Algebra

Ivan Prokić

Fakultet tehničkih nauka, Novi Sad

Predavanje 14

Na prethodnom času

- Malo istorije: polinomi 5. i većeg stepena ne mogu da se reše pomoću radikala
- Polinomske funkcije: nad beskonačnim i konačnim poljima
- Bezuov stav
- Koreni i faktorizacija

Svodljivost i nesvodljivost polinoma

Svodljivost i nesvodljivost polinoma

Podsećanje: Prirodan broj je **složen** ako je jednak proizvodu dva prirodna broja manja od njega. Broj je **prost** ako deljiv samo sa samim sobom i sa 1. Broj 1 nije ni prost ni složen.

Definicija (Svodljivi polinomi)

Polinom $P \in F[t]$ je svodljiv nad poljem F akko je jednak proizvodu dva polinoma stepena nižih od njegovog.

Definicija (Nesvodljivi polinomi)

Polinom $P \in F[t]$ je nesvodiljiv nad poljem F ako je stepena većeg od nule i ako nije svodljiv, tj. ako nije deljiv polinomom stepena većeg od nule a manjeg od njegovog stepena.

Napomena (Konstante nisu ni svodljive ni nesvodljive)

Nula polinom i polinomi stepena nula nisu ni svodljivi ni nesvodljivi.

Svodljivost polinoma drugog i trećeg stepena

Teorema

Ako je $P \in F[t]$ polinom drugog ili trećeg stepena, tada je P svodljiv akko ima koren u polju F.

Dokaz

$(\Rightarrow)$: *Neka je P svodljiv, tj. $P = Q \cdot R$, gde je $dg(Q) \geq 1$ i $dg(R) \geq 1$. Ako je $dg(P) = 2$ onda $dg(Q) = dg(R) = 1$, a ako je $dg(P) = 3$ tada jedan od polinoma Q i R mora biti stepena 1, a drugi stepena 2. Tvrđenje sledi jer polinom prvog stepena $at + b$ u svako polju ima koren $-a^{-1}b$.*

$(\Leftarrow)$: *Neka je P polinom stepena 2 ili 3 i neka je α njegov koren u polju F. Iz Bezuove teoreme tada imamo $(t - \alpha) \mid P$, tj. P je svodljiv.*

Primeri. Svodljivost i koreni

- Polinom prvog stepena $at + b$, sa $a \neq 0$, je nesvodljiv nad svakim poljem
- Polinom $P = t^2 - 2$ je
  - svodljiv nad poljima $\mathbb{R}$ i $\mathbb{C}$ jer se može zapisati kao $(t - \sqrt{2})(t + \sqrt{2})$
  - nesvodljiv nad poljem $\mathbb{Q}$ (nema koren)
  - nesvodljiv nad $\mathbb{Z}_3$, jer je $t^2 - 2 = t^2 + 1$ i $P(0) = 1, P(1) = 2, P(2) = 2$ (nema koren)
- Polinom $P = t^2 + 1$ je
  - svodljiv nad poljem $\mathbb{C}$ jer se može zapisati kao $(t - i)(t + i)$
  - nesvodljiv nad poljima $\mathbb{R}$ i $\mathbb{Q}$ (nema koren)
  - svodljiv nad $\mathbb{Z}_2$, jer je $P(1) = 0$, odnosno $t^2 + 1 = (t + 1)(t + 1)$

Napomena

- *Samo za polinome stepena* 2 *i* 3 *važi da ako su svodljivi onda moraju imati koren u polju. Na primer, polinom* $t^4 + t^2 + 1$ *je svodljiv nad svim poljima, jer je* $t^4 + t^2 + 1 = (t^2 + t + 1)(t^2 - t + 1)$*, a nema koren u, recimo,* $\mathbb{R}$ *i* $\mathbb{Q}$*.*
- *Za sve polinome stepena većeg od* 1 *važi da ako imaju koren onda su i svodljivi.*
- *Polinomi stepena* 1 *imaju koren u svakom polju a nesvodljivi su nad svakim poljem.*

Jedinstvenost faktorizacije za normalizovane polinome

Podsećanje: Svaki prirodan broj se na jedinstven način može napisati kao proizvod (faktorisati) njegovih prostih faktora, ako redosled faktora nije bitan. Kod brojeva kao faktor ne uzimamo u obzir 1, a kod polinoma konstante.

Teorema

Neka je polinom $P \in F[t]$ svodljiv. Tada se P može na jedinstven način napisati kao proizvod svojih nesvodljivih normalizovanih faktora i jedne konstante iz F, ako redosled faktora nije bitan.

