UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO

Matematika – 1. stopnja

Izak Jenko

Kompleksni torusi in eliptične krivulje

Delo diplomskega seminarja

Mentor: izr. prof. dr. Sašo Strle

Ljubljana, 2021

Kazalo

Kompleksni torusi in eliptične krivulje

Povzetek

Complex tori and elliptic curves

Abstract

Math. Subj. Class. (2020):
Ključne besede:
Keywords:

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 kriprografiji, nad racionalnimi števili 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 omogoča analizo holomorfnih funkcij na prostorih, ki niso nujno domene v kompleksni ravnini in jo bomo bolj podrobno preiskali v poglavju 4. V nadaljevanju bomo videli, da tudi torus premore strukturo Riemannove ploskve in ga bomo skupaj s to strukturo imenovali kompleksni torus. Izkaže se, da je kompleksni torus najbolj smiselna domena dvojno periodičnih oz. eliptičnih funkcij. Lastnosti in obnašanje eliptičnih funkcij si bomo ogledali v poglavju 3, klučno vlogo pa bo igrala prav posebna Weierstrassova eliptična funkcija $\wp$. Ta 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.

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 oz. eliptični, če jih gledamo kot funkcije kompleksne spremenljivke. Te dvojno periodične funkcije pa so tesno povezane z enačbo, ki ji zadoščajo eliptične krivulje in se bomo k njim vrnili v poglavju 3.

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 polinom $f \in \mathbb{C}[x, y]$ stopnje vsaj 1, 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

$$f_x(x_0, y_0) = 0, \quad f_y(x_0, y_0) = 0, \quad f(x_0, y_0) = 0.$$

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 αf za $\alpha \in \mathbb{C}^\times$, 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 $f(x, y) = x^2 + y^2 - 1$ in $g(x, y) = (x^2 + y^2 - 1)^2$. Jasno je $V(f) = V(g)$, kar pomeni, da f in g določata isto algebraično krivuljo – kompleksno enotsko sfero $S(\mathbb{C}^2)$. Toda sistem

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

nima nobene rešitve, sistem

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

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 $S(\mathbb{C}^2)$ 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) $X \cap U = F^{-1}(\{0\}) = \{x \in U | F(x) = 0\}$ 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

$$Jg = \begin{pmatrix} u_{x_1} & u_{x_2} & u_{y_1} & u_{y_2} \\ v_{x_1} & v_{x_2} & v_{y_1} & v_{y_2} \end{pmatrix} = \begin{pmatrix} \underbrace{u_{x_1}}_{\frac{\partial f}{\partial x}} & -v_{x_1} & \underbrace{u_{y_1}}_{\frac{\partial f}{\partial y}} & -v_{y_1} \\ \underbrace{v_{x_1}}_{\frac{\partial f}{\partial x}} & u_{x_1} & \underbrace{v_{y_1}}_{\frac{\partial f}{\partial y}} & u_{y_1} \end{pmatrix},$$

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

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

(analogno dobimo za odvod po y) in predpostavka o nesingularnosti krivulje nam zagotovita, da je v vsaki točki na C vsaj eden od parcialnih odvodov u_{x_1}, v_{x_1}, u_{x_2}, v_{x_2} različen od 0. To pa že zadošča za polnost ranga Jacobijeve matrike Jg v dani točki, saj sta leva in desna 2×2 bloka alternativna predstavitev kompleksnih števil kot matrična algebra znotraj realnih 2×2 matrik $M_2(\mathbb{R})$. □

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 na 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

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

Tukaj $\mathbb{C}^\times$ označuje multiplikativno grupo kompleksnih števil oz. $\mathbb{C} \setminus \{0\}$. Pri tem bomo $P^2(\mathbb{C})$ – 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* $\widehat{\mathbb{C}} = P^1(\mathbb{C})$. Včasih jo bomo poimenovali tudi (kompleksna) projektivna premica. Riemannova sfera ima sicer še nekoliko več strukture, ki smo jo zaenkrat pri projektivnih prostorih izpustili, a se bomo k temu vrnili v poglavju o Riemannovih ploskvah 4.

Projektivni prostor si lahko predstavljmo 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 $[x]_\sim = \{(\lambda x_0, \ldots, \lambda x_n) \in \mathbb{C}^{n+1} \mid \lambda \in \mathbb{C}^\times\} \in P^n(\mathbb{C})$ 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 $\lambda \in \mathbb{C}^\times$.

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

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

In sicer vzamemo za odprte množice v $P^n(\mathbb{C})$ *natanko* tiste $U \subseteq P^n(\mathbb{C})$ za katere je $\pi^{-1}(U)$ odprta v $\mathbb{C}^{n+1} \setminus \{0\}$. Hkrati je to tudi največja topologija na $P^n(\mathbb{C})$, za katero je projekcija π še vedno zvezna. Tej topologiji pravimo *kvocientna topologija* in o njej si lahko bralec več pogleda v [5, 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

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

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 $P^n(\mathbb{C})$ kompakten 2-števen in Hausdorffov. Podrobnosti o tem lahko bralec najde v [5, Zgled 3.43. (2)].

