulji priredimo kompleksno strukturo, da ta postane kompaktna Riemannova ploskev. Ta postopek lahko z isto idejo še malce posplošimo in tako pokažemo, da tudi vsaka nesingularna projektivna algebraična krivulja premore kompleksno strukturo in je tako Riemannova ploskev. Začeli bomo z afino različico krivulje v $\mathbb{C}^2$, na njej definirali kompleksen atlas, nato pa ga prenesli in nekoliko dopolnili do kompleksnega atlasa projektivnega zaprtja krivulje.

1. DEL. Naj bo afina različica eliptične krivulje podana z enačbo

$$E: \quad y^2 = 4x^3 - ax - b, \quad a^3 - 27b^2 \neq 0$$

in označimo s $f = y^2 - 4x^3 + ax + b$ njen minimalni polinom. Opazovana krivulja $E = V(f) \subseteq \mathbb{C}^2$ je torej množica ničel polinoma $f$. Zaradi pogoja $a^3 - 27b^2 \neq 0$, je $E$ nesingularna, kar pomeni, da je v vsaki točki krivulje $E$ vsaj eden od parcialnih odvodov polinoma $f$ neničeln.

Osredotočimo se sedaj na eno točko $(\alpha, \beta) \in E$ in brez škode za splošnost predpostavimo, da je $f_y(\alpha, \beta) \neq 0$. Polinom $f$ je seveda holomorfna funkcija v obeh svojih spremenljivkah, zato nam izrek o implicitni funkciji 4.11 zagotavlja obstoj holomorfne preslikave

$$\phi : W \to W',$$

kjer je $W \subseteq \mathbb{C}$ okolica $\alpha$, $W' \subseteq \mathbb{C}$ okolica $\beta$ in za vsak $z \in W$ velja $f(z, \phi(z)) = 0$. Še pomembneje pa nam implicitna funkcija $\phi$ omogoča definirati lokalno parametrizacijo krivulje $E$

$$W \to E, \quad z \mapsto (z, \phi(z)).$$

Ta je med drugim homeomorfizem na svojo sliko $U := (W \times \phi(W)) \cap E$, ki je zaradi holomorfnosti $\phi$ odprta v $E$. Preslikava $\phi$ je holomorfna in nekonstantna in je kot taka odprta preslikava, zato je škatlasta okolica $W \times \phi(W)$ odprta v $\mathbb{C}^2$ in nazadnje $U \subseteq E$ odprta v $E$. Inverz te lokalne parametrizacije je projekcija $\mathrm{pr}_1 : U \subseteq E \to W$, ki jo bomo odslej označevali s $\varphi$ in bo skupaj z okolico $U$ nosila vlogo ene lokalne karte.

*Komentar.* Zelo podobno bi storili v primeru, ko je $f_x(\alpha, \beta) \neq 0$. Tedaj bi lokalna parametrizacija bila oblike $z \mapsto (\phi(z), z)$, okolica $U$ pa bi bila graf holomorfne funkcije $\phi$ nad spremenljivko $y$ namesto $x$. Tako bi za predpis homeomorfizma $\varphi$ uporabili projekcijo $\mathrm{pr}_2$ namesto $\mathrm{pr}_1$. Omenimo še, da v to situacijo pridemo v natanko treh točkah $(e_1, 0)$, $(e_2, 0)$ in $(e_3, 0)$, kjer so $e_1$, $e_2$ in $e_3$ tri *različne* ničle polinoma $4x^3 - ax - b$, ki ima neničelno diskriminanto.

Vsak tak par $(U, \varphi)$ bomo sprejeli kot lokalno karto. Sedaj pa se bomo prepričali, da družina $\mathcal{E}$ vseh takšnih parov tvori kompleksen atlas za $E$. Za lažje nadaljevanje to družino indeksirajmo z neko[2] množico $I$ in tako lahko zapišemo $\mathcal{E} = ((U_i, \varphi_i))_{i \in I}$. Opazimo, da $(U_i)_{i \in I}$ tvori odprto pokritje za $E$, saj njena unija vsebuje vse točke iz $E$, preslikave $\varphi_i$ pa so homeomorfizmi. Preostane preveriti še kompatibilnostni pogoj – da so vse prehodne preslikave

$$\varphi_i \circ \varphi_j^{-1} : \varphi_j(U_i \cap U_j) \to \varphi_i(U_i \cap U_j)$$

holomorfne. Vzemimo poljubni dve karti $(U_i, \varphi_i)$ in $(U_j, \varphi_j)$, označimo s $\phi_i : W_i \to \mathbb{C}$ holomorfno funkcijo, katere graf nad eno izmed spremenljivk je okolica $U_i$. Analogno definiramo tudi $\phi_j : W_j \to \mathbb{C}$ in $U_j$, ob tem pa ločimo dva primera.

(i) Okolici $U_i$, $U_j$ sta grafa funkcij nad istima spremenljivkama. Obravnavajmo samo primer, ko je ta spremenljivka $x$, drugi gre povsem analogno. Tedaj izračunamo

$$(\varphi_i \circ \varphi_j^{-1})(z) = \mathrm{pr}_1(z, \phi_j(z)) = z \quad \text{za vse } z \in \varphi_j(U_i \cap U_j),$$

kar pomeni, da je prehodna preslikava $\varphi_i \circ \varphi_j^{-1} = \mathrm{id}_{\varphi_j(U_i \cap U_j)}$ enaka identiteti na množici $\varphi_j(U_i \cap U_j)$, ki je očitno holomorfna.

(ii) Okolici $U_i$, $U_j$ nista grafa funkcij nad istima spremenljivkama in recimo, da je $U_i$ graf funkcije $\phi_i$ nad spremenljivko $x$, množica $U_j$ pa naj bo graf funkcije $\phi_j$ nad spremenljivko $y$. Tedaj izračunamo

$$(\varphi_i \circ \varphi_j^{-1})(z) = \mathrm{pr}_1(\phi_j(z), z) = \phi_j(z) \quad \text{za vse } z \in \varphi_j(U_i \cap U_j).$$

Funkcija $\phi_j$ je holomorfna na kvečjemu večji množici $W_j \supseteq \varphi_j(U_i \cap U_j)$, zato je prehodna preslikava $\varphi_i \circ \varphi_j^{-1}$ holomorfna na celotnem $\varphi_j(U_i \cap U_j)$. Do povsem enakega zaključka pridemo, če je $U_i$ graf funkcije nad spremenljivko $y$, $U_j$ pa nad spremenljivko $x$. Tako vidimo, da je družina lokalnih kart $((U_i, \varphi_i))_{i \in I}$ res kompleksni atlas za $E$.

2. DEL. *Projektivno zaprtje* afine verzije eliptične krivulje $E$ je projektivna krivulja $\overline{E} \subseteq \mathbb{P}^2_{\mathbb{C}}$, podana s homogenizacijo enačbe za $E$

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

oziroma s homogenim polinomom $F = y^2 z - 4x^3 + axz^2 + bz^3$, ki je homogenizacija polinoma $f$. S pomočjo kompleksnega atlasa za $E$ bomo sedaj konstruirali atlas za $\overline{E}$.

*Komentar.* Ta del bo zahteval znanje iz uvoda v geometrijsko topologijo o kvocientnih topoloških prostorih, zato se bomo za podrobnosti sklicali na [7, poglavje 3.2].

[2] Indeksna množica $I$ zares ni pomembna, lahko pa si predstavljamo, da jo sestavljajo točke $E$, saj smo navsezadnje do vsakega od parov $(U, \varphi)$ prišli ravno z izbiro neke točke iz $E$.

Bralec ga lahko po potrebi tudi preskoči, saj ga obravnavamo zgolj za kompletnost celotne izpeljave.

Definirajmo vložitev

$$\iota : \mathbb{C}^2 \hookrightarrow \mathbb{C}^3 \setminus \{0\} \quad (x,y) \mapsto (x,y,1)$$

in kvocientno projekcijo $q : \mathbb{C}^3 \setminus \{0\} \to \mathbb{P}^2_{\mathbb{C}}$ iz opombe 2.9, kjer smo projektivne prostore opremili s topologijo. Najprej opazimo, da se projektivno zaprtje $\overline{E} \subseteq \mathbb{P}^2_{\mathbb{C}}$ od afine krivulje $E$ v bistvu razlikuje samo v eni točki – edina točka na $\overline{E}$, ki leži na *premici v neskončnosti* $\{[x:y:0] \mid (x,y) \in \mathbb{C}^2 \setminus \{0\}\}$, je le $[0:1:0]$, kar vidimo takoj, ko v polinom $F$ vstavimo $z = 0$. Od tod sledi, da je

$$\overline{E} = q(\iota(E)) \cup \{[0:1:0]\}.$$

Točko $[0:1:0]$ bomo imenovali *točka v neskončnosti* eliptične krivulje in zanjo bo potrebno posebej definirati lokalno karto. Pred tem pa se posvetimo lokalnim kartam za *afini del krivulje* $q(\iota(E)) = \{[x:y:1] \in \mathbb{P}^2_{\mathbb{C}} \mid y^2 = 4x^3 - ax - b\}$.

Označimo $V_i = q(\iota(U_i))$. Kot prej naj bo $W_i \subseteq \mathbb{C}$ slika homeomorfizma $\varphi_i$. Pomožno preslikavo $\varphi_i' : \iota(U_i) \to W_i$ definiramo s predpisom

$$\varphi_i'(x,y,z) = \varphi_i(x,y),$$

za katero velja $\varphi_i' \circ \iota = \varphi_i$.

Preslikava $\pi : \iota(U_i) \to V_i \subseteq \mathbb{P}^2_{\mathbb{C}}$ je injekcija, saj se nobeni dve različni točki iz $\iota(U_i)$ ne razlikujeta za skalarni večkratnik iz $\mathbb{C}^*$ in zaradi tega tvori samo trivialne identifikacije. Kot homeomorfizem je tudi $\varphi_i'$ injekcija, kar pomeni, da imata ti dve preslikavi enaka vlakna – same enoelementne množice. Od tod sklepamo, da je inducirana preslikava $\bar{\varphi}_i$ dobro definirana zvezna injekcija. Iz surjektivnosti $\varphi_i'$ sledi surjektivnost $\bar{\varphi}_i$, ker pa je $\varphi_i'$ homeomorfizem (torej v posebnem kvocientna preslikava), je inducirana preslikava $\bar{\varphi}_i : V_i \to W_i$ homeomorfizem, kot ponazarja komutativen diagram (4.1). Ta premislek utemeljuje [7, posledica 3.23].

$$\begin{tikzcd} \iota(U_i) \arrow[r, "\varphi_i'"] \arrow[d, "\pi"'] & W_i \\ V_i \arrow[ur, dashed, "\bar{\varphi}_i"'] & \end{tikzcd} \tag{4.1}$$

Iz komutativnega diagrama lahko inverz induciranega homeomorfizma izrazimo kot $\bar{\varphi}_i^{-1} = \pi \circ {\varphi_i'}^{-1}$. Z uporabo te zveze se lahko prepričamo o kompatibilnosti lokalnih kart $(V_i, \bar{\varphi}_i)$. Za poljubna $i, j \in I$ velja

$$\bar{\varphi}_i \circ \bar{\varphi}_j^{-1} = \bar{\varphi}_i \circ \pi \circ {\varphi'}_j^{-1} = \varphi_i' \circ {\varphi'}_j^{-1} = \varphi_i' \circ \iota \circ \varphi_j^{-1} = \varphi_i \circ \varphi_j^{-1},$$

kar nas pripelje do prehodne preslikave med lokalnima kartama afine krivulje $E$, za katero smo se že v prvem delu prepričali, da je holomorfna. Kompatibilnostni pogoj torej velja tudi za lokalni karti $(V_i, \bar{\varphi}_i)$, $(V_j, \bar{\varphi}_j)$.

Skupek vseh na ta način konstruiranih parov $(V_i, \bar{\varphi}_i)$ bo del kompleksnega atlasa za $\overline{E}$, za celoto pa nam manjka že prej omenjena lokalna karta okrog točke v neskončnosti $[0:1:0]$. Poglejmo si polinom $F(x,1,z) = z - 4x^3 + axz^2 + bz^3$ okrog točke $(x,z) = (0,0)$. Njegov odvod po $z$

$$\frac{\partial F}{\partial z}(x,1,z) = 1 + ax^2 + 3bz^2$$

je v omenjeni točki različen od nič, kar pomeni, da po izreku o implicitni funkciji obstajata okolici $W_\infty, W' \subseteq \mathbb{C}$ točke 0 in holomorfna funkcija $\phi_\infty : W_\infty \to W'$, da je $F(x, 1, \phi_\infty(x)) = 0$ za vse $x \in W_\infty$. Opomnimo še, da iz $\phi_\infty(x) = 0$ sledi $x = 0$, saj je to edina rešitev enačbe $F(x, 1, 0) = -4x^3 = 0$. Označimo $U_\infty = \{(x, 1, \phi_\infty(x)) \in \mathbb{C}^3 \setminus \{(0, 0, 0)\} \mid x \in W_\infty\}$. Tedaj je pomožna preslikava

$$\varphi'_\infty : U_\infty \to W_\infty \quad (x, y, z) \mapsto x$$

homeomorfizem, ki ima inverz podan s predpisom $x \mapsto (x, 1, \phi_\infty(x))$. Označimo $V_\infty = \pi(U_\infty) \subseteq \overline{E} \subseteq \mathbb{P}^2_{\mathbb{C}}$. Sedaj se pod istimi pogoji kot zgoraj inducira homeomorfizem $\overline{\varphi}_\infty : V_\infty \to W_\infty$, za katerega komutira naslednji diagram.

$$\begin{tikzcd} U_\infty \arrow[r, "\varphi'_\infty"] \arrow[d, "\pi"'] & W_\infty \\ V_i \arrow[ur, dashed, "\overline{\varphi}_\infty"'] & \end{tikzcd} \tag{4.2}$$

Preverimo, da je lokalna karta $(V_\infty, \overline{\varphi}_\infty)$ kompatibilna z ostalimi lokalnimi kartami, torej, da sta

$$\overline{\varphi}_i \circ \overline{\varphi}_\infty^{-1} : \overline{\varphi}_\infty(V_\infty \cap V_i) \to \overline{\varphi}_i(V_\infty \cap V_i),$$
$$\overline{\varphi}_\infty \circ \overline{\varphi}_i^{-1} : \overline{\varphi}_i(V_\infty \cap V_i) \to \overline{\varphi}_\infty(V_\infty \cap V_i)$$

holomorfni za poljuben $i \in I$. Najprej še dodatno predpostavimo, da je $U_i \subseteq E \subseteq \mathbb{C}^2$ graf holomorfne funkcije nad spremenljivko $x$. Obravnava primera, ko je okolica $U_i$ graf holomorfne funkcije nad spremenljivko $y$, bo podobna in bo sledila za tem.

Za holomorfnost omenjenih prehodnih preslikav moremo razumeti njuni domeni oz. še prej množico $V_\infty \cap V_i$. Zanimajo nas samo tisti $i \in I$, za katere je $V_\infty \cap V_i$ neprazna, zato bomo brez škode za splošnost to privzeli, saj je v nasprotnem primeru kompatibilnostni pogoj že na prazno izpolnjen.

