Algebraične krivulje

Hugo Trebše (hugo.trebse@gmail.com)

5. marec 2025

Kazalo

1 Uvod

Definicija 1.1

Algebraična krivulja je množica ničel nekonstantnega polinoma v 2 spremenljivkah.

Definicija 1.2

Za vsak polinom $F \in \mathbb{C}[X, Y]$ definiramo množico njegovih ničel kot

$$V(F) = \{(a, b) \in \mathbb{C}^2 \mid F(a, b) = 0\}$$

Velja, da je

$$V(FG) = V(F) \cup V(G)$$

Definiramo stopnjo polinoma kot maksimalno stopnjo monoma, stopnjo monoma pa kot vsoto stopenj potenc spremenljivk.

Kot opomba dodamo, da v kolobarju $\mathbb{C}[X, Y]$ nimamo istih algebraičnih lastnosti kot v kolobarju $\mathbb{C}[X]$, saj bazni kolobar $\mathbb{C}[X]$ ni polje. V specifičnem primeru nimamo evklidovega izreka o deljenju polinomov. Še zmeraj pa velja izrek o enolični faktorizaciji ter dejstvo, da $\mathbb{C}[X, Y]$ nima deliteljev niča.

Kaj pa če imamo dano množico in želimo najti polinom, katera množica ničel je slednja? Enoličnost takega polinoma ni zagotovljena.

Definicija 1.3

Podmnožica $C \subsetneq \mathbb{C}^2$ je nerazcepna algebraična krivulja, če obstaja tak nerazcepen, nekonstanten polinom $F \in \mathbb{C}[X, Y]$, da je

$$V(F) = C$$

Opazimo, da $f \mid g \implies V(f) \subseteq V(g)$.

Izrek 1.4: Nullstellensatz / Studyjeva lema

Če je f nerazcepen in če velja $V(f) \subseteq V(g)$, potem $f \mid g$

Posledice Nullstellensatza:

Trditev 1.5

Vsaka algebraična krivulja je neprazna.

Dokaz. Denimo $V(f) = \emptyset$. Potem za nerazcepen faktor h polinoma f velja $V(h) = \emptyset$. Tako je $V(h) = \emptyset \subseteq V(h + 1) \implies h \mid h + 1 \implies h$ konstanten. $\square$

V kolikšni meri algebraična krivulja določa svoj polinom? Če je $C = V(f)$ in $C = V(g)$ kakšna je povezava med f in g?

Trditev 1.6

Če je $V(f) = V(g)$ za neka nekonstantna $f, g \in \mathbb{C}[X, Y]$, potem imata f in g iste nerazcepne faktorje.

Dokaz. Pokažemo, da $V(f) \subseteq V(g)$ implicira, da ima g vse nerazcepne faktorje f. Sledi po Nullstellensatzu. □

Trditev 1.7

Vsako krivuljo se da na en sam način zapisati kot unijo nerazcepnih faktorjev.

Dokaz. Posledica zgornjih dveh trditev. □

Definicija 1.8

Produktu nerazcepnih faktorjev pravimo *minimalni polinom* krivulje C.
Iz enoličnosti (do konstante natančno) minimalnega polinoma sledi, da je definicija *stopnje krivulje* kot stopnje njenega minimalnega polinoma dobra.

1.1 Dokaz Nullstellensatza

Za dokaz Nullstellensatza (Studyjeve leme) potrebujemo nekaj pomožnih trditev. Definirali bomo rezultanto dveh polinomov ter pokazali, da je enaka nič natanko tedaj, ko imata nekonstanten skupni faktor.

Delali bomo v večji splošnosti, namreč opazovali bomo $\mathbb{C}[X, Y] = \mathbb{C}[Y][X] = A[X]$, kjer je A komutativen kolobar z enoto, brez deliteljev niča, ter z enolično faktorizacijo na nerazcepne faktorje.

$f, g \in A[X]$,

$$f(X) = a_0 X^m + \ldots + a_m$$
$$g(X) = b_0 X^n + \ldots + b_n$$

Definrajmo rezultanto polinomov kot:

$$Res(f,g) = \begin{vmatrix} a_0 & a_1 & a_2 & \dots & a_m & 0 & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_{m-1} & a_m & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & a_{m-n} & a_{m-n+1} & \dots & a_m \\ b_0 & b_1 & b_2 & \dots & b_n & 0 & \dots & \vdots \\ 0 & b_0 & b_1 & \dots & b_{n-1} & b_n & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & b_0 & b_1 & \dots & b_n \end{vmatrix}$$

Imamo tehnične težave, saj je determinanta nad celim kolobarjem (ne poljem), tako ne velja nujno dejstvo o invertibilnosti in linearni neodvisnosti vrstic/stolpcev ob neničelnosti determinante. To popravimo tako, da A vložimo v njegovo polje ulomkov. Če pomnožimo z imenovalci ulomkov nad poljem ulomkov tako nazaj dobimo željeni dejstvi.