Za definicijo projektivnih algebraičnih krivulj potrebujemo polinome, ki so usklajeni s homogenostjo koordinat na $P^2(\mathbb{C})$. 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 $\lambda \in \mathbb{C}^\times$ 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 koorinat 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 $C \subseteq P^2(\mathbb{C})$ je *projektivna algebraična krivulja*, če obstaja tak nekonstanten homogen polinom $F \in \mathbb{C}[x, y, z]$, da je

$$C = V(F).$$

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 $C = V(F) \subseteq P^2(\mathbb{C})$ 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 nasledja trditev imenovana *Eulerjeva identiteta.*

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

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

Dokaz. Ker je polinom F homogen, velja

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

Če to enakost odvajamo po λ, dobimo

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

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

Sedaj bi radi razvili način, kako malce bolj "generalno" 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 pomagale pri tem.

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

$$\Phi : P^2(\mathbb{C}) \to P^2(\mathbb{C})$$

$$[x:y:z] \mapsto [a_{11}x + a_{12}y + a_{13}z : a_{21}x + a_{22}y + a_{23}z : a_{31}x + a_{32}y + a_{33}z]\,.$$

Projektivnosti Φ je pravzaprav določena z linearno preslikavo $\mathcal{A}_\Phi : \mathbb{C}^3 \to \mathbb{C}^3$, ki predstavlja množenje z matirko 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 $\pi : \mathbb{C}^3 \setminus \{0\} \to P^2(\mathbb{C})$, 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 jo označujemo s $\mathrm{PGL}(3,\mathbb{C}) = \mathrm{GL}(3,\mathbb{C})/\mathbb{C}^\times$, posebej je $\mathrm{Aut}(\widehat{\mathbb{C}}) \cong \mathrm{PGL}(2,\mathbb{C})$. Več o tem lahko bralec najde v [2, poglavje 11]. //mogoče bi bilo fino tudi to dokazati kot trditev.

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

Primer 2.16. //demonstriram projektivno ekvivalenco

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

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

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

Denimo, da velja $C \cong C'$, torej je $G = \lambda(F \circ \mathcal{A}_\Phi)$ za neko projektivnost $\Phi \in \mathrm{PGL}(3, \mathbb{C})$ in $\lambda \in \mathbb{C}^\times$. 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 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 $C, C' \subseteq P^2(\mathbb{C})$ 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 Φ in $\lambda \in \mathbb{C}^\times$, da je

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

Če je C nesingularna, je $(F_x, F_y, F_z) \neq 0$ povsod na $\mathbb{C}^3 \backslash \{0\}$, torej z odvajanjem zveze 2.3 v točki (x, y, z) in upoštevanjem Leibnitzovega pravila za odvajanje produkta dobimo

$$(G_x, G_y, G_z)_{(x,y,z)} = \lambda(F_x, F_y, F_z)_{\mathcal{A}_\Phi(x,y,z)} \cdot A,$$

produkt vrstice in matrike A, ki je konstantna Jacobijeva matrika linearne preslikave $\mathcal{A}_\Phi$. Vrstica $(F_x, F_y, F_z)_{\mathcal{A}_\Phi(x,y,z)}$ je po predpostavki neničelna, matrika A pa obrnljiva, zato je njun produkt spet neničelna vrstica, torej je $(G_x, G_y, G_z)_{(x,y,z)} \neq 0$. □

Z drugimi besedami ta trditev pove, da projektivna ekvivalenca ohranja singularnost oziroma 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 bralec več izve v [2].

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

Definicija 2.19. *Projektivna kubika* je projektivna algebraična krivulja v $P^2(\mathbb{C})$, 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 [2, 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 $C \subseteq P^2(\mathbb{C})$ 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 imenujmo Weierstrassova kubika.

Opomba 2.21. Vrednost $-4\alpha^3 - 27\beta^2$ je med drugim diskriminanta kubičnega polinoma $f(x) = x^3 + \alpha x + \beta$, ki nam pove kako je z večkratnostjo ničel polinoma f. Njena vrednost je enaka 0 natanko tedaj, ko f premore kakšno večkratno ničlo.

To ime privzamemo 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 $F(x, y, z) = y^2z - x^3 - \alpha xz^2 - \beta z^3$. 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

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

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. *Vsaka nesingularna projektivna kubika je projektivno ekvivalentna neki nesingularni Weierstrassovi kubiki.*

Dokaz. [2, lemma 15.2] □

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

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

projektivno ekvivalentni, če velja, denimo $u^4\alpha' = \alpha$ in $u^6\beta' = \beta$ za nek $u \in \mathbb{C}^\times$. Namreč takrat imamo projektivnost

$$\begin{aligned} \Phi : C &\to C' \\ [x:y:z] &\mapsto \left[u^{-2}x : u^{-3}y : z\right], \end{aligned}$$

krajše zapisano

$$x = u^2x' \quad y = u^3y' \quad z = z',$$

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 bo Φ projektivnost med dvema projektivno ekvivalentnima Weierstrassovima kubikama, C, C' kot zgoraj. Tedaj Φ fiksira točko $[0:1:0]$ in je oblike*

