Algebraične krivulje

Luka Horjak (lukahorjak@student.uni-lj.si)

31. marec 2022

Kazalo

Uvod

V tem dokumentu so zbrani moji zapiski s predavanj predmeta Algebraične krivulje v letu 2021/22. Predavatelj v tem letu je bil prof. dr. Jakob Cimprič.

Zapiski niso popolni. Manjka večina zgledov, ki pomagajo pri razumevanju definicij in izrekov. Poleg tega nisem dokazoval čisto vsakega izreka, pogosto sem kakšnega označil kot očitnega ali pa le nakazal pomembnejše korake v dokazu.

Zelo verjetno se mi je pri pregledu zapiskov izmuznila kakšna napaka – popravki so vselej dobrodošli.

1 Algebraične krivulje in projektivno zaprtje

1.1 Definicija

Definicija 1.1.1. Polinom $P \in K[x_1, \ldots, x_n]$ je *nerazcepen*, če se ga ne da zapisati kot produkt dveh nekonstantnih polinomov iz $K[x_1, \ldots, x_n]$.

17. februar 2022

Definicija 1.1.2. Za polinom $F \in K[x, y]$ označimo njegovo množico ničel

$$V(F) = \left\{(a, b) \in K^2 \;\middle|\; F(a, b) = 0\right\}.$$

Opomba 1.1.2.1. Množicam oblike $V(f)$ pravimo *(afine) algebraične množice.*

Definicija 1.1.3. Množica $\mathcal{C} \subseteq K^2$ je *algebraična krivulja*, če obstaja tak nekonstanten polinom $F \in K[x, y]$, da je

$$\mathcal{C} = V(F).$$

Pravimo, da je krivulja *nerazcepna*, če je v zgornji definiciji F nerazcepen polinom.

Definicija 1.1.4. *Afina preslikava* je kompozitum linearne preslikave in translacije. Če je ta linearna preslikava obrnljiva, je tudi afina preslikava obrnljiva in ji pravimo *afina transformacija.*

Trditev 1.1.5. Kompozitum afinih transformacij je afina transformacija.

Dokaz. Afine transformacije so natanko preslikave

$$(x, y) \mapsto (ax + by + \alpha, cx + dy + \beta),$$

kjer je $ad \neq bc$. $\square$

Definicija 1.1.6. Krivulji $\mathcal{C}$ in $\mathcal{D}$ sta *afino ekvivalentni*, če obstaja afina transformacija Φ, za katero je $\Phi(\mathcal{C}) = \mathcal{D}$.

Opomba 1.1.6.1. Afina ekvivalenca je ekvivalenčna relacija.

1.2 Studyjeva lema

24. februar 2022

Definicija 1.2.1. *Minimalni polinom* algebraične množice $V(f)$ je produkt nerazcepnih faktorjev f.

Definicija 1.2.2. *Stopnja* algebraične množice je stopnja njenega minimalnega polinoma.

Definicija 1.2.3. Naj bo A komutativen kolobar in $f, g \in A[x]$. Označimo

$$f = \sum_{i=0}^{m} a_i x^{m-i} \quad \text{in} \quad g = \sum_{i=0}^{n} b_i x^{n-i}.$$

Rezultanto polinomov f in g definiramo kot

$$\operatorname{Res}(f,g) = \det \begin{bmatrix} \underbrace{\boxed{\begin{matrix} a_0 & a_1 & \dots & a_m & & \\ & \ddots & \ddots & \ddots & \ddots & \\ & & a_0 & a_1 & \dots & a_m \end{matrix}}}_{(n+m)\times n} \\ \underbrace{\boxed{\begin{matrix} b_0 & b_1 & \dots & b_n & & \\ & \ddots & \ddots & \ddots & \ddots & \\ & & b_0 & b_1 & \dots & b_n \end{matrix}}}_{(n+m)\times m} \end{bmatrix}$$

Izrek 1.2.4. Naj bo A komutativen kolobar brez deliteljev niča z enolično faktorizacijo. Za nekonstantna polinoma $f, g \in A[x]$ sta naslednji trditvi ekvivalentni:

i) $\operatorname{Res}(f,g) = 0$

ii) f in g imata skupen nekonstanten faktor.

