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

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

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

$$f_x(x, y) = 2x = 0, \quad f_y(x, y) = 2y = 0, \quad f(x, y) = 0 \tag{1}$$

nima nobene rešitve, sistem

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

pa jih ima veliko. Namreč vsaka rešitev enačbe $f(x,y) = x^2+y^2-1 = 0$ reši sistem 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 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 $X \cap U$, t. j. 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

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

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 u_{x_1}, v_{x_1}, u_{x_2}, v_{x_2} neničelni. 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 $x = (x_0, \ldots, x_n) \in \mathbb{C}^{n+1} \setminus \{\mathbf{0}\}$ je predstavnik ekvivalenčnega razreda $[x]_\sim \in P^n(\mathbb{C})$ 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 $\lambda \in \mathbb{C}^\times$.

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 2.9. 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 2.10. 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 2.11 (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 2.12. 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 2.13.
(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 automorfizmov 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 2.14. 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 2.15. //demonstriram projektivno ekvivalenco

Trditev 2.16. *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 2.17. *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

$$G = \lambda(F \circ \mathcal{A}_\Phi). \tag{3}$$

Če je C nesingularna, je $(F_x, F_y, F_z) \neq 0$ povsod na $\mathbb{C}^3$, torej z odvajanjem zveze 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 2.18. *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 lepšo obliko, ki jo bo lažje analizirati. Tej klasični obliki pravimo *Weierstrassova normalna forma* in v njej se enačba kubike glasi

$$y^2z = x^3 + \alpha xz^2 + \beta z^3. \tag{4}$$

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

Trditev 2.19. *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 2.20. Vrednosti $4\alpha^3 + 27\beta^2$ (včasih tudi njeni nasprotni vrednosti) pravimo *diskriminanta* Weierstrassove kubike in jo običajno označimo z Δ. Ta vpeljava je usklajena z diskriminanto kubičnega polinoma $f(x) = x^3 + \alpha x + \beta$, ki pove ali ima f kakšno večkratno ničlo. To se zgodi natanko takrat, ko je njegova diskriminanta enaka 0.

V literaturi se diskriminanta Weierstrassove kubike vpelje kot

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

zaradi razlogov, ki bodo jasni pozneje. To konvencijo bomo privzeli tudi mi.

Dokaz. //računamo... □

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 2.21. *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

$$\Phi : C \to C'$$
$$[x : y : z] \mapsto [u^{-2}x : u^{-3}y : z],$$

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

$$x = u^2x' \quad y = u^3y' \quad z = z', \tag{5}$$

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 pa 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.

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

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 (5) iz prejšnje leme j-invarianta ohranja. Krajši račun pokaže

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

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 2.23. *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 2.22, preostane nam pokazati še implikacijo v levo.
//dokončat... □

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 2.21. 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. 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 2.24. 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 2.25.
(1) Ker nas bodo v nadaljevanju eliptične krivulje zanimale zgolj do projektivne ekvivalence natančno, bomo lahko brez škode za splošnost po trditvi 2.21 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 4 obravnavati malenkost prilagojeno – še vedno pa projektivno ekvivalentno – različico
$$y^2z = 4x^3 - ax^2z - bz^3.$$
Med to in klasično različico enostavno prehajamo preko projektivnosti
$$x = tx', \quad y = y', \quad z = z', \qquad \text{kjer za } t \in \mathbb{C}^\times \text{ velja } t^3 = 4.$$
Osnovne količine se tedaj povežejo preko enakosti
$$a = -t\alpha, \quad b = -\beta$$
diskriminanta in j-invarianta pa se v a in b izražata kot
$$\Delta = 16(a^3 - 27b^2) \quad \text{in} \quad j = 1728\frac{a^3}{a^3 - 27b^2}.$$