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

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

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

Dokaz. Naj bosta $F(x,y,z) = y^2z - x^3 - \alpha xz^2 - \beta z^3$ in $G(x,y,z) = y^2z - x^3 - \alpha' xz^2 - \beta' z^3$ 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 Φ 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 $a_{12} \neq 0$, potem 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 pravtako 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 protislovju 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 z $G(x', y', z')$. 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 škode za splošnost privzamemo $a_{33} = 1$. Če vzamemo $u \in \mathbb{C}^\times$ poljuben, da velja $u^6 = \lambda^{-1}$, bo

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

in tako vidimo, da je projektivnost Φ oblike

$$x = u^2x' \quad y = u^3y' \quad z = z'.$$

□

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

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

Poznaje bomo videli, kako lahko j-invarianto gledamo tudi kot funkcijo kompleksne spremenljivke in tako malce pokomentirali "zanimivost" izbire 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

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

enaki j-invarianti, torej, da velja

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

Kar nam da

$$\alpha^3\beta'^2 = \alpha'^3\beta^2. \tag{2.6}$$

Sedaj iščemo projektivnost oblike $x = u^2x'$, $y = u^3y'$, $z = z'$ za nek $u \in \mathbb{C}^\times$. Ločimo tri primere.

(i) $\alpha = 0$. Tedaj mora biti $\beta \neq 0$, saj bi sicer C bila singularna po 2.20. Od tod iz (2.6) sledi, da je $\alpha' = 0$ in zato je tudi $\beta' \neq 0$, sicer bi bila C' singularna. Zadošča vzeti $u \in \mathbb{C}^\times$ 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 $u \in \mathbb{C}^\times$ 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 α', β' bil ničeln, bi zaradi veze 2.6 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 $u \in \mathbb{C}^\times$ 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 α, 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 [6, III. §3.] in naših potreb v nadaljevanju, eliptične kriulje vpeljemo nekoliko enostavnje. Presenetljivo pa je (vsaj nad $\mathbb{C}$) 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

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

kjer $4\alpha^3 + 27\beta^2 \neq 0$.

(2) Zaradi kompletnosti smo v definicijo eliptične krivulje vključili še izbiro izhodišča, ki igra vlogo identitete, 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

$$x = tx', \quad y = y', \quad z = z', \quad \text{kjer za } t \in \mathbb{C}^\times \text{ velja } t^3 = 4.$$

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

$$\Delta = 16(a^3 - 27b^2) \quad \text{in} \quad j = 1728\frac{a^3}{a^3 - 27b^2}. \tag{2.7}$$

3. Eliptične funkcije

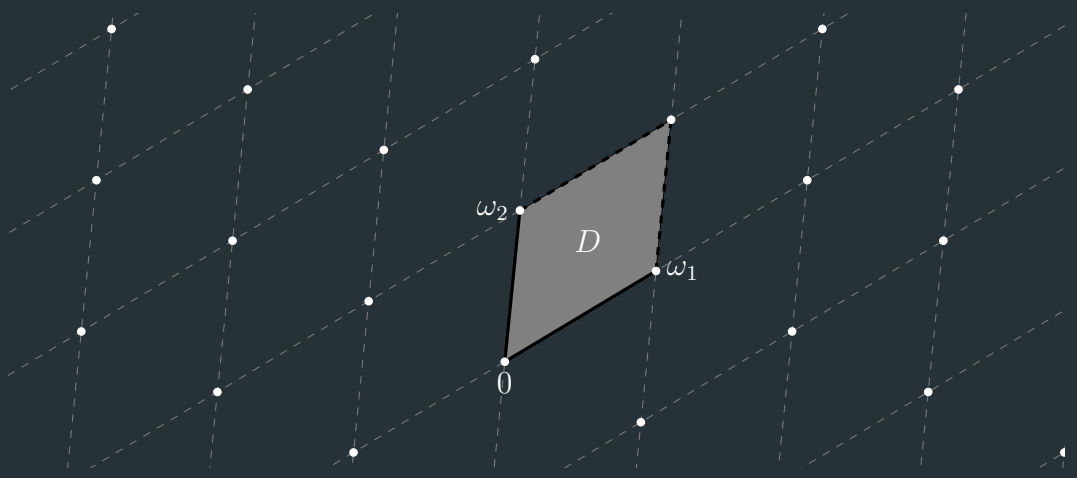
Glavna vez med eliptičnimi krivuljami in kompleksnimi torusi so t. i. *eliptične funkcije*. Da jih vpeljemo, najprej potrebujemo nekaj novih pojmov.

Definicija 3.1. Aditivna podgrupa kompleksnih števil $\mathbb{C}$ izomorfna direktni vsoti $\mathbb{Z} \oplus \mathbb{Z}$ se imenuje *mreža*.

Ekvivalentno je mreža prosta Abelova grupa na dveh generatorjih $\omega_1, \omega_2 \in \mathbb{C}^\times$, 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

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

kot kaže slika 1.



Slika 1. Mreža Λ in fundamentalni paralelogram D.

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

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

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

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_α v $\mathbb{C}$ bomo označili z $\overline{D}_\alpha$.

Opomba 3.3. Kadar bomo govorili o fundamentalnih domenah pogosto izbira izhodišča α ne bo pomembna, zato ga bomo tedaj izpustili in pisali samo D. V tem primeru lahko privzamemo, da je s tem mišljen D_0.