Dokazali bomo ekvivalenco naslednjih trditev:

- $Res(f,g) = 0$.
- $\exists\, \varphi, \psi \in A[X]$, ki nista oba enaka 0, da je
$$\varphi f + \psi g = 0.$$
- f, g imata skupen nekonstanten faktor.

Dokaz. Kdaj je $Res(f,g) = 0$? Natanko tedaj, ko so vrstice $(m+n) \times (m+n)$ matrike linearno neodvisne nad poljem ulomkov A. Hitro dobimo, da je slednje ekvivalentno obstaju $\psi, \varphi \in A[X]$, $\deg(\varphi) < \deg(g)$ ter $\deg(\psi) < \deg(f)$, da je

$$\varphi f + \psi g = 0$$

.

Iz pogoja o stopnjah sledi, da imata f in g skupni faktor. Implikacija v drugo smer je očitna po izbiri $\varphi = \frac{g}{\gcd(f,g)}$ ter $\psi = \frac{-f}{\gcd(f,g)}$ □

S to pomožno trditvijo dokažemo Studyjevo lemo. Naj sta $f = \sum a_i X^{m-1}$ ter $g = \sum b_i X^{n-i}$, kjer so $\{a_i\}$ ter $\{b_i\}$ elementi $\mathbb{C}[Y]$. Ker je $a_0 \neq 0$ obstaja y_0, da je $a_0(y_0) \neq 0$. Naj bo $f_{y_0}(x) = f(x, y_0)$. Zaradi algebraične zaprtosti $\mathbb{C}$ ima ta polinom ničlo x_0. Sledi, da je $(x_0, y_0) \in V(f) \subseteq V(G)$. Sledi, da je rezultanta f_{y_0} ter g_{y_0} ničelna, saj imata oba ničlo x_0. Tako sledi, da je y_0 ničla rezultante $Res(f,g)$. Ker to velja za skoraj vse y_0 (tiste vrednosti v katerih $a_0(y_0) \neq 0$) sledi, da je $Res(f,g) = 0$.

1.2 Vaje

1.2.1 Parametrizacija

Imamo krivuljo $C \in \mathbb{A}^2$ v afini ravnini. Želimo najti parametrizacijo $r : \mathbb{C} \to \mathbb{C}^2$

$$t \mapsto (x(t), y(t)),$$

da je $r(\mathbb{C}) = C$.

Definicija 1.9

Parametrizaciji množice (če obstaja) pravimo racionalna parametrizacija, če velja:

- Za vse razen končno mnogo kompleksnih števil racionalni funkciji $x(t), y(t)$ zadoščata $f(x(t), y(t)) = 0$, kjer je f polinom, za katerega velja $C = V(f)$
- Za vse razen končno mnogo (x, y), ki zadoščajo $f(x, y) = 0$ obstaja enoličen t, da velja $(x, y) = (x(t), y(t))$.

Primer 1.10

Parametrizirajmo krožnico $x^2 + y^2 = 1$ v $\mathbb{R}^2$.

Rešitev. Odstranimo točko $(-1, 0)$ ter izvajamo stereografsko projekcijo, kjer vzamemo za parameter t strmino premice. Ker točka (x, y) leži na premici skozi $(-1, 0)$ velja $y = t(x + 1)$, ker pa je točka (x, y) na krožnici velja $x^2 + y^2 = 1$. Dobimo:

$$\begin{aligned} x^2 + t^2(x+1)^2 - 1 &= 0 \\ x^2(t^2+1) + 2t^2x + t^2 - 1 &= 0 \\ (x+1)(x - 1 + t^2(x+1)) &= 0 \\ x &= \frac{1-t^2}{1+t^2} \end{aligned}$$

kjer smo faktorizacijo opazili, saj imamo gotovo tudi rešitev $x = -1$ iz geometrijske strukture problema. Parametrizacija je tako

$$t \mapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right)$$

□

Primer 1.11

V $\mathbb{R}^2$ poišči racionalno parametrizacijo hiperbole

$$x^2 - y^2 = a^2.$$

Rešitev. Tvorimo premice skozi točko $(-a, 0)$, kjer je parameter t strmina slednje. Velja $y = t(x + a)$ ter $x^2 - y^2 - a^2 = 0$.