Primer

Nad poljem $\mathbb{R}$ imamo da je
$2t^2 - 2 = 2(t+1)(t-1) = (2t+2)(t-1) = (t+1)(2t-2) = (\frac{t}{2} + \frac{1}{2})(4t-4)$. *Ako u obzir uzimamo samo normalizovane nesvodljive faktore imamo*
$2t^2 - 2 = 2(t+1)(t-1)$.

Koreni i svodljivost nad $\mathbb{Q}, \mathbb{R}$ i $\mathbb{C}$

Koreni polinoma nad $\mathbb{C}$

Gaus je krajem *XIX* veka dokazao sledeću teoremu (koju mi dajemo bez dokaza).

Teorema (Osnovni stav algebre)

Svaki polinom stepena većeg od nule nad poljem kompleksnih brojeva ima bar jedan koren u tom polju.

Posledica

Ako je $P \in \mathbb{C}[t]$ *i* $P = a_n t^n + a_{n-1} t^{n-1} + \ldots + a_1 t + a_0$, *za* $n > 0$, *tada postoje* $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ *takvi da je*

$$P = a_n(t - \alpha_1)(t - \alpha_2)\ldots(t - \alpha_n)$$

Dokaz

Imamo da je $P = a_n P_n$, *gde je* P_n *normalizovan polinom stepena* n. *Na osnovu prethodne teoreme, znamo da* P_n *ima jedan koren u* $\alpha_n \in \mathbb{C}$, *pa iz Bezuovog stava sledi* $P = a_n(t - \alpha_n)P_{n-1}$, *gde je* P_{n-1} *normalizovan polinom stepena* $n - 1$. *Ako sada primenimo prethodnu teoremu na* P_{n-1} *i postupak ponovimo još* $n - 2$ *puta, dobijamo* $P = a_n(t - \alpha_n)\ldots(t - \alpha_1)$.

Kompleksni koreni

Napomena

- *Niti teorema niti posledica ne govore ništa o tome kako naći kompleksne korene, samo kažu da postoje*
- *Iz prethodnih rezultata sledi da je svaki polinom stepena većeg od* 1 *nad poljem kompleksnih brojeva svodljiv*

Napomena

- *Za kvadratni polinom* $at^2 + bt + c$ *znamo da su koreni* $\frac{-b \pm \sqrt{b^2-4ac}}{2a}$, *odakle sledi da ako su* $a, b, c \in \mathbb{R}$ *i ako je neki kompleksni broj* $\alpha \in \mathbb{C} \setminus \mathbb{R}$ *koren polinoma (diskriminanta je manja od nule) tada je njegov konjugovani* $\overline{\alpha}$ *takođe koren tog polinoma*
- *Sledeća teorema kaže da ovo važi za sve nekonstantne polinome sa realnim koeficijentima*

Konjugovano kompleksni koreni realnih polinoma

Teorema

Neka je $P \in \mathbb{C}[t]$ i $P = a_n t^n + a_{n-1} t^{n-1} + \ldots + a_1 t + a_0$, za $n > 0$ i $\alpha \in \mathbb{C}$ koren polinoma P. Ako su koeficijenti polinoma P realni brojevi, tj. $a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{R}$, tada je i $\overline{\alpha}$ koren polinoma P.

Dokaz

Pošto je polje $\mathbb{C}$ beskonačno, umesto $\psi(P)$ pisaćemo samo P. Na osnovu prethodnih teorema sledi $P(x) = a_n(x - \alpha_1) \ldots (x - \alpha_n)$, te iz $a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{R}$ imamo $\overline{P(x)} = a_n \overline{x}^n + a_{n-1} \overline{x}^{n-1} + \ldots + a_1 \overline{x} + a_0 = P(\overline{x}) = a_n(\overline{x} - \alpha_1) \ldots (\overline{x} - \alpha_n)$. Sada dobijamo $P(x) = \overline{\overline{P(x)}} = \overline{a_n(\overline{x} - \alpha_1) \ldots (\overline{x} - \alpha_n)} = a_n(x - \overline{\alpha_1}) \ldots (x - \overline{\alpha_n})$. Dakle, ako su $\alpha_1, \ldots, \alpha_n$ koreni polinoma P onda su to i $\overline{\alpha_1}, \ldots, \overline{\alpha_n}$.