Dokaz. Dokazali bomo, da sta obe trditvi ekvivalentni temu, da obstajata $\varphi, \psi \in A[x]$, ne oba enaka 0, za katera velja

$$\varphi f + \psi g = 0, \quad \deg \varphi < \deg g \quad \text{in} \quad \deg \psi < \deg f.$$

Rezultanta je enaka nič natanko tedaj, ko so vrstice linearno odvisne, od koder dobimo polinoma φ in ψ. Zaradi pogoja s stopnjami dobimo, da imata f in g skupen faktor.

Za obratno smer preprosto izberemo

$$\varphi = \frac{g}{\gcd(f,g)} \quad \text{in} \quad \psi = -\frac{f}{\gcd(f,g)}. \qquad \square$$

Lema 1.2.5 (Study)**.** Naj bo $f \in \mathbb{C}[x,y]$ nerazcepen nekonstanten polinom. Tedaj za vsak polinom $g \in \mathbb{C}[x,y]$ velja

$$f \mid g \iff V(f) \subseteq V(g).$$

Dokaz. Naj bo

$$f = \sum_{i=0}^{m} a_i x^{m-i} \quad \text{in} \quad g = \sum_{i=0}^{n} b_i x^{n-i},$$

kjer so $a_i, b_i \in \mathbb{C}[y]$.[1] Brez škode za splošnost naj bo $m \geq 1$. Ker je $a_0 \neq 0$, obstaja tak y_0, da je $a_0(y_0) \neq 0$.

Oglejmo si polinom $f_{y_0}(x) = f(x, y_0)$. Ker je $\mathbb{C}$ algebraično zaprto polje, ima ta polinom ničlo x_0. Sledi, da je $f(x_0, y_0) = 0$, zato $(x_0, y_0) \in V(g)$, zato je tudi

$$g_{y_0}(x_0) = 0.$$

Sledi, da imata polinoma f_{y_0} in g_{y_0} skupni faktor $x - x_0$ in je njuna rezultanta enaka 0. Sledi, da je y_0 ničla rezultante $\mathrm{Res}(f, g)$. Ker to velja za skoraj vse y_0, je $\mathrm{Res}(f, g) = 0$, oziroma, da imata f in g skupni faktor, to je f. □

Opomba 1.2.5.1. Zgornja lema je znana tudi pod imenom *Nullstellensatz*.

Posledica 1.2.5.2. Za vsak nekonstanten polinom $f \in \mathbb{C}[x, y]$ velja $V(f) \neq \emptyset$.

Dokaz. Naj bo h nerazcepen faktor f. Tedaj za vsak $g \in \mathbb{C}[x, y]$ velja $\emptyset = V(h) \subseteq V(g)$, zato $h \mid g$, kar je protislovje. □

Posledica 1.2.5.3. Vsaka algebraična množica enolično določa nerazcepne faktorje pripadajočega polinoma. Vsako algebraično množico lahko na enoličen način zapišemo kot unijo nerazcepnih.

Dokaz. Naj bo

$$f = c \cdot \prod_{i=1}^{k} f_i^{n_i}.$$

Sledi, da je

$$V(f) = \bigcup_{i=1}^{k} V(f_i).$$

Če je $V(f) = V(g)$, od tod sledi, da $f_i \mid g$ za vse i. Simetrično dobimo $g_i \mid f$. □

[1] Ker je $\mathbb{C}$ komutativen, velja $\mathbb{C}[x, y] = \mathbb{C}[y][x]$.

1.3 Projektivna ravnina

3. marec 2022

Definicija 1.3.1. Naj bo K polje. *Afina ravnina* je množica $A_2(K) = K^2$.

Definicija 1.3.2. Naj bo K polje. *Projektivna ravnina* je množica vseh premic v K^3, ki potekajo skozi izhodišče. Označimo jo s $P_2(K)$.