$$x^2 - t^2(x+a)^2 = a^2$$
$$(x+a)\left(x - a - t^2(x+a)\right) = 0$$
$$x = a\frac{1+t^2}{1-t^2}$$

kjer smo pri faktorizaciji ponovno opazili ničlo $x = -a$ iz geometrijske strukture problema. Racionalna parametrizacija je tako

$$t \mapsto \left(a\frac{1+t^2}{1-t^2}, a\frac{-2t}{1-t^2}\right).$$

□

Primer 1.12

V $\mathbb{R}^2$ parametriziraj Descartesov list $x^3 + y^3 - 3xy = 0$.

Rešitev. Premice skozi $(0, 0)$ so oblike $y = tx$.

$$x^3 + t^3x^3 - 3tx^2 = 0$$
$$x^2\left(x + tx - 3t\right) = 0$$
$$x = \frac{3t}{1+t^3}$$

Racionalna parametrizacija je tako:

$$t \mapsto \left(\frac{3t}{1+t^3}, \frac{3t^2}{1+t^3}\right)$$

□

Zgornji postopek je posplošljiv, če na krivulji obstaja točka, za katero velja, da vse premice skozi to točko sekajo krivuljo v natanko eni drugi točki. Očitno so množice ničel polinomov stopnje največ 2 ustrezne. Descartesov list pa smo lahko parametrizirali, saj smo izbrali točko $(0, 0)$, ki ni gladka - krivulja tam nima polnega ranka.

1.2.2 Nerazcepnost

Trditev 1.13

Kolobar $\mathbb{C}[X, Y]$ ima enolično faktorizacijo. To pomeni, da lahko zapišemo

$$f = f_1^{k_1} \cdot \ldots \cdot f_n^{k_n}.$$

Dokaz. $\mathbb{C}[X, Y]$ ni evklidski kolobar, saj ideal $\langle x, y\rangle$ ni glavni. Enolično faktorizacijo pokažemo z minimalnim protiprimerom na stopnji nerazcepnih faktorjev. □

Definicija 1.14

Naj bo I aditivna podgrupa kolobarja K. Množici I pravimo *ideal*, če $\forall a \in K$ velja

$$aI = Ia = I.$$

Trditev 1.15

Če sta I, J ideala kolobarja K so ideali tudi

- $I + J = \{i + j \mid i \in I \wedge j \in J\}$
- $I \cap J$
- $IJ =$ aditivna podgrupa generirana z $\langle ij \mid i \in I \wedge j \in J\rangle$.

Trditev 1.16: Klasifikacija maksimalnih idealov

Maksimalni ideali naslednjih kolobarjev so:

- V $\mathbb{C}[X]$ so vsi maksimalni ideali oblike $\langle x - t\rangle$,
- V $\mathbb{C}[X, Y]$ so vsi maksimalni ideali oblike $\langle x - a, y - b\rangle$.

Kaj geometrijsko predstavljajo maksimalni ideali? Maksimalni ideali v $\mathbb{C}[X]$ so v bijekciji z $\mathbb{C}$ ter analogno z maksimalnimi ideali $\mathbb{C}[X, Y]$ ter $\mathbb{C}^2$. Ta korespondenca je splošnejša - velja tudi za "algebraične mnogoterosti".

Definicija 1.17

Ideal I je *praideal*, če iz $ab \in I$ sledi, da je $a \in I$ ali $b \in I$.

Trditev 1.18

V kolobarjih z enolično faktorizacijo praelementi ter nerazcepni elementi sovpadajo.

Obstaja naslednja korespondenca med algebro in geometrijo:

$$\begin{gathered} \mathbb{A}^2 \longleftrightarrow \mathbb{C}[X, Y] \\ \text{točke } (a, b) \longleftrightarrow \text{maksimalni ideali } (x - a, y - b) \\ \text{nerazcepne krivulje} \longleftrightarrow \text{praideali} \end{gathered}$$

V luči tega podamo naslednji kriterij:

Izrek 1.19: Eisensteinov kriterij

Naj bo

$$Q(X) = \sum_{i=1}^{m} a_i X^i,$$

kjer so $a_i \in \mathbb{C}[Y]$. Polinom $Q \in \mathbb{C}[X,Y]$ je *nerazcepen*, če obstaja tak nerazcepen polinom $p \in \mathbb{C}[Y]$ (kot posledica osnovnega izreka algebre je $p(Y) = Y - \alpha$, $\alpha \in \mathbb{C}$), da velja

$$\begin{gathered} a_i \in \langle p \rangle \quad \forall i \neq m \\ a_m \notin \langle p \rangle \\ a_0 \notin \langle p^2 \rangle \end{gathered}$$

Primer 1.20

$Q = x^2y - y^2x + x + y - 1 = (y)x^2 + (1-y^2)x + (y-1).$

Oris dokaza. $p(y) = y - 1$ □

Namesto, da opazujemo Q kot polinom nad $\mathbb{C}[Y]$ ga lahko opazujemo tudi kot polinom nad $\mathbb{C}[X]$, kar lahko vodi do dodatne uporabe Eisensteinovega izreka.

