Algebraične krivulje

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

24. februar 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

1.1 Definicija

17. februar 2022

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

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 $ad \neq bc$. □

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

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

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

Rezultanta 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 $\operatorname{Res}(f, g)$. Ker to velja za skoraj vse y_0, je $\operatorname{Res}(f, g) = 0$, oziroma, da imata f in g skupni faktor, to je f. $\square$

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. $\square$

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 $g_i \mid f$. $\square$

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

Stvarno kazalo