Definicija 1.3.3. *Projektivne koordinate* projektivne točke je razmerje

$$(x : y : z).$$

Opomba 1.3.3.1. Vsakim projektivnim koordinatam, različnim od $(0 : 0 : 0)$, ustreza natanko ena projektivna točka.

Opomba 1.3.3.2. Projektivno ravnino lahko identificiramo z afino ravnino, ki ji dodamo *točke v neskončnosti*. Točkam v projektivni ravnini, ki so oblike $(x : y : 1)$, identificiramo s točko (x, y) v afini ravnini in jim pravimo *končne točke*.

Točke $(x : y : 0)$ ustrezajo *točkam v neskončnosti*, ki jih identificiramo s snopi vzporednic.

Opomba 1.3.3.3. Projektivno ravnino $P_2(\mathbb{R})$ lahko identificiramo tudi s sfero S^2.

Definicija 1.3.4. *Projektivna premica* je vsaka ravnina, ki gre skozi izhodišče. Identificiramo jo z afino premico, ki ji dodamo pripadajočo točko v neskončnosti, oziroma premico v neskončnosti.

Opomba 1.3.4.1. V sferičnem modelu so premice glavni krogi.

Opomba 1.3.4.2. Vsaki dve različni projektivni premici se sekata v natanko eni projektivni točki. Skozi vsaki dve različni projektivni premici poteka natanko ena projektivna premica.

1.4 Projektivne algebraične krivulje

Definicija 1.4.1. Polinom $F \in \mathbb{C}[x, y, z]$ je *homogen*, če so vsi njegovi monomi iste stopnje.

Opomba 1.4.1.1. F je homogen polinom stopnje n natanko tedaj, ko za vse x, y, z in λ velja

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

Definicija 1.4.2. Množica projektivnih ničel homogenega polinoma $F \in \mathbb{C}[x, y, z]$ je

$$V_h(F) = \{(a : b : c) \in P_2(\mathbb{C}) \mid F(a, b, c) = 0\}.$$

Definicija 1.4.3. Podmnožica $\mathcal{C} \subseteq P_2(\mathbb{C})$ je *projektivna algebraična krivulja*, če obstaja tak nekonstanten homogen polinom $F \in \mathbb{C}[x, y, z]$, da velja

$$\mathcal{C} = V_h(F).$$

Definicija 1.4.4. *Homogenizacija* polinoma $f \in \mathbb{C}[x, y]$ je polinom

$$F(x, y, z) = z^{\deg f} \cdot f\left(\frac{x}{z}, \frac{y}{z}\right).$$

10. marec 2022

Opomba 1.4.4.1. Naj bo F homogenizacija polinoma f. Tedaj je

$$V_h(F) \cap \{(x : y : z) \mid z \neq 0\} = \{(x : y : 1) \mid f(x, y) = 0\}.$$

Množico $V_h(F) \cap \{(x : y : z) \mid z \neq 0\}$ lahko identificiramo z $V(f)$, preostale ničle pa s točkami v neskončnosti.

1.5 Projektivne transformacije

Definicija 1.5.1. *Projektivna transformacija* je bijektivna preslikava $\Phi\colon P_2(\mathbb{C}) \to P_2(\mathbb{C})$, ki deluje po predpisu

$$(x : y : z) \mapsto (ax + by + cz : dx + ey + fz : gx + hy + iz).$$

Opomba 1.5.1.1. Preslikava je dobro definirana, saj sta obe strani homogeni.

Trditev 1.5.2. Preslikava z zgornjim predpisom je bijektivna natanko tedaj, ko je

$$\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} \neq 0.$$

Dokaz. The proof is obvious and need not be mentioned. □

Opomba 1.5.2.1. Kompozitum projektivnih transformacij je projektivna transformacija. Prav tako je tudi inverz projektivne transformacije projektivna transformacija.

Trditev 1.5.3. Slika algebraične krivulje s projektivno transformacijo je algebraična krivulja.

Dokaz. Velja

$$\Phi(V_h(F)) = \{\Phi(x : y : z) \mid F(x, y, z) = 0\} = \left\{(x : y : z) \;\middle|\; (F \circ \Phi^{-1})(x, y, z) = 0\right\}. \quad \square$$

Definicija 1.5.4. Pravimo, da so štiri točke v *splošni legi*, če nobene tri niso kolinearne.