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

Lema 3.4. *Poljuben translat $z + \Lambda$ mreže $\Lambda \subseteq \mathbb{C}$ ima natanko enega predstavnika v fundamentalni domeni D_α.*

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

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

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

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

Če je $S \subseteq D$ diskretna množica brez stekališč v D, potem funkcijam, ki so holomorfne na $D \setminus S$, v točkah iz S pa imajo pole, pravimo *meromorfne* funkcije, točkam iz S pa *singularnosti*. Vsako meromorfno funkcijo f na $D \subseteq \mathbb{C}$, lahko vidimo tudi kot preslikavo $D \to \widehat{\mathbb{C}}$, 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 Λ, pravimo, da je Λ-*periodična*. Polje Λ-periodičnih funkcij označimo z $\mathbb{C}(\Lambda)$.

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. Bralec ga lahko najde v [,].

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 [5, Trditev 2.22]. Zvezna funkcija f je na kompaktu $\overline{D}$ omejena, kot eliptična funkcija pa je tako omejena na celotnem $\mathbb{C}$ [5, 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 $D \subseteq \mathbb{C}$, pravimo, da je f *reda* $m \in \mathbb{Z}$ v točki $z_0 \in D$, če obstaja okolica $U \subseteq D$ točke z_0 in holomorfna funkcija $g \in \mathcal{O}(U)$, ki je neničelna povsod na U, da velja

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

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

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

Izrek 3.9. *Naj bo $f \in \mathbb{C}(\Lambda)$ eliptična funkcija in D fundamentalni paralelogram glede na mrežo Λ, katerega rob ∂D ne vsebuje polov ali ničel f. Tedaj velja*

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

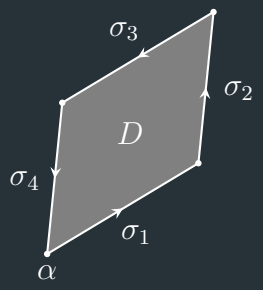
(ii) $\displaystyle\sum_{w \in D} \mathrm{ord}_w(f) = 0$

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

Dokaz. (i) Uporabimo izrek o ostankih [3, Izrek 71], ki pove

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

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

(ii) Po lemi 3.8 je $f' \in \mathbb{C}(\Lambda)$, zato je tudi kvocient $f'/f \in \mathbb{C}(\Lambda)$ 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 [3, 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 pravtako 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 (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 σ_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 σ_2 in tako dobimo

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

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

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

ovojno število krivulje γ okoli 0 in nam pove kolikokrat se krivulja γ ovije okoli izhodišča. Podrobnosti o tem lahko bralec najde v [1, 4.2.1.].

Osredotočimo se sedaj samo na prvi integral, premislek za drugega je analogen. Opazimo, da je zaradi eilptičnosti f krivulja $f(\sigma_4)$ sklenjena, saj sta krajišči daljice σ_4 točki α in $\alpha+\omega_2$ v katerih ima f enaki vrednosti. Pot $\gamma : [0,1] \to f(\sigma_4)$, ki predstavlja to sklenjeno krivuljo, je podana s predpisom $t \mapsto f(\alpha + t\omega_2)$. 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 nek $k_1 \in \mathbb{Z}$. Podobno je tako tudi

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

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

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

□

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 protislovje s principom identičnosti. Ta pravi, da se meromorfni funkciji definirani na neki odprti domeni Ω, ki se ujemata na množici s stekališčem v Ω, ujemata povsod na Ω [,].

(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 temu ni tako, torej da ima vsak fundamentalni paralelogram na svojem robu vsaj en pol eliptične funkcije f. S translacijami

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

delujemo na rob fundamentalnega paralelograma ∂D in tako dobimo števno mnogo različnih polov za f. To zaporedje polov leži v uniji $\cup_{n\in\mathbb{N}}\tau_n(\partial D)$, 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 protislovje z diskretnostjo množice ničel meromorfne funkcije f.

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

Definicija 3.11. *Red* eliptične funkcije je število polov šteto z večkratnostjo v poljubnem fundamentalnem paralelogramu.

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

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

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

Zgled 3.12.

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 α na fundamentalni domeni D, saj že vemo, da bi bila f konstantna, če bi bila brez polov, po izreku 3.6. Predpostavimo lahko tudi, da pol leži v notranjosti D. Tedaj dobimo z integracijo po robu ∂D neničelni residuum

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

To pa je v nasprotju z izrekom 3.9 (i), 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 ∞. 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 pravtako eliptična in ima pol, saj je takšna f in prištevanje konstante na ti dve lastnosti nima vpliva. Po opombi 3.10 (3) ima g ničlo v $\mathbb{C}$, kar pokaže želeno. □

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 preučevanje lastnosti t. i. *Weierstrassove funkcije $\wp$.*

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

Definicija 3.15. Za celo 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 ω in $-\omega \in \Lambda'$ v vsoti odštejeta.