Po eni strani množica $V_\infty \cap V_i$ vsebuje vse točke oblike $[z : 1 : \phi_\infty(z)]$ za neki $z \in W_\infty$, po drugi strani pa ima ta točka zaradi vsebovanosti v $V_i$ tudi obliko $[w : \phi_i(w) : 1]$ za neki $w \in W_i$. Eno projektivno točko smo tako zapisali s pomočjo dveh različnih predstavnikov, ki se razlikujeta za multiplikativno konstanto iz $\mathbb{C}^*$. Tako iz primerjave tretjih komponent (do multiplikativne konstante iz $\mathbb{C}^*$ natančno) ugotovimo, da je $\phi_\infty(z) \neq 0$ in je tako posredno tudi $z \neq 0$. S primerjavo drugih komponent vidimo, da mora veljati $\phi_i(w) \neq 0$, primerjava prvih komponent pa iz pogoja $z \neq 0$ zagotovi še $w \neq 0$. Ker lahko homogene koordinate s temi neničelnimi vrednostmi delimo, je od tod razvidno $[z : 1 : \phi_\infty(z)] = \left[\frac{z}{\phi_\infty(z)} : \frac{1}{\phi_\infty(z)} : 1\right]$ ter $[w : \phi_i(w) : 1] = \left[\frac{w}{\phi_i(w)} : 1 : \frac{1}{\phi_i(w)}\right]$. Če je $z \in \overline{\varphi}_\infty(V_\infty \cap V_i)$ poljuben, potem izračunamo

$$\overline{\varphi}_i(\overline{\varphi}_\infty^{-1}(z)) = \overline{\varphi}_i([z : 1 : \phi_\infty(z)]) = \overline{\varphi}_i\left(\left[\tfrac{z}{\phi_\infty(z)} : \tfrac{1}{\phi_\infty(z)} : 1\right]\right) = \frac{z}{\phi_\infty(z)}.$$

Za $w \in \overline{\varphi}_i(V_\infty \cap V_i)$ pa imamo

$$\overline{\varphi}_\infty(\overline{\varphi}_i^{-1}(w)) = \overline{\varphi}_\infty([w : \phi_i(w) : 1]) = \overline{\varphi}_\infty\left(\left[\tfrac{w}{\phi_i(w)} : 1 : \tfrac{1}{\phi_i(w)}\right]\right) = \frac{w}{\phi_i(w)}.$$

V obeh primerih sta prehodni preslikavi holomorfni na $\overline{\varphi}_\infty(V_\infty \cap V_i)$ oz. $\overline{\varphi}_i(V_\infty \cap V_i)$.

Obravajmo še primer, ko je $U_i \subseteq E$ graf holomorfne funkcije $\phi_i$ nad spremenljivko $y$. Tedaj (neprazna) množica $V_\infty \cap V_i$ vsebuje točke oblike $[z : 1 : \phi_\infty(z)] = [\phi_i(w) : w : 1]$ za neka $z \in W_\infty$ in $w \in W_i$. Podobno kot prej lahko sklepamo, da je $\phi_\infty(z) \neq 0$, od tod dobimo $z \neq 0$. Iz primerjave prve komponente lahko vidimo $\phi_i(w) \neq 0$ in iz primerjave druge komponente dobimo $w \neq 0$. Tako za poljuben $z \in \overline{\varphi}_\infty(V_\infty \cap V_i)$ dobimo

$$\overline{\varphi}_i(\overline{\varphi}_\infty^{-1}(z)) = \overline{\varphi}_i([z : 1 : \phi_\infty(z)]) = \overline{\varphi}_i\left(\left[\tfrac{z}{\phi_\infty(z)} : \tfrac{1}{\phi_\infty(z)} : 1\right]\right) = \frac{1}{\phi_\infty(z)},$$

za poljuben $w \in \overline{\varphi}_i(V_\infty \cap V_i)$ pa vidimo

$$\overline{\varphi}_\infty(\overline{\varphi}_i^{-1}(w)) = \overline{\varphi}_\infty([\phi_i(w) : w : 1]) = \overline{\varphi}_\infty\left(\left[\tfrac{\phi_i(w)}{w} : 1 : \tfrac{1}{w}\right]\right) = \frac{\phi_i(w)}{w}.$$

Tudi ti dve preslikavi sta torej holomorfni, kjer sta definirani, tj. na $\overline{\varphi}_\infty(V_\infty \cap V_i)$ oz. $\overline{\varphi}_i(V_\infty \cap V_i)$, kar nazadnje pomeni, da lokalna karta $(V_\infty, \overline{\varphi}_\infty)$ izpolnjuje kompatibilnostni pogoj s poljubno lokalno karto iz družine $((V_i, \overline{\varphi}_i))_{i\in I}$.

Ko slednji dodamo še karto $(V_\infty, \overline{\varphi}_\infty)$ pri točki $[0 : 1 : 0]$, bo tako celotna družina $((V_i, \overline{\varphi}_i))_{i\in I\cup\{\infty\}}$ tvorila kompleksen atlas za $\overline{E}$. Res, družina $(V_i)_{i\in I\cup\{\infty\}}$ tvori odprto pokritje za $\overline{E}$, vse preslikave $\overline{\varphi}_i$ so homeomorfizmi in vse lokalne karte so med sabo kompatibilne.

**Opomba 4.12.** Na začetku razdelka 4.2 smo omenili, da je eliptična krivulja kompaktna. To bomo sicer videli preko biholomorfizma (ki je v posebnem tudi homeomorfizem) s kompleksnim torusom, lahko pa to pokažemo tudi na sledeč način. Če $F \in \mathbb{C}[x, y, z]$ označuje minimalni polinom krivulje $E$, je množica $\{(x, y, z) \in \mathbb{C}^3 \setminus \{0\} \mid F(x, y, z) = 0\}$ zaprta v $\mathbb{C}^3 \setminus \{0\}$, njen presek s kompleksno enotsko sfero $S(\mathbb{C}^3)$ pa je kompakten. Slika tega preseka s kvocientno projekcijo $S(\mathbb{C}^3) \to \mathbb{P}^2_\mathbb{C}$ je ravno $E \subseteq \mathbb{P}^2_\mathbb{C}$, kot zvezna slika kompakta pa je tudi sama kompaktna, torej je $E$ kompaktna.

Tukaj lahko vlogo eliptične krivulje $E \subseteq \mathbb{P}^2_\mathbb{C}$ prevzame tudi poljubna projektivna algebraična krivulja in enak premislek nam pokaže, da je tudi ta kompaktna podmnožica v $\mathbb{P}^2_\mathbb{C}$.

S tem je zaključena konstrukcija kompleksnega atlasa na eliptični krivulji. Za konec tega razdelka si poglejmo še uporabo kompleksne strukture na primeru holomorfnih funkcij med eliptičnima krivuljama.

4.2.1. *Holomorfne preslikave med eliptičnimi krivuljami.* V 2. poglavju smo definirali pojem projektivne transformacije in nato v lemi 2.23 opazili, da imajo vse projektivnosti med projektivno ekvivalentnima eliptičnima krivuljama točno določeno obliko. V tem zgledu bomo pokazali, da je vsaka takšna projektivnost tudi holomorfna preslikava.

**Trditev 4.13.** *Naj bosta $E_1, E_2 \subseteq \mathbb{P}^2_\mathbb{C}$ projektivno ekvivalentni eliptični krivulji, podani z enačbama*

$$E_1 : \quad y^2z = 4x^3 - a_1xz^2 - b_1z^3 \quad \text{in} \quad E_2 : \quad y^2z = 4x^3 - a_2xz^2 - b_2z^3,$$

*in naj bo $u \in \mathbb{C}^*$ tak, da je*

$$g : E_1 \to E_2, \quad [x : y : z] \mapsto \left[u^2x : u^3y : z\right]$$

*projektivna ekvivalenca med njima. Tedaj je $g$ holomorfna preslikava.*

*Dokaz.* Po definiciji preverimo holomorfnost preslikave $g$. Okoli poljubne točke $p \in E_1$ ter njene slike $g(p) \in E_2$ bomo poiskali par kart $\varphi$ in $\psi$ iz atlasov za $E_1$ in $E_2$ in se prepričali o holomorfnosti preslikave $\psi \circ g \circ \varphi^{-1}$.

Označimo polinoma

$$f_i = y^2 - 4x^3 + a_i x + b_i$$

za $i \in \{1,2\}$. Ker sta $E_i$ eliptični, sta po definiciji nesingularni in imata neničelni diskriminanti, kar pomeni, da ima kubični polinom $4x^3 - a_1 x - b_1$ tri različne (kompleksne) ničle $e_1$, $e_2$, $e_3$. Projektivnost $g$ poveže para keoficientov $(a_i, b_i)$, in sicer po (2.6) velja $a_2 = u^4 a_1$, $b_2 = u^6 b_1$, torej so $u^2 e_1$, $u^2 e_2$, $u^2 e_3$ tri različne ničle polinoma $4x^3 - a_2 x - b_2$. To vidimo tudi direktno z uporabo projektivnosti $g$, ki je bijektivna in slika $[e_i : 0 : 1] \mapsto [u^2 e_i : 0 : 1]$. Hkrati pa so točke oblike $(e_i, 0)$ oz. $(u^2 e_i, 0)$ edine, v katerih je $\frac{\partial f_1}{\partial y} = 0$ oz. $\frac{\partial f_2}{\partial y} = 0$ in ki rešijo enačbo $f_1 = 0$ oz. $f_2 = 0$. Na afinem delu krivulje bo tako, razen v teh treh točkah, možno uporabiti lokalne karte, ki izhajajo iz dejstva, da je krivuljo mogoče predstaviti kot graf holomorfne funkcije nad spremenljivko $x$. Ločimo nekaj možnosti glede na izbrano točko $p \in E_1$.

(i) $p = [e_i : 0 : 1]$: Tedaj vidimo, da je $g(p) = [u^2 e_i : 0 : 1]$, torej izberimo lokalni karti $\varphi$ okrog $p \in E_1$ in $\psi$ okrog $g(p) \in E_2$, ki sta na dovolj majhnih okolicah $p$ oziroma $g(p)$ podani s predpisoma

$$\varphi([x : y : 1]) = y \quad \text{in} \quad \psi([x : y : 1]) = y$$

njuna inverza pa kot

$$\varphi^{-1}(w) = [\phi_1(w) : w : 1] \quad \text{in} \quad \psi^{-1}(w) = [\phi_2(w) : w : 1]\,.$$

Ob tem sta $\phi_1$ in $\phi_2$ holomorfni funkciji, ki v konstrukciji kompleksnega atlasa izhajata iz primera, ko lahko afina dela krivulj $E_1$ in $E_2$ okoli $p$ oz. $g(p)$ izrazimo kot grafa funkcij $\phi_1$ in $\phi_2$ nad spremenljivko $y$. Tedaj izračunamo

$$\psi(g(\varphi^{-1}(w))) = \psi(g([\phi_1(w) : w : 1])) = \psi([u^2\phi_1(w) : u^3 w : 1]) = u^3 w,$$

ki je jasno holomorfna na dovolj majhni odprti okolici točke $\varphi(p)$.

(ii) $p = [0 : 1 : 0]$: Za točko v neskončnosti imamo na obeh krivuljah lokalni karti $\varphi$ okrog $p$ in $\psi$ okrog $g(p) = [0 : 1 : 0]$ podani s predpisoma

$$\varphi([x : 1 : z]) = x \quad \text{in} \quad \psi([x : 1 : z]) = x,$$

njuna inverza pa z

$$\varphi^{-1}(w) = [w : 1 : \phi_1(w)] \quad \text{in} \quad \psi^{-1}(w) = [w : 1 : \phi_2(w)]\,,$$

za ustrezni holomorfni funkciji $\phi_1$ in $\phi_2$ na dovolj majhnih odprtih okolicah $\varphi(p)$ oziroma $\psi(g(p))$. Tedaj na tej majhni okolici $\varphi(p)$ velja

$$\begin{aligned}\psi(g(\varphi^{-1}(w))) &= \psi(g([w : 1 : \phi_1(w)])) \\ &= \psi(\left[u^2 w : u^3 : \phi_1(w)\right]) = \psi\left(\left[\tfrac{w}{u} : 1 : \tfrac{\phi_1(w)}{u^3}\right]\right) = \frac{w}{u}.\end{aligned}$$

Slednji račun pokaže, da je $\psi \circ g \circ \varphi^{-1}$ na tej odprti okolici holomorfna.

(iii) Nazadnje naj bo točka $p \in E_1$ poljubna, ki ni iz zgornjih dveh primerov. Tedaj imamo okoli $p$ in $g(p)$ lokalni karti $\varphi$ in $\psi$ s predpisoma

$$\varphi([x : y : 1]) = x \quad \text{in} \quad \psi([x : y : 1]) = x.$$

Njuna inverza imata predpisa

$$\varphi^{-1}(w) = [w : \phi_1(w) : 1] \quad \text{in} \quad \psi^{-1}(w) = [w : \phi_2(w) : 1]\,,$$

kjer sta $\phi_1$ in $\phi_2$ ustrezni holomorfni funkciji, katerih graf je lokalno afini del krivulj $E_1$ oz. $E_2$ okoli točk $p$ oz. $g(p)$. Tedaj izračunamo

$$\psi(g(\varphi^{-1}(w))) = \psi(g([w : \phi_1(w) : 1])) = \psi(\left[u^2 w : u^3\phi_1(w) : 1\right]) = u^2 w,$$

kar je jasno predpis holomorfne funkcije na odprti okolici točke $\varphi(p)$. $\square$

Poleg tega opazimo, da smo hkrati z istim premislekom pokazali tudi holomorfnost inverza dane projektivnosti, saj njen predpis po menjavi $u$ v $1/u$ še vedno ohranja obliko. Od tod sledi, da sta projektivno ekvivalentni eliptični krivulji tudi izomorfni kot Riemannovi ploskvi. Z drugimi besedami to pomeni, da smo algebraični izomorfizem (projektivnost med krivuljama) prevedli v analitičnega – biholomorfizem Riemmanovih ploskev.

Neformalno opomnimo še, da je vsaka holomorfna funkcija $g : E_1 \to E_2$ v nekem smislu tudi "algebraična" – njen prepis je podan s koordinatnimi funkcijami, ki so racionalne funkcije v spremenljivkah $x$, $y$, $z$. Glavni razlog za to se skriva v trditvi, da lahko vsako eliptično funkcijo glede na neko mrežo $\Lambda$ zapišemo kot neko racionalno funkcijo v spremenljivkah $\wp$ in $\wp'$. Z drugimi besedami to pomeni, da je polje eliptičnih funkcij izomorfno razširitvi $\mathbb{C}$ s $\wp$ in $\wp'$, torej $\mathbb{C}(\wp, \wp')$. Ta pa je kvadratična razširitev polja racionalnih funkcij s kompleksnimi koeficienti $\mathbb{C}(x)$ in sicer velja

$$\mathbb{C}(\wp, \wp') \cong \mathbb{C}(x)[y]/(y^2 - 4x^3 + g_2 x + g_3).$$

Ta izrek najdemo v [6, **1**, §2, theorem 4], bistvne ideje za tem fenomenom pa so opisane v [10, §2 in §3].

