

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

1. Uvod	4
2. Algebraične krivulje	4
2.1. Afine algebraične krivulje	5
2.2. Projektivne algebraične krivulje	6
2.3. Nesingularne kubike	8
3. Eliptične funkcije	8
3.1. Lastnosti eliptičnih funkcij	8
3.2. Weierstrassova funkcija \wp	9
4. Riemannove ploskve	9
4.1. Definicija in lastnosti	9
4.2. Kompleksna struktura na eliptični krivulji	9
4.3. Kompleksna struktura na torusu	10
5. Izomorfizem $\mathbb{C}/\Lambda \rightarrow E(\mathbb{C})$ in njegove posledice	10
Slovar strokovnih izrazov	11
Literatura	11

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 prosotra sploh sprejmemo veljavne rešitve. Spomnimo se fundamentalnega 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 krivulje pomembno vlogo v kriptografiji, 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 strukturo 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, ključno 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 katerimi 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 $\mathbb{C}[x_1, \dots, x_n]$ označuje kolobar polinomov n spremenljivk s kompleksnimi koeficienti. Množica ničel poljubnega polinoma $f \in \mathbb{C}[x_1, \dots, x_n]$ 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 $\nabla f(x_0, y_0) = 0$, $f(x_0, y_0) = 0$. Toda ta definicija zaenkrat ni dobra, saj polinom $f \in \mathbb{C}[x, y]$ ni enolično določen s krivuljo C . Zato najprej uvedemo pojem minimalnega polinoma krivulje C .

Primer 2.2. demonstracija zakaj je pomembno uvesti minimalni polinom.

Definicija 2.3. Naj bo C afina algebraična krivulja. *Minimalni polinom* krivulje C je polinom $f \in \mathbb{C}[x, y]$ najmanjše stopnje, za katerega velja $V(f) = C$.

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.

To nam omogoči formulirati prvo opazko.

Trditev 2.5. Vsaka afina algebraična krivulja $C \subseteq \mathbb{C}^2$ brez singularnih točk je z identifikacijo $\mathbb{C}^2 \equiv \mathbb{R}^4$ gladka 2-podmnogoterost oz. ploskev.

Dokaz. pozneje. □

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 poimenujemo 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 samo zamenjamo polje realnih števil s \mathbb{C} se povedano bistveno ne spremeni. Še vedno ohranimo dejstvo, da

število "linearno neodvisnih" enačb ustreza kodimenzijski podmnogoterosti in analogno tudi dimenzija podmnogoterosti ustreza razliki (kompleksne) dimenzije ambientnega prostora in kodimenzijske. 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. Glavna ideja za konstrukcijo

Definicija 2.6. *Kompleksen projektiven prostor* dimenzije n , je

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

Pri tem \mathbb{C}^\times označuje multiplikativno grupo kompleksnih števil oz. $\mathbb{C} \setminus \{0\}$. [//mo- goče dam to rajši samo v slovar.](#) Pri tem bomo $P^2(\mathbb{C})$ kot projektiven prostor dimenzije 2 imenovali *kompleksna projektivna ravnina*. Pridevnik kompleksna bomo v nadaljevanju pogosto izpustili.

Primer 2.7. 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.

Projektivni prostor si lahko predstavljmo kot množico vseh enodimenzionalnih vektorskih podprostorov. 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 $x = (x_0, \dots, x_n) \in \mathbb{C}^{n+1} \setminus \{0\}$ je predstavnik ekvivalenčnega razreda $[x]_\sim \in P^n(\mathbb{C})$ kar v homogenih koordinatah zapišemo z

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

in zanje velja

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

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 [1, 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 so homogeni polinomi dobro definirani kot funkcije na projektivni ravnini, saj je njihova vrednost zares odvisna od projektivne točke – celotnega ekvivalečnega razreda in ne le od izbranega predstavnika.

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

Definicija 2.8. 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 $V(f) = C$.

2.3. Nesingularne kubike.

3. ELIPTIČNE FUNKCIJE

3.1. Lastnosti eliptičnih funkcij.

3.2. Weierstrassova funkcija \wp .

4. RIEMANNOVE PLOSKVE

4.1. Definicija in lastnosti.

4.2. Kompleksna struktura na eliptični krivulji.

4.3. Kompleksna struktura na torusu.

5. IZOMORFIZEM $\mathbb{C}/\Lambda \rightarrow E(\mathbb{C})$ IN NJEGOVE POSLEDICE

SLOVAR STROKOVNIH IZRAZOV

LITERATURA

- [1] J. Mrčun, *Topologija*, Izbrana poglavja iz matematike in računalništva **44**, DMFA–založništvo, Ljubljana, 2008.
- [2] S. Lang, *Elliptic functions*, Graduate Texts in Mathematics **112**, Springer-Verlag, New York, 1973.
- [3] P. Stevenhagen, *Complex elliptic curves*, verzija 1. 10. 2013, [ogled 9. 2. 2021], dostopno na <http://www.julianlyczak.nl/teaching/EC2015-files/ec.pdf>.