Lema 3.17. *Za vsako celo število $k > 2$ je Eisensteinova vrsta reda k absolutno konvergentna.*

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

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

Preprosto se je prepričati, da je moč posamezne od teh množic $\#C_n = 4n$. Vsak element $\omega \in C_n$ pa lahko po absolutni vrednosti ocenimo $|\omega| > \rho n$, kjer je $\rho > 0$ razdalija 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 celo število $k > 2$, vrsta*

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

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

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

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

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

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

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

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

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

vidimo, da velja

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

Tako pridemo do ocene

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

ki velja povsod na K. Ker je zadnja vsota del (po lemi 3.17) absolutno konvergentne Eisensteinove vrste reda k, nam Weierstrassov M-test zagotovi želeni rezultat. □

Izrek 3.19. *Naj bo $(f_n)_{n \in \mathbb{N}}$ zaporedje holomorfnih funkcij na odprti domeni $\Omega \subseteq \mathbb{C}$, ki enakomerno po kompaktih v Ω konvergira k limitni funkciji f. Tedaj je tudi $f \in \mathcal{O}(\Omega)$ holomorfna na Ω in zaporedje odvodov $(f_n')_{n \in \mathbb{N}}$ konvergira enakomerno po kompaktih k odvodu limitne funkcije f'.*

Dokaz. [1, §5, Theorem 1] □

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 po lemi 3.18 si lahko predstavljamo, da jo seštevamo postopoma po diskih $\Delta(0, n)$ za $n \in \mathbb{N}$ in tako dobimo zaporedje delnih vsot, ki so holomorfne na $\mathbb{C} \setminus \Lambda$ in konvergirajo k f. Po izreku 3.19 je f holomorfna na $\mathbb{C} \setminus \Lambda$ v vsakem $\omega_0 \in \Lambda$ pa ima pol reda k in residuujem 0. O tem se prepričamo, saj lahko zapišemo

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

na neki dovolj majhni prebodeni okolici točke $\omega_0 \in \mathbb{C}$. Glavnemu delu okrog ω_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, računamo

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

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

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 bi lahko rekli, 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 Λ je

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

Trditev 3.22. *Za Weierstrassovo funkcijo* $\wp$ *glede na mrežo* Λ *veljajo naslednje točke.*

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

Dokaz. (i) Podobno kot v dokazu leme 3.18 bomo obravnavo razdelili na periode $\omega \in \Lambda$, ki ležijo znotraj diska $\Delta(0, 2r)$, ki omejuje nek izbrani kompakt $K \subseteq \mathbb{C} \setminus \Lambda$, in 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 $z \in K$, pa najprej ocenimo

$$|z-\omega| \geq |\omega| - |z| \geq \frac{1}{2}|\omega|$$

nato pa še

$$|2\omega - z| \leq |2\omega| - |z| \leq \frac{5}{2}|\omega|.$$

Tako velja

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| = \left| \frac{\omega^2 - (z-\omega)^2}{\omega^2(z-\omega)^2} \right| = \left| \frac{z(2\omega - z)}{\omega^2(z-\omega)^2} \right| \leq \frac{r \cdot \frac{5}{2}|\omega|}{|\omega|^2 \left(\frac{1}{2}|\omega|\right)^2} = \frac{10r}{|\omega|^3},$$

kar pomeni, da lahko del vsote, ki teče po $\omega \in \Lambda', |\omega| \geq 2r$, navzgor omejimo s konstanto $10r$ 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 funckije $\wp$ enak

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

(ii) Preprost račun pokaže

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

kjer smo za predzadnji enačaj upoštevali, da zrcaljenje $\omega \mapsto -\omega$ 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 Λ-periodičnosti funkcije $\wp$ po točki (iii), je dovolj situacijo obravnavati samo okoli točke $0 \in \Lambda$. Podobno kot smo sklepali o polih funkcije iz primera 3.20, tudi tukaj vidimo, da na neki prebodeni okolici točke 0 glavnemu delu Laurentove vrste za $\wp$ okoli 0 prispeva samo člen z^{-2}, ki nam da pol reda 2 z ostankom 0, preostanek vrste pa po dokazu točke (i) na tej prebodeni okolici definira holomorfno funkcijo, ki na glavni del nima vpliva. □

Naše zanimanje za Weierstrassovo eliptično funkcijo se skriva v dejstvu, da ta funkcija zadošča posebni diferencialni enačbi oblike $\wp'(z)^2 = p(\wp(z))$, kjer je $p \in \mathbb{C}[x]$ 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 Λ. Njen Laurentov razvoj okoli točke 0 je*

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

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 drugem enačaju smo zamenjali vrstni red seštevanja, kar nam omogoča absolutna konvergenca obeh vrst, v zadnjem enačaju pa smo preindeksirali vsoto na sode $n \in \mathbb{N}$, saj so vse Eisensteinove vrste lihega reda enake 0. □

Izrek 3.24. *Naj bo Λ mreža. Tedaj za Weierstrassovo eliptično funkcijo $\wp$ glede na Λ velja*

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda), \tag{3.1}$$

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

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

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

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

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

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

$$f(z) = 0 \cdot \frac{1}{z^6} + 0 \cdot \frac{1}{z^2} + 0 + (216G_4(\Lambda)^2 - 84G_8(\Lambda))z^2 + \cdots . \tag{3.2}$$