4.3. **Kompleksna struktura na torusu.** Cilj tega razdelka bo najprej razumeti topologijo kvocienta $\mathbb{C}/\Lambda$, nato pa ga opremiti še s kompleksnim atlasom, da bomo lahko govorili o holomorfnih preslikavah med njim in eliptično krivuljo.

Naj bo $\pi : \mathbb{C} \to \mathbb{C}/\Lambda$ kvocientna projekcija iz začetka poglavja 3 o eliptičnih funkcijah. Zaenkrat jo razumemo samo kot preslikavo množic, ki poljubni točki $z \in \mathbb{C}$ priredi njen ekvivalenčni razred $z + \Lambda$ vseh točk, ki se od $z$ razlikujejo za prišteto periodo iz $\Lambda$. Spomnimo se, da lahko tedaj $\mathbb{C}/\Lambda$ opremimo s kvocientno topologijo, tako da za odprte množice vzamemo natanko tiste $U \subseteq \mathbb{C}/\Lambda$, za katere je $\pi^{-1}(U)$ odprta v $\mathbb{C}$ in na ta način projekcija $\pi : \mathbb{C} \to \mathbb{C}/\Lambda$ postane zvezna preslikava. Poleg tega je $\pi$ tudi odprta, kar je v splošnem res za vse kvocientne projekcije v prostor orbit delovanja neke topološke grupe [7, trditev 3.42], o tem pa se lahko prepričamo tudi z direktnim računom. Za poljubno odprto množico $U \subseteq \mathbb{C}$ je njena slika $\pi(U)$ odprta, saj je njeno *nasičenje*

$$\pi^{-1}(\pi(U)) = U + \Lambda = \bigcup_{\omega \in \Lambda} (U + \omega)$$

unija translatov odprte množice $U$ oblike $U + \omega = \{z + \omega \mid z \in U\}$, ti pa so vsi odprti v $\mathbb{C}$.

Definicija topologije na kvocientu je dobra in precej temeljna, toda sama po sebi še morda nekoliko prikriva, kateremu poznanemu prostoru je homeomorfen kvocient $\mathbb{C}/\Lambda$. Oglejmo si preslikavo

$$f : \mathbb{C} \to S^1 \times S^1, \quad t_1\omega_1 + t_2\omega_2 \mapsto (e^{2\pi i t_1}, e^{2\pi i t_2}),$$

kjer sta $\omega_1$ in $\omega_2$ osnovni periodi mreže $\Lambda$ in $t_1, t_2 \in \mathbb{R}$. Preslikava je dobro definirana, saj $\omega_1$ in $\omega_2$ tvorita realno bazo za $\mathbb{C}$, in je tudi zvezna, saj koeficienta $t_1$ in $t_2$ dobimo s projiciranjem točke $t_1\omega_1 + t_2\omega_2$ na premici skozi izhodišče v smereh $\omega_1$ oziroma $\omega_2$. Slednje dosežemo z realno linearno preslikavo[3] $\mathbb{C} \to \mathbb{R}^2$, podano s slikama baznih vektorjev $\omega_1 \mapsto (1, 0)$ in $\omega_2 \mapsto (0, 1)$. Ključno pa je, da se vrednost preslikave $f$ v dani točki $z \in \mathbb{C}$ ne spremeni, če ji prištejemo katerokoli periodo iz $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.

[3]To je linearni izomorfizem, zato je poleg zveznosti tudi odprta.

To pomeni, da ostaja konstantna na poljubnem ekvivalenčnem razredu $z + \Lambda$. Še več, njena vlakna so množice oblike $\{t_1\omega_1 + t_2\omega_2 + \omega \mid \omega \in \Lambda\}$, kar so natanko ekvivalenčni razredi $\mathbb{C}/\Lambda$. Zato po [7, trditev 3.22] $f$ inducira zvezno bijekcijo

$$h : \mathbb{C}/\Lambda \to S^1 \times S^1, \quad t_1\omega_1 + t_2\omega_2 + \Lambda \mapsto (e^{2\pi i t_1}, e^{2\pi i t_2})$$

za katero velja $h \circ \pi = f$. Preslikava $h$ je ob tem še odprta in zato homeomorfizem. Namreč za odprto množico $U \subseteq \mathbb{C}/\Lambda$, lahko njeno sliko s $h$ zapišemo kot $h(U) = h(\pi(\pi^{-1}(U))) = f(\pi^{-1}(U))$. Ta pa je odprta zaradi odprtosti množice $\pi^{-1}(U)$ in odprtosti preslikave $f$, ki je kompozicija dveh odprtih preslikav – realnega linearnega izomorfizma in odprte eksponentne preslikave $t \mapsto e^{2\pi i t}$. Tako vidimo, da (topološki) kvocient $\mathbb{C}/\Lambda$ predstavlja poznani topološki prostor $S^1 \times S^1$, tj. torus.

Lotimo se sedaj še kompleksne strukture na $\mathbb{C}/\Lambda$. Tukaj bo bistvena kvocientna projekcija $\pi : \mathbb{C} \to \mathbb{C}/\Lambda$, s katero bomo definirali lokalne karte. Izkoristili bomo naslednjo njeno lastnost.

**Lema 4.14.** *Za vsako točko $z + \Lambda \in \mathbb{C}/\Lambda$ obstaja takšna odprta okolica $U \subseteq \mathbb{C}/\Lambda$, te točke, imenujemo jo* fundamentalna okolica, *da je $\pi^{-1}(U)$ homeomorfna produktu $U \times \Lambda$, oziroma ekvivalentno*

$$\pi^{-1}(U) = \coprod_{\omega \in \Lambda} \tilde{U}_\omega \quad \textit{za neke homeomorfne } \text{kopije } \tilde{U}_\omega \subseteq \mathbb{C} \textit{ okolice } U.$$

*Dokaz.* Izberimo točko $z + \Lambda \in \mathbb{C}/\Lambda$ in naj bo $z \in \mathbb{C}$ neki predstavnik tega ekvivalenčnega razreda. Ker je projekcija $\pi : \mathbb{C} \to \mathbb{C}/\Lambda$ odprta, bomo za odprto okolico $z + \Lambda$ vzeli kar sliko diska radija $r > 0$, $U = \pi(\Delta(z, r))$. Tedaj vidimo, da velja

$$\pi^{-1}(\pi(\Delta(z, r))) = \bigcup_{\omega \in \Lambda} \Delta(z + \omega, r).$$

Ta unija ni nujno disjunktna, lahko pa to dosežemo s primerno izbiro radija $r > 0$. Če namreč zahtevamo $0 < r < \frac{1}{2} \min_{\omega \in \Lambda'} |\omega|$, je presek poljubnih dveh diskov tega radija, katerih središči sta v množici $z + \Lambda \subset \mathbb{C}$, prazen.

Prepričajmo se še, da je vsaka od kopij $\tilde{U}_\omega = \Delta(z + \omega, r)$ tudi homeomorfna $\pi(U)$. Zožitev $\pi|_{\tilde{U}_\omega}$ je zvezna in odprta, je pa tudi bijektivna, saj zaradi disjunktnosti vseh kopij projekcija $\pi$ ne naredi nobenih netrivialnih identifikacij na $\tilde{U}_\omega$. Iskani homeomorfizem je tako $\pi|_{\tilde{U}_\omega} : \tilde{U}_\omega \to U$. □

**Opomba 4.15.** V splošnem se preslikave s to lastnostjo imenujejo *krovne projekcije.*

**Trditev 4.16.** *Družina $((U_i, \varphi_i))_{i \in I}$, kjer je $U_i \subseteq \mathbb{C}/\Lambda$ fundamentalna okolica neke točke baznega prostora $\mathbb{C}/\Lambda$ in je $\varphi_i = (\pi|_{V_i})^{-1}$ za neko kopijo fundamentalne okolice $V_i \subseteq \mathbb{C}$, tvori kompleksni atlas prostora $\mathbb{C}/\Lambda$.*

*Dokaz.* Za poljubno točko $z + \Lambda \in \mathbb{C}/\Lambda$ naj bo $U \subseteq \mathbb{C}/\Lambda$ njena fundamentalna okolica in $V \subseteq \mathbb{C}$ poljubna njej homeomorfna kopija. Tedaj vemo, da je $\pi|_V : V \to U$ homeomorfizem, ki kompleksno strukturo okolice $V \subseteq \mathbb{C}$ prenese na torus. Tako bo njen inverz $(\pi|_V)^{-1}$ dober kandidat za lokalno karto. Pokažimo, da je res tako, tj. da družina vseh takšnih parov $(U, (\pi|_V)^{-1})$ tvori kompleksen atlas za $\mathbb{C}/\Lambda$.

Po konstrukciji vse fundamentalne okolice pokrijejo bazni prostor $\mathbb{C}/\Lambda$ in kot smo že omenili, so vse lokalne karte homeomorfizmi. Da bo omenjena družina kompleksen atlas, preostane preveriti še kompatibilnostni pogoj. Vzemimo poljubni dve lokalni karti, sestavljeni iz okolic $U_1, U_2 \subseteq \mathbb{C}/\Lambda$ in pripadajočih homeomorfizmov $(\pi|_{V_1})^{-1}$ :

$V_1 \to U_1$ ter $(\pi|_{V_2})^{-1} : V_2 \to U_2$, ki ju označimo s $\varphi_1$ in $\varphi_2$. Prepričajmo se, da je preslikava

$$\varphi_1 \circ \varphi_2^{-1} : \varphi_2(U_1 \cap U_2) \to \varphi_1(U_1 \cap U_2)$$

holomorfna na odprti množici $\varphi_2(U_1 \cap U_2) \subseteq \mathbb{C}$. Najlažje bo, če si ogledamo njen predpis. Za poljuben $z \in \varphi_2(U_1 \cap U_2)$ je $\varphi_1(\varphi_2^{-1}(z)) = z + \omega_z$ za neki $\omega_z \in \Lambda$, ki je odvisen od $z$. Zvezna preslikava $\varphi_1 \circ \varphi_2^{-1} - \mathrm{id}_{\mathbb{C}}$ bo tako slikala iz okolice $\varphi_2(U_1 \cap U_2)$ točke $z$ v mrežo $\Lambda$. Slednja je opremljena z diskretno topologijo, zato bo omenjena preslikava konstantna na vsaki povezani komponenti odprte množice $\varphi_2(U_1 \cap U_2)$. To pomeni, da ima na vsaki povezani komponenti prehodna preslikava predpis oblike

$$\varphi_1(\varphi_2^{-1}(z)) = z + \omega,$$

za neki $\omega \in \Lambda$ (ta je zares odvisen samo od komponente za poveznost množice $\varphi_2(U_1 \cap U_2)$). Od tod je razvidno, da je preslikava $\varphi_1 \circ \varphi_2^{-1}$ holomorfna. $\square$

**Definicija 4.17.** Naj bo $\Lambda \subseteq \mathbb{C}$ mreža. Kvocientnemu prostoru $\mathbb{C}/\Lambda$ skupaj s pripadajočim kompleksnim atlasom pravimo *kompleksni torus*.

**Lema 4.18.** *Kvocientna projekcija $\pi : \mathbb{C} \to \mathbb{C}/\Lambda$ je holomorfna.*

*Dokaz.* Preverili bomo holomorfnost preslikave $\pi$ okoli vsake točke v $\mathbb{C}$. Bistveno je opaziti, da je $\pi$ lokalni homeomorfizem. Naj bo $z_0 \in \mathbb{C}$ poljubna in $V \subseteq \mathbb{C}$ njena dovolj majhna odprta okolica, ki se s $\pi$ homeomorfno preslika na odprto množico $U \subseteq \mathbb{C}/\Lambda$, torej je $(\pi|_V)^{-1} : U \to V$ lokalna karta za $\mathbb{C}/\Lambda$.

Za dokaz holomorfnosti preslikave $\pi$, si jo oglejmo v kartah. Kompleksna struktura na $\mathbb{C}$ je podana že z eno samo karto, tj. $(\mathbb{C}, \mathrm{id}_{\mathbb{C}})$, zato bomo preverili holomorfnost preslikave

$$((\pi|_V)^{-1} \circ \pi) : V \to \mathbb{C}.$$

Ker nas zares zanima samo obnašanje te preslikave okoli točke $z_0$, lahko obravnavamo zgolj njeno zožitev na odprto okolico $V \subseteq \pi^{-1}(U) = \bigcup_{\omega \in \Lambda}(V + \omega)$. Od tod pa takoj sledi, da je $((\pi|_V)^{-1} \circ \pi)|_V = \mathrm{id}_V$ holomorfna funkcija na $V \subseteq \mathbb{C}$, kar dokaže želeno. $\square$

**Opomba 4.19.** Preko leme 4.14 vidimo, da je $\pi$ lokalni homeomorfizem. To pomeni, da ima vsaka točka v $\mathbb{C}/\Lambda$ odprto okolico $U \subseteq \mathbb{C}/\Lambda$ in odprto kopijo $\tilde{U} \subseteq \mathbb{C}$, za kateri je $\pi|_{\tilde{U}} : \tilde{U} \to U$ homeomorfizem. Ker pa je $\pi$ holomorfna, je takšna jasno tudi zožitev $\pi|_{\tilde{U}}$, ki je bijekcija in zato po trditvi 4.9 celo biholomorfizem. Tedaj rečemo, da je $\pi$ *lokalni biholomorfizem*.

Zadnja opomba in zgled 4.8 nam omogočata eliptične funkcije pogledati še z vidika Riemannovih ploskev. Eliptična funkcija $f \in \mathbb{C}(\Lambda)$ je meromorfna funkcija na $\mathbb{C}$, ki jo po omenjenem zgledu lahko realiziramo kot holomorfno funkcijo $\mathbb{C} \to \widehat{\mathbb{C}}$. Poleg tega je po definiciji njena vrednost dobro definirana na translatih oblike $z + \Lambda$, torej inducira zvezno preslikavo na kvocientu $\mathbb{C}/\Lambda \to \widehat{\mathbb{C}}$, ki pa ni le zvezna, ampak tudi holomorfna. Ekvivalentno lahko torej rečemo, da so eliptične funkcije glede na mrežo $\Lambda$ natanko holomorfne funkcije $\mathbb{C}/\Lambda \to \widehat{\mathbb{C}}$. Imamo bijektivno korespondenco množic

$$\{\Lambda\text{-periodične funkcije}\} \longleftrightarrow \{\text{holomorfne preslikave } \mathbb{C}/\Lambda \to \widehat{\mathbb{C}}\}.$$

4.3.1. *Holomorfne preslikave med kompleksnimi torusi.* Podobno kot smo obravnavali holomorfne preslikave med eliptičnima krivuljama, si bomo v tem podrazdelku pogledali holomorfne preslikave med kompleksnima torusoma. Začeli bomo s konstrukcijo ene takšne preslikave, ki izhaja iz linearne holomorfne funkcije, nato pa z manjšo pomočjo teorije krovnih prostorov pokazali, da v resnici vsaka holomorfna preslikava med kompleksnima torusoma izhaja iz takšne cele holomorfne funkcije.