Za dokazovanje nevsebovanosti polinoma v idealu uporabimo protislovje s stopnjo polinoma ali pa protislovje s stopnjo ničle polinoma.

V primeru, da Eisensteinov kriterij ne pokaže nerazcepnosti pa gremo po definiciji, upoštevajoč lastnosti modula polinomov nad kolobarjem.

Druga možnost je, da pokažemo, da je kolobar $\mathbb{C}[X,Y]/\langle y^2 - x^3 \rangle$ cel.

Primer 1.21

Pokaži, da je polinom $y^2 - x^3$ nerazcepen.

Rešitev. Upamo, da je

$$\mathbb{C}[X,Y]/\langle y^2 - x^3 \rangle \cong \mathbb{C}[t^2, t^3] \subseteq \mathbb{C}[t].$$

$\varphi : p(x,y) \mapsto p(t^2, t^3)$ je ustrezen homomorfizem. □

1.2.3 Projektivnost

Primer 1.22

$C = V(y^2 - x^2 + x^4)$. Poiščite presečno večkratnost v izhodišču množice C s poljubno premico skozi izhodišče.

Rešitev. Premice skozi izhodišče so $y = tx$. Dobimo

$$0 = t^2x^2 - x^2 + x^4 = x^2(t^2 - 1 + x^2).$$

Sledi, da je za $|t| \neq 1$ presečna večkratnost 2, v primeru $t \in \{-1, 1\}$ pa je presečna večkratnost 4. $\square$

Ideja presečne večkratnosti je to, da lahko identificiramo tangente glede na to, da je presečna večkratnost več kot 1.

Definiramo $\mathbb{P}^2 = \mathbb{C}^3/$, kjer je ekvivalenčna relacija ležanja na isti premici. Točke v $\mathbb{P}^2$ so premice, ki potekajo skozi izhodišče v $\mathbb{C}^3$. Naj bo Φ obrnljiva linearna preslikava v $\mathbb{C}^3$. Φ slika premice, ki potekajo skozi izhodišče v druge premice skozi izhodišče. Tako Φ porodi bijekcijo iz $\mathbb{P}^2$ v $\mathbb{P}^2$, ki ji rečemo *projektivnost*.

Primer 1.23

Poišči projektivnost, ki preslika točke iz $\mathbb{P}^2$ v $\mathbb{P}^2$, ter

$$\begin{gathered}(1 : 1 : 0) \mapsto (0 : -1 : 0)\\ (1 : 0 : 1) \mapsto (1 : 0 : -2)\\ (1 : -1 : 0) \mapsto (1 : 1 : 0)\\ (1 : 0 : -1) \mapsto (1 : 0 : -1)\end{gathered}$$

Rešitev. Naj bo

$$A = \begin{vmatrix} 1 & 1 & 1 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{vmatrix}$$

ter

$$B = \begin{vmatrix} 0 & 1 & 1 \\ -1 & 0 & 1 \\ 0 & -2 & 0 \end{vmatrix}.$$

Iščemo $X \in \mathbb{C}^{3\times 3}$, da je $X \cdot A = B$. Prevedemo problem na $A^T \cdot X = B^T$ ter tvorimo matriko $[A^T \mid B^T]$ ter delamo Gaussovo eliminacijo, da dobimo X.

Ko gledamo, če se matrika X na želen način obnaša pri četrti vrednosti opazimo, da to ne velja. Ker so projektivne točke definirane do konstantega večkratnika natančno pravzaprav rešujemo sistem $X \cdot A = C$, kjer je

$$C = \begin{vmatrix} 0 & b & c \\ -a & 0 & c \\ 0 & -2b & 0 \end{vmatrix}$$

$\square$

Literatura

[1] prof. dr. Jaka Cimprič. *Predavanja iz predmeta Algebraične krivulje*. 2025.

[2] asist. dr. Matej Filip. *Vaje iz predmeta Algebraične krivulje*. 2025.