Funkcija f tako nima glavnega dela pri 0 in je zato na okolici U holomorfna. Zaradi Λ-periodičnosti je holomorfna tudi na vsaki okolici poljubne periode $\omega \in \Lambda$ in je tako cela eliptična funcija, kot takšna pa je po izreku 3.6 konstantna. Preostane le še ugotoviti kateri konstanti je enaka. Iz razvoja 3.2 takoj sledi, da je ta konstanta 0, ko vanjo vstavimo točko 0, to pa tudi zaključi dokaz izreka. □

Izrek 3.24 nam namiguje, da lahko s poljubno mrežo Λ definiramo eliptično krivuljo

$$E_\Lambda : \quad y^2z = 4x^3 - g_2(\Lambda)xz^2 - g_3(\Lambda)z^3. \tag{3.3}$$

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 na levo.

Ker je $\wp$ soda po 3.22 (ii), vemo, da je njen odvod $\wp'$ liha funkcija. Tako lahko za $2z \in \Lambda$ in upoštevajem Λ-periodičnosti $\wp'$ zapišemo

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

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

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

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

in vse tri so po zgornjem ničle $\wp'$. Kot smo se prepričali v primeru 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 $f(x) = 4x^3 - g_2x - g_3$ enaka $16(g_2^3 - 27g_3^2)$ in, da nam ta pove kdaj ima polinom f kakšno večkratno ničlo. Pokazali bomo, da ima za poljubno mrežo Λ polinom $4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ same različne ničle, saj je natanko takrat njegov diskriminanta neničelna.

Naj bosta $\omega_1, \omega_2 \in \Lambda$ osnovni periodi in označimo tri polperiode kot

$$r_1 = \frac{\omega_1}{2}, \quad r_2 = \frac{\omega_2}{2}, \quad r_3 = \frac{\omega_1 + \omega_2}{2}.$$

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 3.1 iz izreka 3.24 vstavimo osnovne tri polperiode r_1, r_2, r_3.

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

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

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

Naj bo $h_i(z) = \wp(z) - \wp(r_i)$. Funkcija h_i je eliptična funkcija reda 2 s poli v mreži Λ. Očitno je r_i njena ničla, ki pa mora biti reda 2, saj je tudi ničla odvoda $h_i' = \wp'$ po lemi 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 $g_2(\Lambda)^3 - 27g_3(\Lambda)^2 \neq 0$. □

Poljubni mreži $\Lambda \subseteq \mathbb{C}$ lahko torej priredimo eliptično krivuljo podano z enačbo 3.3. 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 5.1.

4. Riemannove ploskve

uvodni opis...

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.*

Zgled 4.2. (i) Kompleksna ravnina $\mathbb{C}$ je Riemannova ploskev podana z eno samo lokalno karto $(\mathbb{C}, \mathrm{id}_{\mathbb{C}})$.

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

(iii) Riemannova sfera

Definicija 4.3. Naj bosta X in Y Riemannovi ploskvi. Pravimo, da je zvezna preslikava $f : X \to Y$ *holomorfna*, kadar za vsak $x \in X$ obstaja lokalna karta (U, φ) iz kompleksnega atlasa X, da je $x \in U$, in lokalna karta (V, ψ) 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 okolici točke $\varphi(x) \in \mathbb{C}$.

Trditev 4.4. *V posamezni točki $x \in X$, je definicija 4.3 (oziroma holomorfnost preslikave $\psi \circ f \circ \varphi^{-1}$) neodvisna od izbire lokalnih kart (U, φ) in (V, ψ).*

Dokaz. Naj bosta (U', φ') in (V', ψ') drugi lokalni karti, 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 4.5. kako je meromorfna funkcija v resnici holomorfna preslikava v Riemannovo ploskev (glede na to definicijo)

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

Trditev 4.6. *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 4.7. Takšni holomorfni preslikavi $f : X \to Y$, katere inverz je pravtako 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. Vzemimo iz kompleksnih atlasov za X oziroma Y lokalni karti (U, φ) ozioma (V, ψ). 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 [3, 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 z $\varphi \circ f^{-1} \circ \psi^{-1}$ na ustrezni domeni. Tako storimo za vsak $z_0 \in \varphi(U \cap f^{-1}(V))$, kar nam 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, kar zagotovi biholomorfnost preslikave f in zaključi dokaz. □

Izrek 4.8. *(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 α in $V \subseteq \mathbb{C}$ okolica točke β 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 ϕ nad eno izmed spremenljivk. Za nas pa bo pomembno, da ta funkcija ϕ ni le gladka, ampak tudi holomorfna, če je le f holomorfna.

Dokaz. Dokaz gladke verzije izreka bralec najde v [3, Izrek 14], preostane nam le še obravnava holomorfnosti implicitne funkcije ϕ.

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

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

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 ϕ, ki drži – ekvivalentno holomorfnosti funkcije ϕ na U. □

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 kako prirediti kompleksno strukturo poljubni nesingularni projektivni algebraični krivulji. 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 z $f(x,y) = y^2 - 4x^3 + ax + b$ 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 4.8 zagotavlja obstoj holomorfne preslikave

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

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

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

Ta je med drugim homeomorfizem na svojo sliko $U := (W \times \phi(W)) \cap E$, ki je zaradi holomorfnosti ϕ odprta v E. Preslikava ϕ 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 φ 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 ϕ nad spremenljivko y namesto x. Tako bi za predpis homeomorfizma φ uporabili projekcijo pr_2 namesto pr_1.