**Zgled 4.20.** Naj bosta $\Lambda_1$ in $\Lambda_2$ mreži v kompleksni ravnini in $\alpha, \beta \in \mathbb{C}$ kompleksni števili, da velja

$$\alpha\Lambda_1 \subseteq \Lambda_2.$$

Naj bo $f : \mathbb{C} \to \mathbb{C}$ funkcija podana s predpisom $f(z) = \alpha z+\beta$ in označimo kvocientni projekciji $\pi_1 : \mathbb{C} \to \mathbb{C}/\Lambda_1$ ter $\pi_2 : \mathbb{C} \to \mathbb{C}/\Lambda_2$.

Zaradi pogoja $\alpha\Lambda_1 \subseteq \Lambda_2$, za poljubni točki $z, w \in \mathbb{C}$, za kateri je $\pi_1(z) = \pi_1(w)$ oz. $z + \Lambda_1 = w + \Lambda_1$, sledi tudi $\pi_2(f(z)) = \pi_2(f(w))$ oz. $\alpha z + \beta + \Lambda_2 = \alpha z + \beta + \Lambda_2$. Od tod se po trditvi [7, trditev 3.22] inducira zvezna preslikava $\overline{f} : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$, da velja $\overline{f} \circ \pi_1 = \pi_2 \circ f$, oziroma da komutira naslednji diagram.

$$\begin{tikzcd}
\mathbb{C} \arrow[r, "f"] \arrow[d, "\pi_1"'] & \mathbb{C} \arrow[d, "\pi_2"] \\
\mathbb{C}/\Lambda_1 \arrow[r, dashed, "\overline{f}"'] & \mathbb{C}/\Lambda_2
\end{tikzcd}$$

Poleg tega pa je $\overline{f}$ tudi holomorfna. Ker je $\pi_1$ lokalni homeomorfizem, ima vsaka točka na torusu $\mathbb{C}/\Lambda_1$ odprto okolico $U$ homeomorfno neki odprti množici $V \subseteq \mathbb{C}$, tako da je $\pi_1|_V : V \to U$ homeomorfizem. Preslikava $\pi_1$ je po lemi 4.18 holomorfna, torej je takšna tudi njena zožitev $\pi_1|_V$, hkrati pa je ta zožitev tudi homeomorfizem, zato je po trditvi 4.9 njen inverz $(\pi_1|_V)^{-1}$ holomorfen. Tedaj vidimo, da lahko iz enačbe $\overline{f} \circ \pi_1 = \pi_2 \circ f$ lokalno izrazimo $\overline{f}$, od koder sledi, da je

$$\overline{f}|_U = \pi_2 \circ f \circ (\pi_1|_V)^{-1}$$

holomorfna preslikava na okolici $U$. Pokazali smo, da je $\overline{f}$ holomorfna na neki odprti okolici vsake točke iz $\mathbb{C}/\Lambda_1$, zato je holomorfna tudi kot preslikava $\overline{f} : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$. Po tej konstrukciji lahko zapišemo predpis inducirane preslikave

$$\overline{f} : z + \Lambda_1 \mapsto \alpha z + \beta + \Lambda_2.$$

V posebnem, kadar obstaja tako število $\alpha \in \mathbb{C}^*$, da velja celo enakost $\alpha\Lambda_1 = \Lambda_2$, bo inducirana preslikava $\overline{f} : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$, podana s predpisom $\overline{f}(z+\Lambda_1) = \alpha z+\beta+\Lambda_2$, biholomorfizem. Njen inverz bo preslikava s predpisom $z + \Lambda_2 \mapsto \frac{z}{\alpha} - \frac{\beta}{\alpha} + \Lambda_1$, ki je tudi holomorfna, saj jo inducira inverz funkcije $f$, ki je tudi iste oblike kot $f$, s predpisom $f^{-1}(z) = \frac{z}{\alpha} - \frac{\beta}{\alpha}$. Inverz $\mathbb{C}/\Lambda_2 \to \mathbb{C}/\Lambda_1$ se torej inducira ravno zaradi zveze $\alpha^{-1}\Lambda_2 \subseteq \Lambda_1$, ki jasno sledi iz enakosti $\alpha\Lambda_1 = \Lambda_2$.

Izkaže se, da velja tudi neke vrste obrat te konstrukcije. Namreč vsaka zvezna funkcija $\overline{f} : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ izhaja iz takšne zvezne funkcije $f : \mathbb{C} \to \mathbb{C}$, da $f$ po zgornjem premisleku inducira ravno preslikavo $\overline{f}$ med torusoma. To pove naslednja trditev.

**Trditev 4.21.** *Naj bo $\overline{f} : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ zvezna preslikava.*

*(i) Tedaj obstaja zvezna funkcija* $f : \mathbb{C} \to \mathbb{C}$, *da velja*

$$\overline{f} \circ \pi_1 = \pi_2 \circ f.$$

*Ob tem je* $f$ *enolično določena s* $\overline{f}$, *do prištevanja konstante iz* $\Lambda_2$ *natančno.*

*(ii) Če je* $\overline{f}$ *tudi holomorfna, je* $f$ *holomorfna in oblike* $f(z) = \alpha z + \beta$ *za neka* $\alpha, \beta \in \mathbb{C}$ *in ob tem posledično velja* $\alpha\Lambda_1 \subseteq \Lambda_2$ *ter* $\overline{f}(z + \Lambda_1) = \alpha z + \beta + \Lambda_2$.

*Dokaz.* $(i)$ Dokaz obstoja preslikave $f : \mathbb{C} \to \mathbb{C}$ se dotakne teorije krovnih prostorov, ki izkoristi enostavno povezanost $\mathbb{C}$ ter lepo strukturo kvocientne projekcje $\pi_2$, in je ne bomo razvijali, zato se skličimo na [10, lemma 3.1]. Idejno si konstrukcijo te preslikave lahko predstavljamo kot nekakšen usklajen način združitve določenih lokalnih biholomorfizmov, ki izhajajo iz projekcije $\pi_2$, komponiranih s $\overline{f}$.

Pokažimo še njeno enoličnost. Če bi imeli dva dviga $f$ in $g$, ki zadoščata enačbi $\pi_2 \circ f = \overline{f} \circ \pi_1 = \pi_2 \circ g$, bi njuna razlika $f - g : \mathbb{C} \to \Lambda_2$ slikala v mrežo $\Lambda_2$. Zvezna funkcija, ki slika v diskretno množico, kot je mreža $\Lambda_2$, pa je lahko samo konstantna, od koder dobimo $f = g + \omega$ za neko periodo $\omega \in \Lambda_2$.

$(ii)$ Podobno kot smo v zgledu 4.20 izkoristili lokalno biholomorfnost projekcije $\pi_1$, tokrat uporabimo lokalno biholomorfnost $\pi_2$, da lokalno izrazimo $f$ kot kompozicijo holomorfnih funkcij. Sledi, da je $f$ cela holomorfna funkcija.

Oglejmo si še obliko funkcije $f : \mathbb{C} \to \mathbb{C}$. Naj bo $\omega \in \Lambda_1$ poljubna perioda in tvorimo celo holomorfno funkcijo s predpisom $g_\omega(z) = f(z + \omega) - f(z)$. Tedaj velja

$$\pi_2(f(z + \omega)) = \overline{f}(\pi_1(z + \omega)) = \overline{f}(\pi_1(z)) = \pi_2(f(z)),$$

kar pomeni, da $g_\omega$ slika v diskretno mrežo $\Lambda_2$ in je tako lahko le konstantna. Njen odvod je torej ničeln, torej za vse $z \in \mathbb{C}$ velja $f'(z + \omega) = f'(z)$. Ker je bila perioda $\omega \in \Lambda_1$ poljubna, sledi, da je $f'$ eliptična glede na $\Lambda_1$. Kot holomorfna eliptična funkcija pa je ponovno lahko le konstanta po trditvi 3.6. Tedaj je $f' \equiv \alpha$ za neki $\alpha \in \mathbb{C}$ in posledično za vse $z \in \mathbb{C}$ velja $f(z) = \alpha z + \beta$ za neki $\beta \in \mathbb{C}$, kar smo hoteli pokazati. □

**Primer 4.22.** Vzemimo mreži $\Lambda_1 = \mathbb{Z} + i\mathbb{Z}$ ter $\Lambda_2 = \mathbb{Z} + 2i\mathbb{Z}$. Tedaj velja

$$2\Lambda_1 = 2\mathbb{Z} + 2i\mathbb{Z} \subseteq \mathbb{Z} + 2i\mathbb{Z} = \Lambda_2,$$

zato množenje z 2, kot avtomorfizem kompleksne ravnine $\mathbb{C}$, po zgledu 4.20 inducira holomorfno preslikavo med kompleksnima torusoma

$$\mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2, \quad z + \Lambda_1 \mapsto 2z + \Lambda_2.$$

Opazimo, da ta preslikava *ni* biholomorfizem, saj $2\Lambda_1 \neq \Lambda_2$ (obstaja točka $1 + 2i \in \Lambda_2 \setminus 2\Lambda_1$). Da inducirana preslikava ni biholomorfna, alternativno vidimo že iz njene neinjektivnosti – dve različni točki $0 + \Lambda_1$ in $\frac{1}{2} + \Lambda_1$ iz $\mathbb{C}/\Lambda_1$ se namreč preslikata v isto točko $0 + \Lambda_2 \in \mathbb{C}/\Lambda_2$.

## 5. Uniformizacija

Zadnje poglavje o uniformizaciji povezuje vsa prejšnja. Na začetku se bomo posvetili mrežam v kompleksni ravnini in si ogledali, kako smemo dano mrežo transformirati, da še vedno ostanemo v istem izomorfnostnem razredu kompleksnih torusov, ki ju dani mreži porodita, po navdihu razprave o holomorfnih preslikavah iz zaključka prejšnjega poglavja. Ena od teh podob mreže bo prav posebne oblike, kar bomo izkoristili za nekoliko drugačno interpretacijo Eisensteinovih vrst $G_k(\Lambda)$ iz 3. poglavja, in sicer kot holomorfnih funkcij na zgornji polravnivni

$$\mathfrak{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}.$$

To analogijo bomo nadaljevali še z $j$-invarianto, kjer se bomo dotaknili *modularnih funkcij* z mnogo simetrije, povezanih z grupo $\mathrm{SL}_2(\mathbb{Z})$.

Nadaljevali bomo s konstrukcijo preslikave, ki nam jo je namigoval izrek 3.24. Ta preslikava se bo preko kompleksnih struktur, ki smo ju za kompleksni torus in eliptično krivuljo konstruirali v prejšnjem poglavju, izkazala za bijekcijo in celo biholomorfizem. Interpretacija $j$-invariante kot modularne funkcije nam bo nazadnje omogočila vse skupaj povezati in združiti kompleksne toruse in eliptične krivulje nad poljem $\mathbb{C}$ v uniformizacijskem izreku 5.18.

5.1. **Mreže in modularnost.** Spomnimo se trditve 4.21, ki opisuje holomorfne preslikave med kompleksnima torusoma. V primeru, ko imamo holomorfno preslikavo $\mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$, smo ugotvili, da za mreži $\Lambda_1$ in $\Lambda_2$ obstaja takšen $\alpha \in \mathbb{C}^*$, da je $\alpha\Lambda_1 \subseteq \Lambda_2$. Če pa je $\mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ dodatno še biholomorfina, velja analogna zveza za $\alpha^{-1} \in \mathbb{C}^*$, torej $\alpha^{-1}\Lambda_2 \subseteq \Lambda_1$. Skupaj je to razvidno v enakosti

$$\alpha\Lambda_1 = \Lambda_2.$$

Z drugimi besedami to pomeni, da obstaja kompozicija središčnega raztega in rotacije okoli izhodišča – skupaj *homotetija* kompleksne ravnine, ki eno mrežo preslika v drugo.

**Definicija 5.1.** Pravimo, da sta mreži $\Lambda_1$ in $\Lambda_2$ *homotetični* ali *ekvivalentni*, kadar obstaja $\alpha \in \mathbb{C}^*$, da velja $\alpha\Lambda_1 = \Lambda_2$. To označimo z $\Lambda_1 \simeq \Lambda_2$.

**Opomba 5.2.** Dve podmnožici v evklidski ravnini imamo za *podobni*, kadar obstaja kompozicija translacij, rotacij, središčnih raztegov in zrcaljenj, ki eno podmnožico preslika v drugo. Biti homotetičen torej *ni* isto kot biti podoben. Pomembno je, da homotetije dodatno ohranjajo tudi orientacijo in izhodišče, kar na primer ni res za zrcaljenja in translacije. Opomnimo še, da je homotetičnost očitno ekvivalenčna relacija.

**Primer 5.3.** Mreži $\langle 1, \frac{1}{3} + i\rangle$ in $\langle 1, -\frac{1}{3} + i\rangle$ sta si podobni, saj med njima prehajamo z zrcaljenjem preko imaginarne osi, nista pa homotetični, kot bo kmalu razvidno iz trditve 5.8 in izreka 5.7 v nadaljevanju.

Pri mrežah je do izraza prišel t. i. fundamentalni paralelogram in posebej ima pomen razmerje dolžin njegovih stranic. Če na paralelogramu delujemo s togimi transformacijami in v posebnem s homotetijami, ugotovimo, da to razmerje ostaja vseskozi nespremenjeno – predstavlja invarianto paralelograma. Tako lahko s kompozicijo skaliranja in rotacije vedno normaliziramo eno od stranic paralelograma na dolžino 1 in da ta leži na pozitivnem poltraku realne osi.

Zaradi tesne zveze mrež s svojimi fundamentalnimi paralelogrami, smo motivirani podobno storiti tudi z mrežami – do homotetije natančno najti neko kanonični obliko zanje. Tudi tukaj lahko zahtevamo, da je ena od osnovnih period fiksirana na 1. Natančneje splošno mrežo $\Lambda = \langle \omega_1, \omega_2\rangle$, preko homotetije, ki je množenje z $\omega_1^{-1}$, predstavimo kot

$$\Lambda \simeq \langle 1, \tau\rangle,$$

kjer je $\tau = \frac{\omega_2}{\omega_1}$. Brez škode za splošnost lahko predpostavimo, da je $\mathrm{Im}\left(\frac{\omega_2}{\omega_1}\right) > 0$, saj v nasprotnem primeru, ko je $\mathrm{Im}\left(\frac{\omega_2}{\omega_1}\right) < 0$, z menjavo vlog osnovnih period $\omega_1$ in $\omega_2$

dosežemo želeno. Tako vidimo, da lahko poljubni mreži $\Lambda$ priredimo tak $\tau \in \mathfrak{H}$, da je $\Lambda \simeq \langle 1, \tau \rangle$.

5.1.1. *Modularna grupa.* Naslednje se porodi vprašanje o enoličnosti izbire predstavnika $\tau \in \mathfrak{H}$, prirejenega neki določeni mreži $\Lambda$. Izkaže se, kot bomo tudi videli, da imamo na voljo precej veliko primernih $\tau \in \mathfrak{H}$, ki skupaj z 1 generirajo mreže, ekvivalentne $\Lambda$.