Opomba 1.5.4.1. Tri točke so kolinearne natanko tedaj, ko so linearno odvisne, oziroma ko je determinanta njihovih koordinat enaka 0.

Lema 1.5.5 (O štirih točkah)**.** Če so točke p_1, p_2, p_3 in p_4 ter q_1, q_2, q_3 in q_4 v splošni legi, obstaja natanko ena projektivna transformacija Φ, za katero je $\Phi(p_i) = q_i$ za vse i.

Dokaz. Dovolj je pokazati, da lahko točke p_i preslikamo v točke

$$t_1 = (1 : 0 : 0), \quad t_2 = (0 : 1 : 0), \quad t_3 = (0 : 0 : 0) \quad \text{in} \quad t_4 = (1 : 1 : 1).$$

Naj bo $p_i = (x_i : y_i : z_i)$. Naj bo

$$A = \begin{bmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{bmatrix}^{-1}.$$

Naj bo Φ projektivna transformacija, ki ustreza matriki A. Sledi, da so točke $\Phi(p_i)$ v splošni legi, zato za $(a : b : c) = \Phi(p_4)$ velja, da so $a, b, c \neq 0$. Sedaj zgornjo projektivno transformacijo preprosto komponiramo s transformacijo

$$(x : y : z) \mapsto \left(\frac{x}{a}, \frac{y}{b}, \frac{z}{c}\right). \quad \square$$

1.6 Presečišča in njihove večkratnosti

Definicija 1.6.1. *Večkratnost* presečišča projektivne premice in krivulje je stopnja pripadajočega linearnega faktorja v faktorizaciji polinoma

$$F(t(x,y)),$$

kjer je t parametrizacija premice. Označimo jo z $\operatorname{mult}_p(F \cap L)$.

Opomba 1.6.1.1. Vsota večkratnosti vseh presečišč je enaka $\deg F$.

Trditev 1.6.2. Naj bosta f in g polinoma v dveh spremenljivkah, monična v spremenljivki y. Tedaj imata za vsako ničlo a polinoma $\operatorname{Res}(f,g)$ polinoma $f(a,y)$ in $g(a,y)$ skupno ničlo.

Dokaz. Velja

$$\operatorname{Res}(f(a,y), g(a,y)) = 0,$$

zato imata skupni faktor. □

Trditev 1.6.3. Naj bosta

$$F(x,y,z) = \sum_{i=0}^{m} a_i(x,y) z^{m-i} \quad \text{in} \quad G(x,y,z) = \sum_{i=0}^{n} b_i(x,y) z^{n-i}$$

homogena polinoma. Tedaj je $\operatorname{Res}(f,g)$ homogen polinom stopnje

$$\deg F \cdot \deg G - \deg a_0 \cdot \deg b_0.$$

Dokaz. Naj bo $d = \deg a_0$ in $e = \deg b_0$. Sledi, da je

$$\deg a_i = d + i \quad \text{in} \quad \deg b_i = e + i.$$

Naj bo $R = \operatorname{Res}(f,g)$. Dovolj je pokazati, da za vse λ velja

$$R(\lambda x, \lambda y) = \lambda^{mn+dn+em} R(x,y).$$

Z uporabo $a_i(\lambda x, \lambda y) = \lambda^{d+i} a_i(x,y)$ lahko determinanto rezultante poenostavimo. Prvo vrstico razširimo z λ^e, drugo z λ^{e+1} in tako dalje v prvih n vrsticah, nato pa podobno naredimo v zadnjih m vrsticah. S tem smo zagotovili, da so v vsakem stolpcu eksponenti λ enaki in jih lahko izpostavimo. Sledi, da je

$$\prod_{i=e}^{e+n-1} \lambda^i \cdot \prod_{i=d}^{d+m-1} \lambda^i \cdot R(\lambda x, \lambda y) = \prod_{i=e+d}^{d+e+m+n-1} \lambda^i \cdot R(x,y),$$

oziroma

$$\lambda^{\frac{n(2e+n-1)}{2} + \frac{m(2d+m-1)}{2}} R(\lambda x, \lambda y) = \lambda^{\frac{(2d+2e+m+n-1)(m+n)}{2}} R(x,y).$$