Vsak tak par (U, φ) 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[1] 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 njihova unija vsebuje vse točke iz E, preslikave φ_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, φ_i) in (U_j, φ_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 $\phi_j : W_j \to \mathbb{C}$ ob tem pa ločimo dva primera.

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

(1) 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.

(2) Okolici U_i, U_j nista grafa funkcij nad istima spremenljivkama in recimo, da je U_i graf funkcije ϕ_i nad spremenljivko x, množica U_j pa naj bo graf funkcije ϕ_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 ϕ_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 bo projektivna krivulja $\overline{E} \subseteq P^2(\mathbb{C})$ podana s homogenizacijo enačbe za E

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

oziroma s homogenim polinomom $F(x, y, z) = y^2 z - 4x^3 + axz^2 + bz^3$, 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 [5, poglavje 3.2.]. Bralec ga lahko po potrebi tudi preskoči, saj ga obravnavamo zgolj za kompletnost celotne izpeljave.

Naj bo

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

vložitev, $\pi : \mathbb{C}^3 \setminus \{0\} \to P^2(\mathbb{C})$ pa kvocientna projekcija iz opombe 2.9, kjer smo projektivne prostore opremili s topologijo. Najprej opazimo, da se projektivno zaprtje $\overline{E} \subseteq P^2(\mathbb{C})$ od afine krivulje E v bistvu razlikuje samo v eni točki. Natančneje vidimo, da je

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

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 $\pi(\iota(E))$.

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

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

in tako bo $\varphi_i' \circ \iota = \varphi_i$.

Preslikava $\pi : \iota(U_i) \to V_i \subseteq P^2(\mathbb{C})$ je injekcija, saj se nobeni dve različni točki iz $\iota(U_i)$ ne razlikujeta za skalarni večkratnik iz $\mathbb{C}^\times$ in zaradi tega tvori samo trivialne identifikacije. Kot homeomorfizem je tudi φ_i' injekcija, kar pomeni, da imata ti dve preslikavi enaka vlakna – same enoelementne množice. Od tod sklepamo, da je inducirana preslikava $\overline{\varphi}_i$ dobro definirana zvezna injekcija. Iz surjektivnosti φ_i'

sledi surjektivnost $\overline{\varphi}_i$, ker pa je φ_i' homeomorfizem (torej v posebnem kvocientana presliava), je inducirana preslikava $\overline{\varphi}_i : V_i \to W_i$ homeomorfizem, kot ponazarja komutativen diagram. Ta premislek utemeljuje [5, Posledica 3.23].

$$\begin{array}{ccc} \iota(U_i) & \xrightarrow{\varphi_i'} & W_i \\ {\scriptstyle\pi}\downarrow & \nearrow_{\overline{\varphi}_i} & \\ V_i & & \end{array} \tag{4.1}$$

Iz komutativnega diagrama lahko inverz induciranega homeomorfizma izrazimo kot $\overline{\varphi}_i^{-1} = \pi \circ \varphi_i'^{-1}$. To pa nam omogoči prepričati se o kompatibilanosti lokalnih kart $(V_i, \overline{\varphi}_i)$. Za poljubna $i, j \in I$ velja

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

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 karti $(V_i, \overline{\varphi}_i)$, $(V_j, \overline{\varphi}_j)$.

Skupek vseh na ta način konstruiranih parov $(V_i, \overline{\varphi}_i)$ bo prispeval kompleksnemu atlasu 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

$$F_z(x,1,z) = 1 + ax^2 + 3bz^2$$

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 $U_\infty = \{(x, 1, \phi_\infty(x)) \subseteq \mathbb{C}^3 \setminus \{(0,0,0)\} \mid x \in W_\infty\}$. 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 $V_\infty = \pi(U_\infty) \subseteq \overline{E} \subseteq P^2(\mathbb{C})$. Sedaj se pod istimi pogoji kot zgoraj inducira homeomorfizem $\overline{\varphi}_\infty : V_\infty \to W_\infty$, da komutira diagram.

$$\begin{array}{ccc} U_\infty & \xrightarrow{\varphi_\infty'} & W_\infty \\ {\scriptstyle\pi}\downarrow & \nearrow_{\overline{\varphi}_\infty} & \\ V_\infty & & \end{array} \tag{4.2}$$

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 potrebujemo 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 so v nasprotnem primeru kompatibilnostni pogoji že na prazno izpolnjeni.

Po eni strani, množica $V_\infty \cap V_i$ vsebuje vse točke oblike $[z : 1 : \phi_\infty(z)]$, za nek $z \in W_\infty$, po drugi strani pa ima ta točka zaradi vsebovanosti v V_i tudi obliko $[w : \phi_i(w) : 1]$ za nek $w \in W_i$. Eno projektivno točko smo tako zapisali s pomočjo dveh različnih predstavnikov, ki se razlikujeta za multiplikativno konstanto iz $\mathbb{C}^\times$. Tako iz primerjave tretjih komponent (do multiplikativne konstante iz $\mathbb{C}^\times$ 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 $w \neq 0$. Od tod je potem 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

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

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 ϕ_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

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

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

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

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 lokana karta $(V_\infty, \overline{\varphi}_\infty)$ izpolnjuje kompatibilnostni pogoj s poljubno lokalno karto iz družine $\mathcal{E}$.