Na prvi tak primer naletimo, ko pogledamo mrežo $\langle 1, \tau \rangle \simeq \Lambda$ po elementih. Sestavljajo jo namreč vse $\mathbb{Z}$-linearne kombinacije generatorjev 1 in $\tau$. Te so oblike $m + n\tau$, kjer sta $m$ in $n$ celi števili. Opazimo, da vsak tak element leži tudi v mreži $\langle 1, \tau + 1 \rangle$, saj ga lahko zapišemo kot

$$m + n\tau = (m - n) + n(\tau + 1).$$

Obenem pa je vsak element mreže $\langle 1, \tau + 1 \rangle$ jasno tudi del mreže $\langle 1, \tau \rangle$, torej sta ti dve mreži v resnici enaki, predstavnika $\tau$ in $\tau + 1$ pa oba ležita v zgornji polravnini.

Še en pomemben primer ekvivalentnih mrež sta $\langle 1, \tau \rangle$ in $\left\langle 1, -\frac{1}{\tau} \right\rangle$. Res sta ekvivalentni, saj imamo homotetijo

$$(-\tau) \cdot \left\langle 1, -\tfrac{1}{\tau} \right\rangle = \langle 1, \tau \rangle ,$$

hkrati pa je tudi $-\frac{1}{\tau} \in \mathfrak{H}$, torej je mreža $\left\langle 1, -\frac{1}{\tau} \right\rangle$ ekvivalentna mreži $\Lambda$.

Tako smo ugotovili, da transformaciji

$$T : \tau \mapsto \tau + 1 \quad \text{in} \quad S : \tau \mapsto -\tfrac{1}{\tau}$$

preslikata zgornjo polravnino $\mathfrak{H}$ samo vase, še pomembneje pa ohranjata ekvivalenčni razred mreže $\Lambda$. Iz tranzitivnosti relacije homotetičnosti mrež vidimo, da bo vsaka mreža $\langle 1, \tau' \rangle$, kjer $\tau'$ dobimo kot neko zaporedje delovanj transformacij $S$ in $T$ na $\tau$, ekvivalentna mreži $\langle 1, \tau \rangle$. Poleg tega pa sta ti dve transformaciji v tesni zvezi z zelo posebno grupo in njenim delovanjem na zgornji polravnini. Tu se vplete t. i. *specialna linearna grupa* $\mathrm{SL}_2(\mathbb{Z})$, ki ji bomo rekli tudi *modularna grupa*[4]

$$\Gamma = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \; a, b, c, d \in \mathbb{Z} \text{ in } ad - bc = 1 \right\},$$

in je diskretna podgrupa splošne linearne grupe $\mathrm{GL}_2(\mathbb{C})$.

Spomnimo se, da preko *Möbiusovih transformacij* ali *lomljenih linearnih preslikav* že poznamo delovanje grupe $\mathrm{GL}_2(\mathbb{C})$ na Riemannovi sferi $\widehat{\mathbb{C}}$ na sledeč način:

$$\mathrm{GL}_2(\mathbb{C}) \to \mathrm{Aut}(\widehat{\mathbb{C}}), \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \left( z \mapsto \frac{az + b}{cz + d} \right), \tag{5.1}$$

kjer vrednost racionalne funkcije $z \mapsto \frac{az+b}{cz+d}$ interpretiramo kot $\infty$ v točki $z = -\frac{d}{c}$ ter $\frac{a}{c}$ v točki $z = \infty$, kadar je $c \neq 0$, in kot $\infty$ v točki $z = \infty$, kadar je $c = 0$. Delovanje elementa $\gamma = \left( \begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \in \mathrm{GL}_2(\mathbb{C})$ na $z \in \widehat{\mathbb{C}}$ označimo kot

$$\gamma z = \begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az + b}{cz + d}. \tag{5.2}$$

[4]Ponekod v literaturi je bolj standardno modularna grupa nekoliko manjša kvocientna grupa $\mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$. Razlog za to se skriva v dejstvu, da delovanje z elementoma $\gamma, -\gamma \in \mathrm{SL}_2(\mathbb{Z})$ določa isti avtomorfizem zgornje polravnine, ima pa tudi določene prednosti pri formulaciji nekaterih izrekov o njej.

**Opomba 5.4.** Opisano delovanje morda izgleda nekoliko komplicirano, a je vendarle zelo naravno. Izhaja namreč iz delovanja grupe $\mathrm{GL}_2(\mathbb{C})$ na kompleksni projektivni premici $\mathbb{P}^1_{\mathbb{C}}$, podanega s predpisom

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \big([x:y] \mapsto [ax+by : cx+dy]\big).$$

Če $\mathbb{C}$ identificiramo s točkami oblike $[z:1]$ iz $\mathbb{P}^1_{\mathbb{C}}$, točko v neskončnosti $\infty \in \widehat{\mathbb{C}}$ pa s točko $[1:0] \in \mathbb{P}^1_{\mathbb{C}}$, dobimo ravno lomljeno linearno preslikavo od prej.

*Komentar.* Odslej naj matrika $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, če ne bo drugače rečeno, vedno predstavlja element $\gamma \in \Gamma$.

Ker je $\Gamma$ podgrupa v $\mathrm{GL}_2(\mathbb{C})$, je z istim predpisom definirano tudi delovanje grupe $\Gamma$ na Riemannovi sferi. Zaradi posebne strukture grupe $\Gamma$ lahko pokažemo, da avtomorfizmi, porojeni z delovanjem te grupe, ohranjajo predznak imaginarnega dela. Natančneje imamo naslednjo trditev.

**Trditev 5.5.** *Za vse $z \in \mathbb{C}$ in $\gamma \in \Gamma$ velja*

$$\mathrm{Im}(\gamma z) = \frac{\mathrm{Im}(z)}{|cz+d|^2}. \tag{5.3}$$

*Dokaz.* Zvezo preverimo z računom.

$$\begin{aligned} \mathrm{Im}(\gamma z) &= \mathrm{Im}\left(\frac{az+b}{cz+d}\right) = \mathrm{Im}\left(\frac{(az+b)(c\bar{z}+d)}{|cz+d|^2}\right) = \\ &= \mathrm{Im}\left(\frac{ac\,|z|^2 + bd + adz + bc\bar{z}}{|cz+d|^2}\right) = \frac{(ad-bc)\,\mathrm{Im}(z)}{|cz+d|^2} = \frac{\mathrm{Im}(z)}{|cz+d|^2} \qquad \square \end{aligned}$$

**Opomba 5.6.** Tako vidimo, da zaradi zveze (5.3) predpis (5.2) podaja dobro definirano delovanje grupe $\Gamma$ na zgornji polravnini $\mathfrak{H}$.

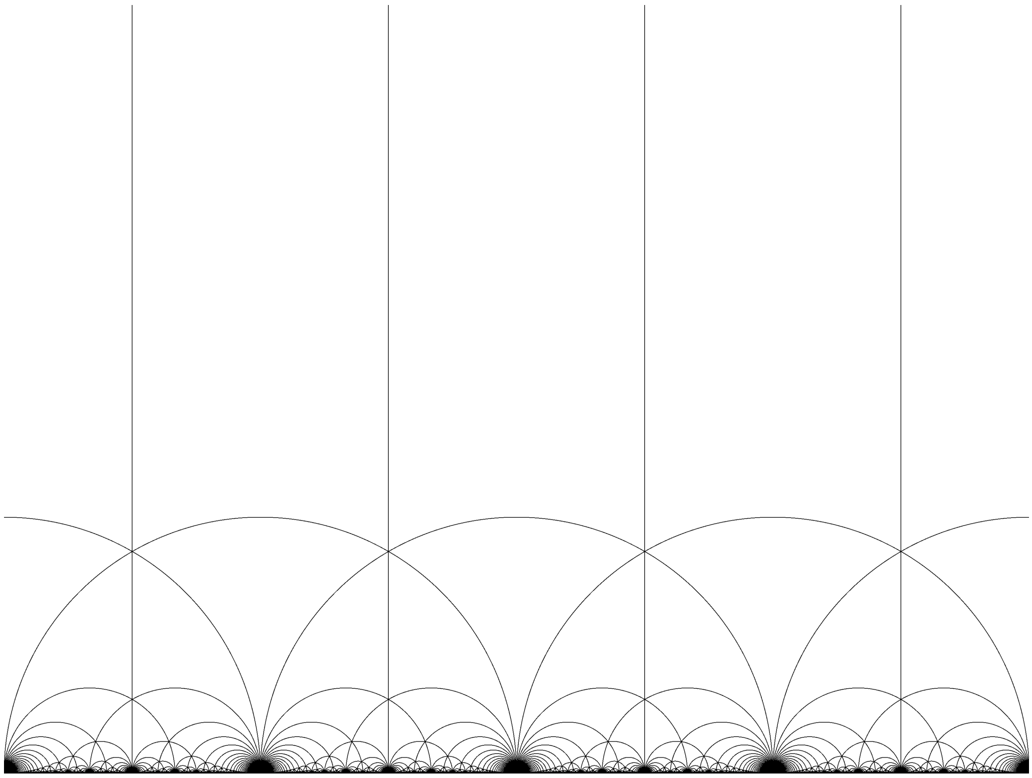
V smislu grupe $\Gamma$ lahko sedaj transformaciji $T$ in $S$ od prej predstavimo tudi kot elementa te grupe. Ustrezata jima istoimenovana grupna elementa

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{in} \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

saj zanju velja $Tz = z+1$ in $Sz = -1/z$. Poleg tega $T$ in $S$ nista zanimiva le z vidika njunih delovanj na mrežah, ampak celo generirata modularno grupo $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. Njuni sliki v kvocientni grupi $\Gamma/\{\pm I\}$ imata namreč vlogo generatorjev, za kar se skličemo na izrek [8, VII, §1, theorem 2], element $-I \in \Gamma$ pa lahko izrazimo s $S$ kot $S^2 = -I$. Skupaj to pomeni, da $S$ in $T$ geneirata celotno grupo $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. V smislu avtomorfizmov Riemannove sfere, $S$ in $T$ generirata podgrupo v $\mathrm{Aut}(\widehat{\mathbb{C}})$, ki je slika zožitve homomorfizma (5.1) na podgrupo $\Gamma$. Več o tem najdemo v [8, VII, §1].

*Fundamentalna domena.* V začetku poglavja 3 smo vpeljali pojem fundamentalnega paralelograma mreže. To je povezana množica v $\mathbb{C}$, ki vsebuje po enega predstavnika vsakega ekvivalenčnega razreda kvocienta $\mathbb{C}/\Lambda$ oz. z drugimi besedami vsebuje po enega predstavnika vsake orbite delovanja $\Lambda$ na $\mathbb{C}$. Podobno območje imamo tudi pri delovanju modularne grupe $\Gamma$ na $\mathfrak{H}$, to je množica

$$D = \{z \in \mathfrak{H} \mid |\mathrm{Re}(z)| \leq 1/2 \text{ in } |z| \geq 1\},$$



SLIKA 3. Delovanje modularne grupe $\Gamma$ na $\mathfrak{H}$. Vir [3].

ki jo imenujemo *fundamentalna domena.* Na sliki 3 vidimo, kako fundamentalno domeno $D$ transformirajo nekateri elementi grupe $\Gamma$.

Naslednja trditev pove, da vsaka orbita seka fundamentalno domeno vsaj v eni točki.

**Trditev 5.7.** *Za vsak $z \in \mathfrak{H}$ obstaja $\gamma \in \Gamma$, da je $\gamma z \in D$.*

*Dokaz.* Spomnimo se identitete (5.3), ki nam pove, kako se transformira imaginarni del kompleksnega števila, ko na njem delujemo z grupo $\Gamma$. Izraz $|cz + d|$ meri razdaljo elementa $cz+d$ iz mreže $\langle 1, z\rangle$ do izhodišča. Za dano konstanto $M > 0$ tako že vemo, da obstaja zgolj končno mnogo parov $(c, d) \in \mathbb{Z}^2$, da je $|cz + d| < M$. V posebnem imamo torej tudi končno mnogo parov $(c, d)$, kjer sta $c$ in $d$ tuji in zadoščata tej oceni. Kadar sta $c$ in $d$ tuji, namreč ravno ustrezata nekemu elementu $\gamma' \in \Gamma$, saj tedaj obstajata še $a, b \in \mathbb{Z}$, da velja $ad - bc = 1$. Za neki tak par $(c, d)$ oz. element $\gamma' \in \Gamma$ je vrednost izraza $|cz + d|$ minimalna. Posledično je zato vrednost $\operatorname{Im}(\gamma' z)$ maksimalna. Vzemimo enega izmed teh $\gamma' \in \Gamma$, pri katerem je $\operatorname{Im}(\gamma' z)$ maksimalna, in s $T$ delujmo na $\gamma' z$ tolikokrat, da bo za $z' = T^n \gamma' z$ veljalo

$$-1/2 \leq \operatorname{Re}(z') \leq 1/2.$$

To je vedno mogoče, saj delovanje z elementom $T$ predstavlja translacijo za eno enoto v pozitivni smeri realne osi. Ob tem še opomnimo, da takšne translacije s $T$ nimajo vpliva na imaginarni del, torej na koncu še vedno velja $\operatorname{Im}(z') = \operatorname{Im}(\gamma' z)$.

Če je tedaj $|z'| \geq 1$, smo končali in lahko vzamemo $\gamma = T^n \gamma'$, za katerega velja $\gamma z \in D$. V nasprotnem primeru, če je $|z'| < 1$, pa ugotovimo, da velja $\operatorname{Im}(Sz') = \frac{\operatorname{Im}(z')}{|z'|^2} > \operatorname{Im}(z')$, kar je v nasprotju z maksimalnostjo $\operatorname{Im}(z') = \operatorname{Im}(\gamma' z)$, torej do tega primera sploh ne pridemo. $\square$

*Komentar.* Z našo definicijo fundamentalne domene $D$ zares ne dosežemo, da ta vsebuje *enoličnega* predstavnika iz vsake orbite, saj nekatere točke na robu domene še vedno ležijo v isti orbiti. Imamo pa te vrste enoličnost v notranjosti domene $D$. Natančneje $z$ in $z'$ iz $D$ ležita v isti orbiti natanko tedaj, ko je $|\mathrm{Re}(z)| = \frac{1}{2}$ in $z = z' \pm 1$ ali pa je $|z| = 1$ in je $z' = -1/z$. Dokaz tega najdemo v [8, VII, §1, theorem 1].

Vrnimo se sedaj nazaj k mrežam oblike $\langle 1, \tau \rangle$, kjer je $\tau \in \mathfrak{H}$. Omenili smo že, da sta mreži $\langle 1, \tau_1 \rangle$ in $\langle 1, \tau_2 \rangle$ homotetični, če med $\tau_1$ in $\tau_2$ lahko prehajamo z nekim zaporedjem delovanj $S$ in $T$. Naslednja trditev nam poda karakterizacijo homotetičnosti mrež preko modularne grupe $\Gamma$.