Sledi, da je

$$R(\lambda x, \lambda y) = \lambda^{mn+dn+em} R(x,y).$$ □

Trditev 1.6.4. Naj bosta F in G nekonstantna polinoma brez skupnega nekonstantnega faktorja. Tedaj je $V_h(F) \cap V_h(G)$ končna množica.

Dokaz. Naj bo S točka, ki ne leži na $V_h(FG)$. Naj bo ℓ premica, ki ne gre skozi S. S pomočjo leme o štirih točkah lahko privzamemo, da je $S = (0:0:1)$ in ima premica ℓ enačbo $z = 0$.

Naj bo $(a:b:0)$ projekcija presečišča prek S na premico ℓ. Sledi, da ima presečišče koordinate $(a:b:c)$. Iščemo torej taka števila a in b, da imata $F(a,b,z)$ in $G(a,b,z)$ skupno ničlo, to pa so ravno ničle polinoma $\mathrm{Res}_{f,g}(a,b)$, to pa je neničeln homogen polinom v dveh spremenljivkah. Sledi, da ga lahko faktoriziramo na linearne faktorje, zato ima končno mnogo ničel.

Opazimo še, da na vsaki premici skozi S leži končno mnogo presečišč. V nasprotnem primeru je namreč premica vsebovana v eni izmed krivulj, kar je v protislovju s tem, da S ne leži na krivuljah. □

Izrek 1.6.5 (Bezout)**.** Naj bosta F in G tuja homogena polinoma v treh spremenljivkah. Število presečišč F in G je navzgor omejeno z $\deg F \cdot \deg G$.

24. marec 2022

Dokaz. Naj bo S projektivna točka, ki ne leži na $F = 0$ in $G = 0$ ter niti na nobeni premici, ki gre skozi dve presečišči teh krivulj, ℓ pa premica, ki ne gre skozi S. Presečišča F in G prek S projeciramo na ℓ. Po izbiri točke S projekciji nobenih dveh presečišč ne sovpadata. Sedaj s projektivno transformacijo preslikamo S v $(0:0:1)$ in ℓ v premico v neskončnosti.

Točka $(a:b:0)$ je projekcija nekega presečišča natanko tedaj, ko obstaja tak c, da je $F(a,b,c) = G(a,b,c) = 0$, kar je ekvivalentno temu, da je

$$\mathrm{Res}_{F,G}(a,b) = 0,$$

zato je število presečišč manjše od stopnje rezultante. □

Opomba 1.6.5.1. Ker je

$$0 \neq F(0,0,1),$$

velja $\deg a_0 = \deg b_0 = 0$. Zgornje meje na ta način zato ne moremo izboljšati.

Definicija 1.6.6. *Večkratnost* v točki $(a:b:c)$ krivulj $F = 0$ in $G = 0$ je stopnja ničle $(a:b:c)$ v $\mathrm{Res}_{F,G}$. Označimo jo z $\mathrm{mult}_p(F \cap G)$.

Posledica 1.6.6.1. Vsota večkratnosti presečišč je enaka produktu stopenj.

Opomba 1.6.6.2. Projektivne transformacije ohranjajo večkratnosti (Gibson).

Opomba 1.6.6.3. Ta definicija se ujema z definicijo večkratnosti premice in krivulje.

2 Tangente in singularnosti

2.1 Tangente

Definicija 2.1.1. Naj bo f polinom v treh spremenljivkah in (a, b) njegova ničla. *Tangenta* na f v (a, b) je premica

$$\frac{\partial f}{\partial x}(x-a)+\frac{\partial f}{\partial y}(y-b)=0,$$

če nista oba odvoda enaka 0.

Definicija 2.1.2. Točka (a, b) na $f(x, y) = 0$ je *regularna*, če velja

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

sicer je *singularna*.