Če družini $((V_i, \overline{\varphi}_i))_{i \in I}$ 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.

Zgled 4.9.

Opomba 4.10. 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 $S(\mathbb{C}^3) \to P^2(\mathbb{C})$, je ravno $E \subseteq P^2(\mathbb{C})$, kot zvezna slika kompakta pa je tudi sama kompaktna, torej je E kompaktna.

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

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 preslkavah 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 Λ. 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 π tudi odprta, kar je v splošnem res za vse kvocientne projekcije v prostor orbit delovanja neke topološke grupe [5, Trditev...], prepričamo pa se lahko tudi z direktnim računom. Za poljubno odprto množico $U \subseteq \mathbb{C}$ je 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.

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 ω_1 in ω_2 osnovni periodi mreže Λ in $t_1, t_2 \in \mathbb{R}$. Preslikava je dobro definirana, saj ω_1 in ω_2 tvorita realno bazo za $\mathbb{C}$, in je tudi zvezna, saj koeficienta t_1 in t_2 dobimo s projeciranjem točke $t_1\omega_1 + t_2\omega_2$ na premici skozi izhodišče v smereh ω_1 oziroma ω_2. Slednje dosežemo z realno linearno preslikavo[2] $\mathbb{C} \to \mathbb{R}^2$, 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 $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$. 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 [5, Trditev...] 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 topološko kvocient $\mathbb{C}/\Lambda$ predstavlja torus $S^1 \times S^1$.

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 4.11. *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*

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

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

Dokaz. Izberimo točko $z+\Lambda \in \mathbb{C}/\Lambda$ in naj bo $z \in \mathbb{C}$ neki predstavnik tega ekvivalnčnega 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 radija r s središčema 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 disjunktnostni vseh kopij, projekcija π ne naredi nobenih netrivialnih identifikacij na $\tilde{U}_\omega$. Iskani homeomorfizem je tako $\pi|_{\tilde{U}_\omega} : \tilde{U}_\omega \to U$. □

Opomba 4.12. V splošnem se preslikave s to lastnostjo imenujejo *krovne projekcije*.

Trditev 4.13. *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 $\varphi_i = (\pi|_{V_i})^{-1}$, kjer je $V_i \subseteq \mathbb{C}$ kopija fundamentalne okolice, tvori kompleksni atlas prostora $\mathbb{C}/\Lambda$.*

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 φ_1 in φ_2. Prepričajmo se, da je preslikava

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

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 Λ. 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 komponenti prehodna prelikava predpis oblike

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

za neki $\omega \in \Lambda$ (ta je zares odvisen samo od komponente za poveznost). Iz tega predpisa je torej razvidno, da je preslikava $\varphi_1 \circ \varphi_2^{-1}$ holomorfna.

Definicija 4.14. Naj bo $\Lambda \subseteq \mathbb{C}$ mreža. Kvocientnemu prostoru $\mathbb{C}/\Lambda$ skupaj s pripadajočim kompleksnim atlasom pravimo *kompleksni torus*.

Primer 4.15. Poglejmo si primer preslikave med tvema kompleksnima torusoma. Naj bosta Λ_1 in Λ_2 mreži v $\mathbb{C}$

5. Izomorfizem $\mathbb{C}/\Lambda \to E(\mathbb{C})$ in njegove posledice

5.1. Uniformizacija.

Izrek 5.1. *Za vsako kompleksno eliptično krivuljo $E(\mathbb{C})$ podano z enačbo*

$$E: \quad y^2z = x^3 + axz^2 + bz^3; \quad a^3 - 27b^2 \neq 0,$$

obstaja mreža $\Lambda \subseteq \mathbb{C}$, da je $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ izomorfizem Riemannovih ploskev.

Slovar strokovnih izrazov

Literatura

[1] L. V. Ahlfors, *Complex analysis*, third edition, McGraw-Hill, Inc., New York, 1979.
[2] C. G. Gibson, *Elementary geometry of algebraic curves: An undergraduate introduction*, Cambridge University Press, Cambridge, 1998.
[3] J. Globevnik in M. Brojan, *Analiza II*, verzija 10. 8. 2010, [ogled 28. 7. 2021], dostopno na `https://www.fmf.uni-lj.si/~globevnik/skriptaII.pdf`.
[4] S. Lang, *Elliptic functions*, Graduate Texts in Mathematics **112**, Springer-Verlag, New York, 1973.
[5] J. Mrčun, *Topologija*, Izbrana poglavja iz matematike in računalništva **44**, DMFA–založništvo, Ljubljana, 2008.
[6] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, New York, 1986.
[7] P. Stevenhagen, *Complex elliptic curves*, verzija 1. 10. 2013, [ogled 9. 2. 2021], dostopno na `http://www.julianlyczak.nl/teaching/EC2015-files/ec.pdf`.