**Trditev 5.8.** *Naj bosta $\Lambda_1 = \langle 1, \tau_1 \rangle$ in $\Lambda_2 = \langle 1, \tau_2 \rangle$ mreži s $\tau_1, \tau_2 \in \mathfrak{H}$. Tedaj velja $\Lambda_1 \simeq \Lambda_2$ natanko tedaj, ko obstaja $\gamma \in \Gamma$, da je*

$$\tau_1 = \gamma \tau_2.$$

*Dokaz.* Denimo, da velja $\Lambda_1 \simeq \Lambda_2$. Tedaj obstaja $\alpha \in \mathbb{C}^*$, da je $\langle \alpha, \alpha\tau_1 \rangle = \langle 1, \tau_2 \rangle$. To pomeni, da lahko osnovni periodi $\alpha$ in $\alpha\tau_1$ izrazimo kot $\mathbb{Z}$-linearni kombinaciji 1 in $\tau_2$, denimo

$$\alpha\tau_1 = a\tau_2 + b \quad \text{in} \quad \alpha = c\tau_2 + d$$

za neke $a, b, c, d \in \mathbb{Z}$. Z drugimi besedami to pomeni, da obstaja celoštevilska matrika $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, ki bazo $(1, \tau_2)$ preslika v bazo $(\alpha, \alpha\tau_1)$. Ker je homotetičnost mrež ekvivalenčna relacija, po enakem razmisleku obstaja tudi celoštevilska matrika $\gamma'$, ki bazo $(1, \tau_1)$ preslika v bazo $(\alpha^{-1}, \alpha^{-1}\tau_2)$, od koder sledi, da sta $\gamma$ in $\gamma'$ obrnljivi. Determinanta celoštevilske obrnljive matrike je lahko samo 1 ali $-1$, ker pa velja

$$\mathrm{Im}(\tau_1) = \mathrm{Im}\left(\frac{a\tau_2 + b}{c\tau_2 + d}\right) = \frac{(ad - bc)\,\mathrm{Im}(\tau_2)}{|c\tau_2 + d|^2} > 0$$

in sta $\tau_1, \tau_2 \in \mathfrak{H}$, mora biti $\det \gamma = ad - bc = 1$ oz. $\gamma \in \Gamma$ in tako je $\tau_1 = \gamma\tau_2$.

Obratno, če velja $\tau_1 = \gamma\tau_2$ za neki $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, imamo

$$\langle 1, \tau_1 \rangle = \left\langle 1, \tfrac{a\tau_2 + b}{c\tau_2 + d} \right\rangle \simeq \langle c\tau_2 + d, a\tau_2 + b \rangle,$$

preko homotetije, ki jo porodi množenje s številom $\alpha = c\tau_2 + d$. Ker je $\mathrm{Im}(\tau_2) > 0$, je $\alpha$ res neničeln. Opazimo, da je mreža $\langle c\tau_2 + d, a\tau_2 + b \rangle$ kar enaka $\langle 1, \tau_2 \rangle$, saj lahko njeni osnovni periodi 1 in $\tau_2$ izrazimo kot $\mathbb{Z}$-linearni kombinaciji osnovnih period $a\tau_2 + b$ in $c\tau_2 + d$:

$$\begin{aligned} a(c\tau_2 + d) - c(a\tau_2 + b) &= ad - bc = 1, \\ d(a\tau_2 + b) - b(c\tau_2 + d) &= (ad - bc)\tau_2 = \tau_2. \end{aligned}$$

Ker je $\gamma \in \Gamma$, smo upoštevali $ad - bc = 1$. Tako dobimo $\langle 1, \tau_1 \rangle \simeq \langle 1, \tau_2 \rangle$. □

Zgornja diskusija o fundamentalni domeni $D$ in prejšnja trditev nam tako povesta, da lahko vsaki mreži $\Lambda \subseteq \mathbb{C}$ priredimo točko $\tau \in D$ v fundamentalni domeni, da je $\Lambda \simeq \langle 1, \tau \rangle$.

5.1.2. *Modularne funkcije.*

**Definicija 5.9.** Naj bo $k$ celo število. Meromorfna funkcija $f$ na zgornji polravnini $\mathfrak{H}$ je *šibko modularna reda* $2k$, če zadošča *modularnostnemu pogoju*

$$f(z) = (cz + d)^{-2k} f\left(\frac{az + b}{cz + d}\right) \quad \text{za vse} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}). \tag{5.4}$$

Če dodatno obstaja limita $f$ v neskončnosti (v posplošenem smislu – dovoljujemo tudi konvergenco proti $\infty$), pravimo, da je $f$ *modularna funkcija reda* $2k$.

**Opomba 5.10.** Matriki $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ in $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ generirata grupo $\mathrm{SL}_2(\mathbb{Z})$, zato se modularnostni pogoj prepiše v ekvivalentnega

$$f(z) = z^{-2k} f(-1/z) \quad \text{ in } \quad f(z) = f(z+1),$$

za vse $z \in \mathfrak{H}$, od koder vidimo, da so vse (šibko) modularne funkcije v posebnem tudi periodične s periodo 1.

**Opomba 5.11.** Definicija namiguje, da šibko modularnih funkcij lihega reda sploh ni in izkaže se, da je to res, če ob tem izvzamemo ničelno funkcijo. Če bi namreč $f$ bila lihega reda, za $\gamma = -I \in \mathrm{SL}_2(\mathbb{Z})$ velja

$$f(z) = (-1)^{2k+1} f(\gamma z) = -f(z) \quad \text{ za vse } z \in \mathfrak{H},$$

od koder sledi $f = 0$.

*Eisensteinove vrste.* Zaenkrat nimamo še nobenih konkretnih primerov (šibko) modularnih funkcij, razen konstant. Videli pa bomo, da bodo Eisensteinove vrste reda $2k$, kjer je $k > 1$, prirejene mreži $\Lambda$

$$G_{2k}(\Lambda) = \sum_{\omega \in \Lambda'} \frac{1}{\omega^{2k}},$$

služile kot dober vir za konstrukcijo prvih netrivialnih primerov modularnih funkcij. V ta namen si poglejmo naslednjo trditev.

**Trditev 5.12.** *Naj bo $\Lambda$ mreža v $\mathbb{C}$ in $\alpha \in \mathbb{C}^*$. Tedaj velja*

$$G_{2k}(\alpha\Lambda) = \alpha^{-2k} G_{2k}(\Lambda) \tag{5.5}$$

*Dokaz.* Identiteto pokažemo z računom

$$G_{2k}(\alpha\Lambda) = \sum_{\omega \in \Lambda'} \frac{1}{(\alpha\omega)^{2k}} = \alpha^{-2k} \sum_{\omega \in \Lambda'} \frac{1}{\omega^{2k}} = \alpha^{-2k} G_{2k}(\Lambda). \qquad \square$$

Za poljuben $\tau \in \mathfrak{H}$ imamo mrežo $\langle 1, \tau \rangle$, na kateri lahko izračunamo vrsto $G_{2k}$. Tako dobimo funkcijo z enako oznako, podano s predpisom

$$G_{2k} : \mathfrak{H} \to \mathbb{C}, \quad G_{2k}(\tau) = \sum_{(m,n) \in \mathbb{Z}^2 \setminus \{(0,0)\}} \frac{1}{(m + n\tau)^{2k}}.$$

Naj bo $\gamma \in \Gamma$ poljuben. Homotetični mreži $\langle 1, \tau \rangle$ in $\langle 1, \gamma\tau \rangle$, kot v dokazu trditve 5.8, povezuje $\alpha = c\tau + d$, da velja

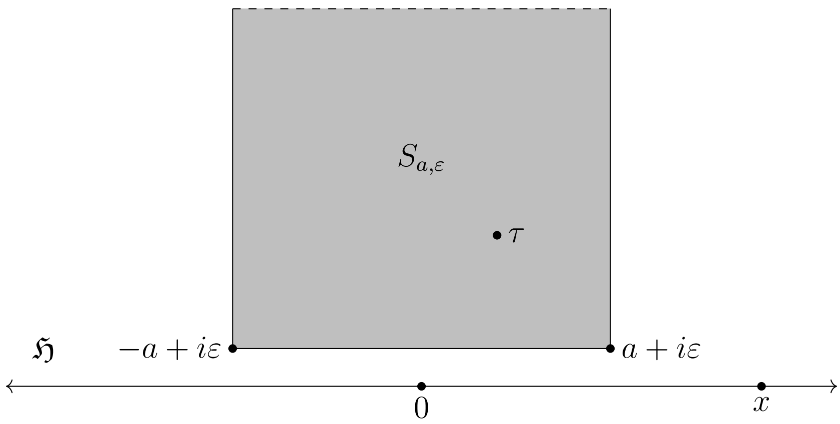
$$\langle 1, \tau \rangle = \alpha \left\langle 1, \tfrac{a\tau + b}{c\tau + d} \right\rangle.$$

Preko zveze (5.5) lahko tako izpeljemo modularnostni pogoj za funkcijo $G_{2k}$

$$G_{2k}(\tau) = (c\tau + d)^{-2k} G_{2k}\left(\frac{a\tau + b}{c\tau + d}\right).$$

Nekoliko tehničen dokaz nam pokaže še, da so funkcije $G_{2k} : \mathfrak{H} \to \mathbb{C}$ tudi holomorfne.

**Trditev 5.13.** *Naj bo $k > 1$ naravno število. Eisensteinova vrsta reda $2k$ s predpisom $G_{2k}(\tau) = G_{2k}(\langle 1, \tau \rangle)$ podaja holomorfno funkcijo $\mathfrak{H} \to \mathbb{C}$ na zgornji polravnini.*




Slika 4. Množica $S_{a,\varepsilon}$ v zgornji polravnini $\mathfrak{H}$.

*Dokaz.* Zaradi Weierstrassovega M-testa in izreka 3.19 zadošča vsak člen vrste $G_{2k}$ po kompaktih v $\mathfrak{H}$ majorizirati s členom neke konvergentne vrste. Če je $K \subseteq \mathfrak{H}$ poljuben kompakt, obstajata taka $a, \varepsilon > 0$, da je $K$ vsebovan v množici

$$S_{a,\varepsilon} = \{z \in \mathfrak{H} \mid |\mathrm{Re}(z)| \leq a,\ \mathrm{Im}(z) \geq \varepsilon\}.$$

Izkaže se, da obstaja tak $\delta \in (0,1)$, za katerega je

$$|m + n\tau| \geq \delta\, |m + ni|\,, \tag{5.6}$$

za vse $(m,n) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ in vse $\tau \in S_{a,\varepsilon}$. To oceno uporabimo na kompaktu $K$ za majorizacijo vsakega od členov vrste $G_{2k}(\tau)$ na sledeč način

$$\frac{1}{|m+n\tau|^{2k}} \leq \delta^{-2k} \frac{1}{|m+ni|^{2k}}.$$

Zadnje predstavlja ravno s konstanto pomnožen člen absolutno konvergentne vrste $G_{2k}(\langle 1, i\rangle)$, zato je $G_{2k}$ res holomorfna na $\mathfrak{H}$.

Vrnimo se sedaj še k oceni (5.6). Če je $n = 0$, ocena drži za katerikoli $\delta < 1$, zato bo ekvivalentno pokazati obstoj takega $\delta \in (0,1)$, da bo za vse $(m,n) \in \mathbb{Z}^2$, kjer je $n \neq 0$, in $\tau \in S_{a,\varepsilon}$ veljalo

$$\left| \frac{\tau + \frac{m}{n}}{i + \frac{m}{n}} \right| \geq \delta.$$

Definirajmo funkcijo $f : S_{a,\varepsilon} \times \mathbb{R} \to (0, \infty)$ s predpisom $f(\tau, x) = \left|\frac{\tau - x}{i - x}\right|$. Za vsak fiksen $\tau$ velja $\lim_{x\to\pm\infty} f(\tau, x) = 1$, torej obstaja $R_\tau > 0$, da je $\left|\frac{\tau-x}{i-x}\right| \geq \frac{1}{2}$ za vse $|x| \geq R_\tau$. Hkrati pa zaradi zveznosti funkcija $f$ na kompaktu $\{\tau\} \times [-R_\tau, R_\tau]$ doseže minimum $c_\tau > 0$. Tedaj zadošča vzeti $\delta_\tau = \min\{c_\tau, \frac{1}{2}\}$, za katerega je $f(\tau, x) \geq \delta_\tau$ za vse $x \in \mathbb{R}$.

To oceno izpeljimo še enakomerno glede na $\tau$. Za poljuben $\tau \in S_{a,\varepsilon}$ in $x > a$ velja

$$\left|\frac{\tau - x}{i - x}\right| \geq \left|\frac{a + i\varepsilon - x}{i - x}\right|,$$

kot vidimo na sliki 4, torej bo za vse $\tau \in S_{a,\varepsilon}$ in vse $x > a$ veljalo $\left|\frac{\tau-x}{i-x}\right| \geq \delta_{a+i\varepsilon}$. Simetrično lahko sklepamo, da bo $\left|\frac{\tau-x}{i-x}\right| \geq \delta_{-a+i\varepsilon}$ za vse $\tau \in S_{a,\varepsilon}$ in vse $x < -a$. Za $x \in [-a, a]$ in vse $\tau \in S_{a,\varepsilon}$ pa velja $\left|\frac{\tau-x}{i-x}\right| \geq \frac{\varepsilon}{|i-x|} \geq \frac{\varepsilon}{|i-a|}$. Skupaj je torej

$$\left|\frac{\tau - x}{i - x}\right| \geq \delta, \qquad \text{za vse } \tau \in S_{a,\varepsilon} \text{ in vse } x \in \mathbb{R},$$

če za $\delta$ vzamemo $\delta := \min\left\{\delta_{a+i\varepsilon}, \delta_{-a+i\varepsilon}, \frac{\varepsilon}{|i-a|}\right\} \in (0,1)$, kar zaključi dokaz. $\square$

Pomembna lastnost funkcij $G_{2k}$, ki bo tudi precej koristna, je njihovo obnašanje v neskončnosti. Naj $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ označuje *Riemannovo $\zeta$-funkcijo*, kjer je $\mathrm{Re}(s) > 1$. Tedaj velja naslednja trditev.

**Trditev 5.14.** *Za funkcije $G_{2k}$ obstaja limita v neskončnosti, ki je končna in enaka*

$$\lim_{\tau \to \infty} G_{2k}(\tau) = 2\zeta(2k).$$

*Dokaz.* Izračunajmo limito preko zaporedij. Naj bo $(z_\ell)_{\ell \in \mathbb{N}}$ poljubno zaporedje v zgornji polravnini $\mathfrak{H}$, ki konvergira proti $\infty$[5]. Ker $G_{2k}$ zadošča modularnostnemu pogoju, je v posebnem invariantna na translacije s $T$, zato lahko brez škode za splošnost predpostavimo, da za vsak člen zaporedja velja $-\frac{1}{2} \leq \mathrm{Re}(z_\ell) \leq \frac{1}{2}$. Poleg tega, zaradi konvergence proti $\infty$, obstaja $\varepsilon > 0$, da je $\mathrm{Im}(z_\ell) > \varepsilon$ za vse $\ell \in \mathbb{N}$. Tako smemo predpostaviti, da zaporedje $(z_\ell)_{\ell \in \mathbb{N}}$ leži v množici $S_{1/2,\varepsilon}$. Iz dokaza trditve 5.13 vemo, da $G_{2k}$ na množicah te oblike konvergira enakomerno, torej lahko zamenjamo limiti

$$\lim_{\ell \to \infty} G_{2k}(z_\ell) = \sum_{(m,n) \in \mathbb{Z}^2 \setminus \{0\}} \lim_{\ell \to \infty} \frac{1}{(m + n z_\ell)^{2k}} = \sum_{m \in \mathbb{Z} \setminus \{0\}} \frac{1}{m^{2k}} = 2 \cdot \sum_{m=1}^{\infty} \frac{1}{m^{2k}} = 2\zeta(2k),$$

kar da željeni rezultat. Omenimo še, da v vsoti limit (po menjavi vrstnega reda limite in seštevanja) neničelni prispevek primorejo samo členi pri indeksih oblike $(m, 0)$, za $m \in \mathbb{Z} \setminus \{0\}$, kar pojasni drugi enačaj. $\square$

Tako družina funkcij $G_{2k}$ podaja prvi netrivialen primer modularnih funkcij redov $2k$, za vsa naravna števila $k > 1$.