Definicija 2.1.3. Naj bo F nekonstanten homogen polinom v treh spremenljivkah in $(a : b : c)$ njegova ničla. *Tangenta* na F v $(a : b : c)$ je premica

$$\frac{\partial F}{\partial x}(a,b,c)\cdot(x-a)+\frac{\partial F}{\partial y}(a,b,c)\cdot(y-b)+\frac{\partial F}{\partial z}(a,b,c)\cdot(z-c)=0,$$

če niso vsi odvodi enaki 0.

Izrek 2.1.4 (Eulerjeva identiteta)**.** Če je F homogen polinom v treh spremenljivkah stopnje n, je

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

Dokaz. Velja

$$F(tx,ty,tz)=t^nF(x,y,z),$$

zato je

$$x\frac{\partial F}{\partial x}(tx,ty,tz)+y\frac{\partial F}{\partial y}(tx,ty,tz)+z\frac{\partial F}{\partial z}(tx,ty,tz)=n\cdot t^{n-1}F(x,y,z).$$

Sedaj preprosto vstavimo $t = 1$. $\square$

Posledica 2.1.4.1. Enačba tangente se poenostavi v

$$\frac{\partial F}{\partial x}(a,b,c)\cdot x+\frac{\partial F}{\partial y}(a,b,c)\cdot y+\frac{\partial F}{\partial z}(a,b,c)\cdot z=0.$$

Definicija 2.1.5. Naj bo p singularna točka na $f(x, y) = 0$. *Tangente* v točki p na krivuljo $f(x, y) = 0$ so tiste premice, za katere je presečna večkratnost večja od minimalne. Minimumu presečnih večkratnosti pravimo *red* točke p in ga označimo z $\operatorname{ord}_p(f)$.

2.2 Singularne točke

31. marec 2022

Trditev 2.2.1. Če je f minimalen polinom krivulje, velja

$$\operatorname{ord}_p(f) = \min\left\{i+j \;\middle|\; \frac{\partial^{i+j} f}{\partial x^i \partial y^j}(p) \neq 0\right\}.$$

Dokaz. Naj bo

$$g(t) = f(x_0 + at, y_o + bt).$$

Tedaj za največjo potenco t^k, ki deli g, velja

$$g(0) = g'(0) = \cdots = g^{(k-1)}(0) = 0 \quad \text{in} \quad g^{(k)} \neq 0.$$

Velja pa

$$g^{(s)}(0) = \sum_{i+j=s} \binom{s}{i} \frac{\partial^s f}{\partial x^i \partial y^j}(x_0, y_0) a^i b^j. \qquad \square$$

Opomba 2.2.1.1. Če je singularna točka izhodišče, je red enak najmanjši stopnji monoma v f.

Posledica 2.2.1.2. Za tuja polinoma f in g velja

$$\operatorname{ord}_p(fg) = \operatorname{ord}_p(f) + \operatorname{ord}_p(g).$$

Dokaz. The proof is obvious and need not be mentioned. $\square$

Posledica 2.2.1.3. Če je $\operatorname{ord}_p(\mathcal{C}) = \deg \mathcal{C} - 1$, ima $\mathcal{C}$ racionalno parametrizacijo.

Dokaz. Velja

$$f(x, tx) = f_{d-1}(x, tx) + f_d(d, tx) = x^{d-1} f_{d-1}(1, t) + x^d f_d(1, t).$$

Sledi, da je

$$x = -\frac{f_{d-1}(1,t)}{f_d(1,t)} \quad \text{in} \quad y = -\frac{t f_{d-1}(1,t)}{f_d(1,t)}. \qquad \square$$

Posledica 2.2.1.4. Naj bo L premica, ki seka $\mathcal{C}$ v končno mnogo točkah. Tedaj velja

$$\sum_{p \in \mathcal{C} \cap L} \operatorname{ord}_p \leq \deg \mathcal{C}.$$

Dokaz. Uporabimo Bezoutov izrek. $\square$

2.3 Tangente v singularnih točkah

Stvarno kazalo