3. Eliptične funkcije

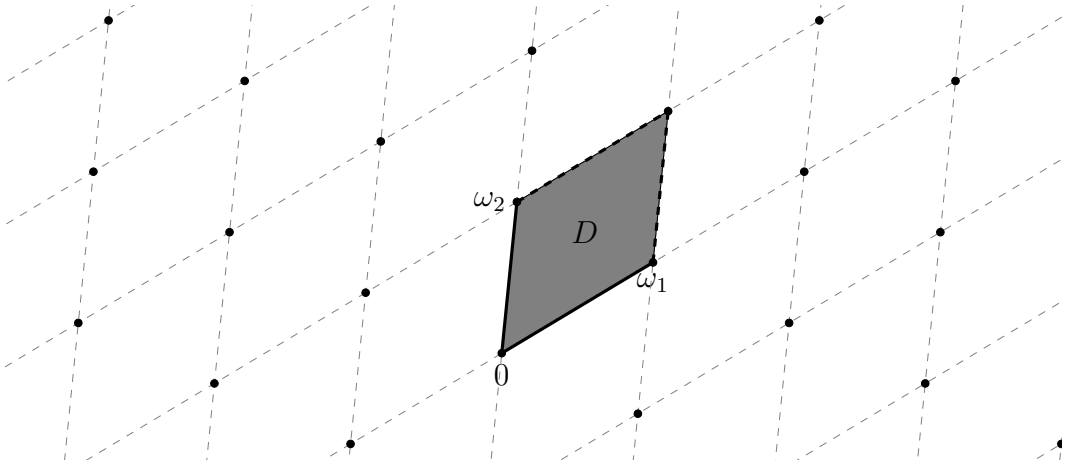
Glavna vez med eliptičnimi krivuljami in kompleksnimi torusi so t. i. *eliptične funkcije*. Da jih vpeljemo, najprej potrebujemo nekaj priprave.

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 $\Im \frac{\omega_1}{\omega_2} \neq 0$, 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.

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 s 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

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

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*

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

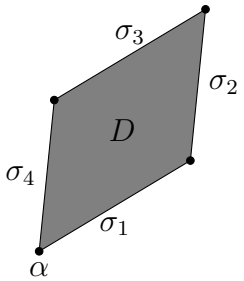
(b) $\displaystyle\sum_{w \in D} \mathrm{ord}_w(f) = 0$

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

Dokaz. (a) 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

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

s preprosto zamenjavo spremenljivk pa je zaradi periodičnosti f preprosto videti, da se integrala po nasprotnih stranicah odštejeta, kar nam da želeni rezultat.

(b) 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 (a), ki velja zaradi eliptičnosti f'/f.

(c) 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 (a) razbijemo na vsoto integralov po štirih stranicah. Argument o odštevanju integralov po nasprotnih stranicah paralelograma pa tokrat zaradi neperiodičnosti funkcije $z \mapsto z\frac{f'(z)}{f(z)}$ ne bo deloval. Z uvedbo nove spremenljivke $w = z + \omega_2$ v integral po stranici σ_1 vidimo

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

Podobno z uvedbo nove spremenljivke $w = z + \omega_1$ storimo z integralom po stranici σ_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 kosoma 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 (b) 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 pol z_0 je 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. Denimo, da je $f \in \mathbb{C}(\Lambda)$ eliptična funkcija z enim polom na fundamentalni domeni D, saj vemo že, da bi bila konstantna, če nebi imela nobenega pola po izreku 3.6. Brez škode za splošnost lahko predpostavimo, da pol leži v notranjosti D. Tedaj dobimo z integracijo po robu ∂D neničelni residuum

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

To pa je v nasprotju z izrekom 3.9 (a), ki pove, da je ta residuum – 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 t. i. *Weierstrassova funkcija* $\wp$.

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 $k > 2$ 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

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

Zadnja vrsta konvergira natanko tedaj, ko je $k - 1 > 1$ in tako po primerjalnem kriteriju dobimo absolutno kovergenco 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) Za vse $\omega \in \Lambda' \cap \Delta(0, 2r)$ zaradi kompaktnosti K obstaja

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

Ker pa je takšnih period, za katere je $|\omega| < 2r$, zgolj končno mnogo, denimo $n \in \mathbb{N}$, lahko za ϵ izberemo najmamnjšega 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 $|\omega| \geq 2r$ pa 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 absolutno konvergentne Eisensteinove vrste reda k po lemi 3.17, nam Weierstrassov M-test zagotavlja 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] □

Primer 3.20. Tako smo prišli, do prvega netrivialnega primera eliptične funkcije. Prepričajmo se, da je funkcija podana s predpisom

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

res ne le meromorfna, ampak tudi eliptična (to je vrsta iz leme 3.18, ki smo ji prišteli člen z^{-k}).

Če je $z \in \mathbb{C}$ poljuben in $\omega_0 \in \Lambda$ poljubna perioda, računamo

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

kjer smo v predzadnji enakosti upoštevali, da je translacija $\omega \mapsto \omega - \omega_0$ bijekcija mreže Λ samo vase, ki nam zgolj premeša vrstni red seštevanja v zadnji vsoti.

4. Riemannove ploskve

4.1. **Definicije in lastnosti.**

4.2. **Kompleksna struktura na eliptični krivulji.**

4.3. **Kompleksna struktura na torusu.**

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

5.1. **Uniformizacija.**

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`.