*Modularna diskriminanta.* Iz definicije je razvidno, da je množica šibko modularnih funkcij danega reda $2k$ zaprta za $\mathbb{C}$-linearne kombinacije, torej tvori kompleksen vektorski prostor. Na ta način lahko iz danih šibko modularnih funkcij reda $2k$ dobimo nove, ki so spet reda $2k$. Pomembna konstrukcija, ki nam omogoča prehajanje med različnimi redi, pa je produkt. Če sta $f_1$ in $f_2$ šibko modularni redov $2k_1$ in $2k_2$, je njun produkt $f_1 f_2$ šibko modularna funkcija reda $2k_1 + 2k_2$. To sledi iz modularnostnega pogoja, ki mu zadošča $f_1 f_2$. Za vsak $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ namreč velja

$$\begin{aligned} f_1(z) f_2(z) &= (cz+d)^{-2k_1} f_1(\gamma z)\,(cz+d)^{-2k_2} f_2(\gamma z) \\ &= (cz+d)^{-2k_1-2k_2} f_1 f_2(\gamma z). \end{aligned}$$

Kompleksen vektorski prostor vseh šibko modularnih funkcij tako postane kompleksna algebra z enoto, ki je konstantna funkcija 1 reda 0.

Spomnimo se oznak $g_2(\Lambda) = 60 G_4(\Lambda)$ in $g_3(\Lambda) = 140 G_6(\Lambda)$ iz poglavja 3. Povsem analogno definiramo modularni funkciji

$$g_2(\tau) = 60 G_4(\tau) \quad \text{in} \quad g_3(\tau) = 140 G_6(\tau)$$

redov 4 in 6. Iz njiju lahko konstruiramo *modularno diskriminanto*

$$\Delta = g_2^3 - 27 g_3^2,$$

[5]Zaporedje $(z_n)_{n \in \mathbb{N}}$ *konvergira* proti $\infty$, kadar za vsak $M > 0$ obstaja $n_0 \in \mathbb{N}$, da za vse $n \in \mathbb{N}$, za katere je $n \geq n_0$, velja $|z_n| > M$.

ki je šibko modularna funkcija reda 12. Poleg tega $\Delta$ nima ničle na zgornji polravnini $\mathfrak{H}$, kot smo preko mrež in Weierstrassove $\wp$-funkcije videli v dokazu trditve 3.26. Trditev 5.14 pa nam omogoči sklepati še o njeni limiti v neskončnosti, ki je

$$\lim_{\tau\to\infty} \Delta(\tau) = 0.$$

Za izračun te limite smo uporaili limiti

$$\lim_{\tau\to\infty} g_2(\tau) = 60 \cdot 2\zeta(4) = \frac{4\pi^4}{3},$$
$$\lim_{\tau\to\infty} g_3(\tau) = 140 \cdot 2\zeta(6) = \frac{8\pi^6}{27}.$$

Za izračun slednjih, pa smo uporabili poznani vrednosti $\zeta(4) = \frac{\pi^4}{2\cdot 3^3\cdot 5}$ in $\zeta(6) = \frac{\pi^6}{3^3\cdot 5\cdot 7}$, ki ju lahko izpeljemo s pomočjo Fourierovih vrst in Parsevalove enakosti, ali pa se skličemo na [8, VII, §4.1].

*Modularna $j$-invarianta.* Celotna razprava o modularnih funkcijah nas na koncu privede še do *modularne $j$-invariante.* V osnovi je $j$-invarianta število

$$j = 1728\frac{a^3}{a^3 - 27b^2},$$

prirejeno eliptični krivulji z enačbo $y^2z = 4x^3 - axz^2 - bz^3$, kjer je $a^3 - 27b^2 \neq 0$. Nad poljem kompleksnih števil nam je $j$-invarianta omogočila karakterizirati vse projektivne kubike do projektivne ekvivalence natančno. Na podoben način tedaj vpeljemo *modularno $j$-invarianto*, podano s predpisom

$$j(\tau) = 1728\frac{g_2(\tau)^3}{\Delta(\tau)} = 1728\frac{g_2(\tau)^3}{g_2(\tau)^3 - 27g_3(\tau)^2}.$$

Funkcija $j$ je holomorfna na $\mathfrak{H}$, saj sta takšni že $g_2^3$ in $\Delta$, slednja pa na $\mathfrak{H}$ nima ničle. Poleg tega sta $g_2^3$ in $\Delta$ modularni funkciji in obe sta reda 12. Od tod sledi, da je $j$ modularna funkcija reda 0, kar pomeni, da delovanje grupe $\Gamma$ na njenem argumentu nima vpliva na njeno vrednost – na vsaki $\Gamma$-orbiti delovanja je $j$ konstantna. Njena limita v neskončnosti je

$$\lim_{\tau\to\infty} j(\tau) = \infty,$$

kar je razvidno iz obnašanja funkcij $g_2$ in $\Delta$ v neskončnosti. Vse skupaj lahko povzamemo v naslednji trditvi.

**Trditev 5.15.** *Funkcija $j : \mathfrak{H} \to \mathbb{C}$ je modularna funkcija reda 0 z limito v neskončnosti $\lim_{\tau\to\infty} j(\tau) = \infty$.*

*Komentar.* Kot vsaka modularna funkcija, tudi $j$ zadošča zvezi $j(\tau) = j(\tau+1)$, torej je periodična. Ker je tudi holomorfna, jo lahko razvijemo v nekakšno Fourierovo vrsto. Če pišemo $q = e^{2\pi i\tau}$, nam konec razdelka [8, VII, §3], kjer lahko izvemo še več o $j$-invarianti, zagotovi ravoj

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots .$$

Vrsto te oblike imenujemo tudi *$q$-razvoj.* Število 1728 v predpisu za $j$ je tradicionalno in je najmanjše pozitivno število, ki zagotovi celoštevilskost koeficientov $q$-razvoja $j$-invariante.

5.2. **Izomorfizem $\mathbb{C}/\Lambda \to E(\mathbb{C})$ in uniformizacija.** V tem razdelku podamo izomorfizem Riemannovih ploskev – kompleksnega torusa $\mathbb{C}/\Lambda$ in eliptične krivulje $E_\Lambda(\mathbb{C})$, podane z enačbo

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

Nazadnje s pomočjo modularne $j$-invariante dokažemo še uniformizacijo, ki opisuje, kako poljubni eliptični krivulji nad $\mathbb{C}$ priredimo mrežo $\Lambda$ in posledično njej izomorfen kompleksni torus $\mathbb{C}/\Lambda$.

**Izrek 5.16.** *Naj bo $\Lambda \subseteq \mathbb{C}$ mreža, $\wp$ Weierstrassova eliptična funkcija glede na mrežo $\Lambda$ in naj bo $E(\mathbb{C}) \subseteq \mathbb{P}^2_{\mathbb{C}}$ eliptična krivulja, podana z enačbo*

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

*Tedaj je preslikava $\phi : \mathbb{C}/\Lambda \to E(\mathbb{C})$, 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 biholomorfizem Riemannovih ploskev.*

*Dokaz.* Razdelimo dokaz trditve na naslednje štiri dele: dobro definiranost, zveznost, bijektivnost in holomorfnost preslikave $\phi$.

*Dobra definiranost.* Po izreku 3.24 za poljuben $z \in \mathbb{C} \setminus \Lambda$ velja $[\wp(z) : \wp'(z) : 1] \in E(\mathbb{C})$ in posebej je tudi $[0 : 1 : 0] \in E(\mathbb{C})$, torej bo slika preslikave $\phi$ res vsebovana v eliptični kriulji $E(\mathbb{C})$.

Predpis za $\phi$ je podan na kvocientu $\mathbb{C}/\Lambda$, torej se moramo prepričati še o neodvisnosti 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 velja $z \notin \Lambda$, velja tudi $w \notin \Lambda$, in tedaj zaradi $\Lambda$-periodičnosti funkcije $\wp$ sledi

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

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

*Zveznost.* 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 3.22 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 $\Lambda$-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 $\Lambda$, 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 3.25 vemo, da ima $\wp'$ po tri enostavne ničle na fundamentalnem paralelogramu v polperiodah mreže $\Lambda$, 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 $\Lambda$ smo izvzeli, saj ima v vsaki izmed njih $\wp'$ pol tretje stopnje. Funkciji $\frac{\wp}{\wp'}$ in $\frac{1}{\wp'}$ lahko torej vidimo kot dobro definirani holomorfni $\Lambda$-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 $\phi$ natanko preslikava, ki skupaj s $\pi$ faktorizira preslikavo

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

zato bo zaradi trditve [7, trditev 3.22] dovolj preveriti zveznost $\Phi$, ker je $\pi$ kvocientna. Podali bomo dva predpisa za $\Phi$, 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

$$\begin{aligned} \Phi_0 : U_0 \to E(\mathbb{C}), &\quad z \mapsto [\wp(z) : \wp'(z) : 1]\,, \\ \Phi_1 : U_1 \to E(\mathbb{C}), &\quad z \mapsto \left[\tfrac{\wp(z)}{\wp'(z)} : 1 : \tfrac{1}{\wp'(z)}\right]. \end{aligned}$$

Zaradi omenjenih lastnosti $\frac{\wp}{\wp'}$ in $\frac{1}{\wp'}$ sta $\Phi_0$ in $\Phi_1$ 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

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

saj je $\wp'(z) \in \mathbb{C}^*$ za $z \in \mathbb{C} \setminus \frac{1}{2}\Lambda$. Ker preslikavi $\Phi_0$ in $\Phi_1$ skupaj določata ravno $\Phi$, je slednja zvezna, od koder sledi, da je tudi $\phi$ zvezna.

*Bijektivnost.* Začnimo s surjektivnostjo. Očitno je $\phi(0 + \Lambda) = [0 : 1 : 0]$, zato izberimo poljubno točko oblike $[x_0 : y_0 : 1] \in E(\mathbb{C}) \setminus \{[0 : 1 : 0]\}$. Ker je po trditvi 3.14 eliptična funkcija $\wp$ surjektivna, obstaja $z \in \mathbb{C}\setminus\Lambda$, da je $\wp(z) = x_0$. Iz identitete (3.2) 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 $\phi$. Omejili se bomo samo na injektivnost zožitve $\phi|_{\pi(\mathbb{C}\setminus\Lambda)}$, saj je $0 + \Lambda$ edina točka, ki se preslika v neskončnost, 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 omejitve na območje $\pi(\mathbb{C} \setminus \Lambda)$, imamo opravka samo z afinim delom krivulje $E$ in se zato zgornji pogoj prevede v ekvivalentnega

$$(\wp(z_1), \wp'(z_1)) = (\wp(z_2), \wp'(z_2)). \tag{5.7}$$

Ločimo dve možnosti:

- Če je $2z_1 \in \Lambda$, je $z_1$ polperioda, torej je $\wp'(z_1) = 0$ po lemi 3.25. Posledično iz predpostavke (5.7) sledi $\wp'(z_2) = 0$, zato je tudi $z_2$ polperioda. Predstavnik točke $z_1 + \Lambda$ je tako do prištete periode iz $\Lambda$ natanko ena od polperiod

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

Iz dokaza leme 3.26 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
$$z_2 + \Lambda = \pm z_1 + \Lambda.$$
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 (5.7).

Skupaj je tako $\phi$ res bijektivna.

*Holomorfnost.* Nazadnje si poglejmo, zakaj je $\phi$ holomorfna. Ker je $\pi$ lokalni biholomorfizem, bo zadoščalo pokazati le holomorfnost kompozicije
$$\mathbb{C} \xrightarrow{\pi} \mathbb{C}/\Lambda \xrightarrow{\phi} E(\mathbb{C}) \ .$$
Okoli poljubne točke na $\mathbb{C}/\Lambda$ imamo namreč odprto okolico $U \subseteq \mathbb{C}/\Lambda$ in odprto množico $V \subseteq \mathbb{C}$, da je $(\pi|_V)^{-1} : U \to V$ biholomorfizem (in hkrati tudi lokalna karta za $\mathbb{C}/\Lambda$). Tedaj bo kompozicija holomorfnih preslikav $\phi \circ \pi$ in $(\pi|_V)^{-1}$ spet holomorfna in enaka
$$(\phi \circ \pi) \circ (\pi|_V)^{-1} = \phi \circ \mathrm{id}_U = \phi|_U.$$
Pokažimo torej, da je $\phi \circ \pi$ holomorfna na okolici poljubne točke $z_0 \in \mathbb{C}$. Ločimo tri možnosti.

(i) Če je $z_0 \in \Lambda$, bo $\phi(\pi(z_0)) = [0 : 1 : 0]$. Naj bo $\psi$ lokalna karta na $E(\mathbb{C})$ pri točki $[0 : 1 : 0]$. Tedaj vemo, da je ta podana s predpisom $\psi([x : 1 : z]) = x$, torej na dovolj majhni okolici točke $z_0$ velja
$$\psi(\phi(\pi(z))) = \psi([\wp(z) : \wp'(z) : 1]) = \psi\left(\left[\frac{\wp(z)}{\wp'(z)} : 1 : \frac{1}{\wp'(z)}\right]\right) = \frac{\wp(z)}{\wp'(z)}.$$
To je predpis holomorfne funkcije, saj ima funkcija $\frac{\wp}{\wp'}$ odpravljivo singularnost pri $z_0 \in \Lambda$.

(ii) Če je $z_0 \in \frac{1}{2}\Lambda \setminus \Lambda$, je $\phi(\pi(z_0)) = [\wp(z_0) : 0 : 1]$. Na odprti okolici te točke imamo lokalno karto $\psi$, s predpisom $\psi([x : y : 1]) = y$. Na dovolj majhni odprti okolici točke $z_0$ bo torej veljalo
$$\psi(\phi(\pi(z))) = \psi([\wp(z) : \wp'(z) : 1]) = \wp'(z),$$
ki je očitno predpis holomorfne funkcije na tej odprti okolici.

(iii) Če je $z_0 \in \mathbb{C} \setminus \frac{1}{2}\Lambda$, pa imamo na okolici točke $\phi(\pi(z_0))$ lokalno karto $\psi$, ki je oblike $\psi([x : y : 1]) = x$ in na dovolj majhni odprti okolici $z_0$ velja
$$\psi(\phi(\pi(z))) = \psi([\wp(z) : \wp'(z) : 1]) = \wp(z),$$
ki je jasno tudi holomorfna.

Skupaj vidimo, da je $\phi$ holomorfna bijekcija, od koder po trditvi 4.9 sledi, da je $\phi : \mathbb{C}/\Lambda \to E(\mathbb{C})$ biholomorfizem. □

**Izrek 5.17.** *$j$-invarianta $j : \mathfrak{H} \to \mathbb{C}$ inducira bijektivno preslikavo $\mathfrak{H}/\Gamma \to \mathbb{C}$.*

*Dokaz.* Vemo že, da je $j$-invarianta modularna funkcija reda 0, torej je invariantna na delovanje $\Gamma$ in tako inducira dobro definirano funkcijo na prostoru orbit $\mathfrak{H}/\Gamma$.

Nadalje, če za $\tau_1, \tau_2 \in \mathfrak{H}$ velja $j(\tau_1) = j(\tau_2)$, imata mreži $\langle 1, \tau_1 \rangle$ in $\langle 1, \tau_2 \rangle$ isti $j$-invarianti, od koder po trditvi 6.1 iz dodatka sledi, da sta homotetični. Za homotetični mreži takšne oblike pa nam trditev 5.8 zagotavlja obstoj elementa $\gamma \in \Gamma$, da velja $\tau_1 = \gamma\tau_2$. To pomeni, da sta $\tau_1$ in $\tau_2$ del iste orbite in zato $j$ inducira injektivno preslikavo na kvocientu $\mathfrak{H}/\Gamma$.

Oglejmo si še, zakaj je $j$ surjektivna. Od tod bo namreč sledila surjektivnost in posledično bijektivnost inducirane preslikave na prostoru orbit. Ker je $j$ nekonstantna holomorfna funkcija, je $j(\mathfrak{H})$ odprta množica v $\mathbb{C}$. Kompleksna ravnina $\mathbb{C}$ je povezana, zato bo zadoščalo preveriti, da je $j(\mathfrak{H})$ tudi zaprta v $\mathbb{C}$, od koder bo sledilo $j(\mathfrak{H}) = \mathbb{C}$ in pokazalo surjektivnost $j$.

Vemo, da je podmnožica v $\mathbb{C}$ zaprta natanko tedaj, ko vsebuje vsa svoja stekališča. Naj bo $j_0 \in \mathbb{C}$ poljubno stekališče slike $j(\mathfrak{H})$. Tedaj obstaja zaporedje $(z_n)_{n\in\mathbb{N}}$ v $\mathfrak{H}$, katerega slike z $j$ konvergirajo k $j_0$ tj.

$$j(z_n) \xrightarrow{n\to\infty} j_0. \tag{5.8}$$

Po izreku 5.7 ima vsak od členov zaporedja $z_n$ predstavnika v fundamentalni domeni delovanja

$$D = \{z \in \mathfrak{H} \mid |z| \geq 1 \text{ in } -1/2 \leq \mathrm{Re}(z) \leq 1/2\}.$$

Zaradi invariance $j$ na delovanje $\Gamma$, lahko po potrebi zato vsakega od členov $z_n$ zamenjamo s takšnim, ki leži v $D$, in konvergenca (5.8) še vedno velja. Ravno zaradi tega, lahko predpostavimo, da so realni deli zaporedja $(z_n)_{n\in\mathbb{N}}$ omejeni. Sedaj ločimo dve možnosti.

Če je zaporedje imaginarnih delov $(\mathrm{Im}(z_n))_{n\in\mathbb{N}}$ omejeno, je zaporedje $(z_n)_{n\in\mathbb{N}}$ omejeno in ima zato stekališče $z \in \mathfrak{H}$. Izberemo si lahko podzaporedje $(z_{n_k})_{k\in\mathbb{N}}$, ki konvergira k $z$, od koder zaradi zveznosti $j$, velja

$$j_0 = \lim_{k\to\infty} j(z_{n_k}) = j(z) \in j(\mathfrak{H}).$$

Če pa je zaporedje $(\mathrm{Im}(z_n))_{n\in\mathbb{N}}$ neomejeno, ima to zaporedje konvergentno podzaporedje $(z_{n_k})_{k\in\mathbb{N}}$, ki konvergira proti $\infty$. Brez škode za splošnost lahko predpostavimo, da je $(z_n)_{n\in\mathbb{N}}$ že takšno zaporedje. Iz obravnave modularne $j$-invariante v prejšnjem razdelku vemo, da bo tedaj $\lim_{n\to\infty} j(z_n) = \infty \neq j_0$, kar je v nasprotju z (5.8) in zaključi dokaz. □

Izrek 5.16 je pokazal, kako lahko vsak kompleksni torus realiziramo kot eliptično krivuljo. Vsako eliptično krivuljo namreč podaja par koeficientov $(a, b)$, ki nastopata v enačbi $y^2z = 4x^3 - axz^2 - bz^3$ in za katera velja $a^3 - 27b^2 \neq 0$. Kompleksnemu torusu $\mathbb{C}/\Lambda$ smo tako priredili eliptično krivuljo s parom koeficientov $(g_2(\Lambda), g_3(\Lambda))$ in pokazali, da je temu torusu res tudi izomorfna. Uniformizacijski izrek pa s pomočjo modularne $j$-invariante razkrije še obrat – da poljuben takšnen par koeficientov $(a, b)$ vedno izhaja iz nekega kompleksnega torusa oz. pripadajoče mreže na zgoraj opisan način.

**Izrek 5.18** (Uniformizacija)**.** *Za vsako kompleksno eliptično krivuljo $E(\mathbb{C})$, podano z enačbo*

$$E: \quad y^2z = 4x^3 - axz^2 - bz^3, \quad \textit{kjer je} \quad a^3 - 27b^2 \neq 0,$$

*obstaja mreža $\Lambda \subseteq \mathbb{C}$, da je $a = g_2(\Lambda)$ in $b = g_3(\Lambda)$. Posledično sta kompleksni torus $\mathbb{C}/\Lambda$ in eliptična krivulja $E(\mathbb{C})$ izomorfna v smislu Riemannovih ploskev, preko izomorfizma podanega v izreku 5.16.*

*Dokaz.* Naj bo $j_E = 1728\frac{a^3}{a^3-27b^2}$ $j$-invarianta eliptične krivulje $E$. Tedaj po izreku 5.17 obstaja tak $\tau \in \mathfrak{H}$, da je $j(\tau) = j_E$. Mreža $\Lambda_0 = \langle 1, \tau \rangle$ ima tedaj $j$-invarianto enako

$$j(\Lambda_0) = 1728\frac{g_2(\Lambda_0)^3}{g_2(\Lambda_0)^3 - 27g_3(\Lambda_0)^2} = 1728\frac{a^3}{a^3 - 27b^2} = j_E.$$

Eliptična krivulja $E_0$, ki izhaja iz mreže $\Lambda_0$, podana z enačbo

$$E_0 : \quad y^2 z = 4x^3 - g_2(\Lambda_0)xz^2 - g_3(\Lambda_0)z^3,$$

ima $j$-invarianto enako ravno $j(\Lambda_0)$, zato je po trditvi 2.24 projektivno ekvivalentna krivulji $E(\mathbb{C})$. Lema 2.23 nam tedaj pove, da obstaja tak $\alpha \in \mathbb{C}^*$, da velja $a = \alpha^{-2}g_2(\Lambda_0)$ in $b = \alpha^{-3}g_3(\Lambda_0)$. Če upoštevamo še enakost (5.5), zadošča vzeti $\Lambda = \alpha\Lambda_0$, od koder dobimo želeno zvezo

$$a = g_2(\Lambda) \quad \text{in} \quad b = g_3(\Lambda).$$

Izrek 5.16 nazadnje zagotovi še izomorfizem Riemannovih ploskev $\mathbb{C}/\Lambda \to E(\mathbb{C})$. □

**Posledica 5.19.** *Eliptični krivulji sta projektivno ekvivalentni natanko tedaj, ko sta izomorfni kot Riemannovi ploskvi.*

*Dokaz.* Naj bosta $E_1$ in $E_2$ eliptični kriulji s pripadajočima kompleksnima strukturama. Če sta projektivno ekvivalentni, nam trditev 4.13 pove, da je projektivnost med njima holomorfna preslikava s holomorfnim inverzom, torej je biholomorfizem med $E_1$ in $E_2$.

Obratno, denimo, da sta $E_1$ in $E_2$ izomorfni kot Riemannovi ploskvi. Tedaj po uniformizacijskem izreku 5.18 dobimo mreži $\Lambda_1$ in $\Lambda_2$, da sta $\mathbb{C}/\Lambda_1 \cong E_1$ in $\mathbb{C}/\Lambda_2 \cong E_2$ biholomorfizma. Posledično dobimo biholomorfizem kompleksnih torusov $\mathbb{C}/\Lambda_1 \cong \mathbb{C}/\Lambda_2$. Po trditvi 4.21 v posebnem obstaja $\alpha \in \mathbb{C}^*$, za katerega je $\alpha\Lambda_1 = \Lambda_2$, od tod pa sledi, da sta $j$-invarianti mrež $\Lambda_1$ in $\Lambda_2$ enaki. Ker velja $j(\Lambda_1) = j_{E_1}$ in $j(\Lambda_2) = j_{E_2}$, sta $j$-invarianti eliptičnih krivulj $E_1$ in $E_2$ enaki, torej sta ti dve projektivno ekvivalentni po trditvi 2.24. □

## 6. Dodatek

V dokazu izreka 5.17 omenjamo $j$-invarianto mreže $\Lambda$, ki jo definiramo kot $j$-invarianto eliptične krivulje, podane z enačbo

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

torej s formulo

$$j(\Lambda) = 1728\frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2}.$$

**Trditev 6.1.** *Dve mreži sta homotetični natanko tedaj, ko sta njuni $j$-invarianti enaki.*

*Dokaz.* Ker že vemo, da imata homotetični mreži enako $j$-invarianto, se posvetimo še obratu. Denimo, da imata mreži $\Lambda_1$ in $\Lambda_2$ enaki $j$-invarianti, tj.

$$j(\Lambda_1) = 1728\frac{g_2(\Lambda_1)^3}{g_2(\Lambda_1)^3 - 27g_3(\Lambda_1)^2} = 1728\frac{g_2(\Lambda_2)^3}{g_2(\Lambda_2)^3 - 27g_3(\Lambda_2)^2} = j(\Lambda_2).$$

Para $(g_2(\Lambda_1), g_3(\Lambda_1))$ in $(g_2(\Lambda_2), g_3(\Lambda_2))$ si lahko tedaj predstavljamo kot koeficiente dveh projektivno ekvivalentnih eliptičnih kirvulj, torej bo po lemi 2.23 obstajal tak $\alpha \in \mathbb{C}^*$, da je

$$g_2(\Lambda_2) = \alpha^{-4}g_2(\Lambda_1) = g_2(\alpha\Lambda_1) \quad \text{in} \quad g_3(\Lambda_2) = \alpha^{-6}g_3(\Lambda_1) = g_3(\alpha\Lambda_1).$$

Radi bi sklepali, da tedaj velja $\Lambda_2 = \alpha\Lambda_1$.

Za poljubno mrežo $\Lambda$ se spomnimo zveze (3.2)

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

Z odvajanjem dobimo

$$2\wp'(z)\wp''(z) = 12\wp(z)^2\wp'(z) - g_2(\Lambda)\wp'(z)$$

$$\wp''(z) = 6\wp(z)^2 - \frac{g_2(\Lambda)}{2}. \tag{6.1}$$

Lauretov razvoj $\wp$ okoli izhodišča (3.1) je

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}(\Lambda)z^{2k} = \frac{1}{z^2} + \sum_{k=1}^{\infty} a_k z^{2k}.$$

S primerjavo koeficientov, podobno kot v dokazu izreka 3.24, iz zveze (6.1), za $k \geq 2$, pred potenco $z^{2k}$ dobimo

$$(2k+2)(2k+1)a_{k+1} = 6\left(2a_{k+1} + \sum_{j=1}^{k-1} a_j a_{k-j}\right).$$

Od tod za vse $k \geq 2$ izpeljemo rekurzivno zvezo za koeficient $a_{k+1}$

$$a_{k+1} = \frac{6}{(2k+2)(2k+1) - 12}\sum_{j=1}^{k-1} a_j a_{k-j},$$

ki je popolnoma določena s poznanima začetnima členoma $a_1 = g_2(\Lambda)/20$ in $a_2 = g_3(\Lambda)/28$, ki ju preberemo iz Laurentovega razvoja (3.1) funkcije $\wp$. Koeficienti Laurentovega razvoja $\wp$ okoli izhodišča so torej popolnoma določeni že z vrednostima $g_2(\Lambda)$ in $g_3(\Lambda)$, zato velja $\wp_{\Lambda_2}(z) = \wp_{\alpha\Lambda_1}(z)$ za vse $z \in \mathbb{C}$. V posebnem to pomeni, da se $\wp_{\Lambda_2}$ in $\wp_{\alpha\Lambda_1}$ ujemata tudi v množici njunih polov, od koder sledi željeni rezultat $\Lambda_2 = \alpha\Lambda_1$, ki pove, da sta mreži $\Lambda_1$ in $\Lambda_2$ homotetični. □

## Slovar strokovnih izrazov

**algebraic curve** algebraična krivulja
**complex structure** kompleksna struktura
**complex torus** kompleksni torus
**Eisenstein series** Eisensteinova vrsta
**elliptic curve** eliptična krivulja
**elliptic function** eliptična funkcija
**fundamental domain** fundamentalna domena
**holomorphic map** holomorfna preslikava
**$j$-invariant** $j$-invarianta
**lattice** mreža
**modular function** modularna funkcija
**modular discriminant** modularna diskriminanta
**Riemann surface** Riemannova ploskev
**uniformization** uniformizacija
**Weierstrass $\wp$-function** Weierstrassova funkcija $\wp$

# Literatura


[1] L. V. Ahlfors, *Complex analysis*, third edition, McGraw-Hill, Inc., New York, 1979.

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

[3] A. Chéritat, *Galerie III: Geometry*, [ogled 6. 6. 2022], dostopnno na `www.math.univ-toulouse.fr/~cheritat/GalIII/galery.html`

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

[5] J. Globevnik in M. Brojan, *Analiza II*, verzija 10. 8. 2010, [ogled 28. 7. 2021], dostopno na `www.fmf.uni-lj.si/~globevnik/skriptaII.pdf`.

[6] S. Lang, *Elliptic functions*, Graduate Texts in Mathematics **112**, Springer-Verlag, New York, 1973.

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

[8] J. P. Serre, *A course in arithmetic*, Graduate Texts in Mathematics **7**, Springer-Verlag, New York, 1973.

[9] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, New York, 1986.

[10] P. Stevenhagen, *Complex elliptic curves*, verzija 1. 10. 2013, [ogled 9. 2. 2021], dostopno na `www.julianlyczak.nl/teaching/EC2015-files/ec.pdf`.