Faktorizacija realnih polinoma

Napomena

Primetimo da za sve $\alpha \in \mathbb{C}$ važi
$(t-\alpha)(t-\overline{\alpha}) = t^2 - (\alpha+\overline{\alpha})t + \alpha\overline{\alpha} = t^2 - 2Re(\alpha)t + |\alpha|^2$, *te da je ovo polinom sa realnim koeficijentima jer su $Re(\alpha)$ i $|\alpha|$ realni brojevi.*

Teorema

Ako je $P \in \mathbb{R}[t]$ i $dg(P) > 1$ tada se P nad poljem $\mathbb{R}$ može zapisati kao proizvod linearnih i kvadratnih polinoma (i konstante).

Dokaz

Pošto je $\mathbb{R} \subset \mathbb{C}$, znamo da je
$P = a_n t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0 = a_n(x-\alpha_1)\ldots(x-\alpha_n)$, *gde su* $\alpha_1, \ldots, a_n \in \mathbb{C}$. *Ako je $\alpha_i \in \mathbb{R}$ onda je $t - \alpha_i$ linearni polinom sa realnim koeficijentima. Ako je $\alpha_i \in \mathbb{C}\backslash\mathbb{R}$ onda je $\overline{\alpha_i} = \alpha_j$ za neko $j \neq i$, pa je na osnovu prethodne napomene $(t-\alpha_i)(t-\alpha_j)$ kvadratni polinom sa realnim koeficijentima.*

Svodljivost i koreni polinoma nad $\mathbb{R}$

Posledica

Ako je $P \in \mathbb{R}[t]$ *i* $dg(P) \geq 3$ *tada je* P *svodljiv.*

Primer

- *Ako je* $f \in \mathbb{R}[x]$ *i* $f(e^{i\alpha}) = 0$, *za* $\alpha \in \mathbb{R} \setminus \{k\pi \mid k \in \mathbb{Z}\}$ *tada je*
  - $x - e^{i\alpha} \mid f(x)$
  - $x - e^{-i\alpha} \mid f(x)$ *(Konjugovani koren)*
  - $(x^2 - 2x\cos\alpha + 1) \mid f(x)$ *(Prozivod prethodna dva)*
- *Ako je* $f \in \mathbb{R}[x]$ *i* $f(e^{i\alpha}) = 0$, *za* $\alpha \in \mathbb{R}$ *tada je*
  - $x - e^{i\alpha} \mid f(x)$
  - $x - e^{-i\alpha} \mid f(x)$
  - *ali* $(x^2 - 2x\cos\alpha + 1) \mid f(x)$ *ne mora da važi. Npr. za* $\alpha = 0$ *iz* $f(1) = 0$ *ne možemo zaključiti da* $(x^2 - 2x + 1) \mid f(x)$

Potencijalni koreni polinoma nad $\mathbb{Q}$

Teorema

Neka je $S = a_n t^n + a_{n-1} t^{n-1} + \ldots + a_1 t + a_0$, gde su svi koeficijenti celi brojevi. Ako je racionalan broj $\frac{p}{q}$ koren polinoma S, gde su p i q uzajamno prosti celi brojevi, tada $p \mid a_0$ i $q \mid a_n$.

Dokaz

Ako je $\frac{p}{q}$ koren polinoma P tada važi $a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \ldots + a_1\left(\frac{p}{q}\right) + a_0 = 0$. Ako pomnožimo sa q^{n-1} dobijamo

$$a_n \frac{p^n}{q} + a_{n-1} p^{n-1} + \ldots + a_1 p q^{n-2} + a_0 q^{n-1} = 0$$

U ovoj jednakosti svi sabirci sem prvog su očigledno celi brojevi, pa zato i prvi sabirak $a_n \frac{p^n}{q}$ mora biti ceo broj, a pošto su p i q uzajamno prosti, sledi da $q \mid a_n$. Ako sada poslednju jednakost pomnožimo sa $\frac{q}{p}$ dobijamo

$$a_n p^{n-1} + a_{n-1} p^{n-2} q + \ldots + a_1 q^{n-1} + a_0 \frac{q^n}{p} = 0$$

Sada slično dobijamo da $p \mid a_0$.

Primer

Zaokruži oznaku polja nad kojima je polinom $P = t^3 + t + 1$ nesvodljiv

$\mathbb{Q}$ $\mathbb{R}$ $\mathbb{C}$ $\mathbb{Z}_2$ $\mathbb{Z}_3$ $\mathbb{Z}_5$ $\mathbb{Z}_7$

Primer

Zaokruži oznaku polja nad kojima je polinom $P = t^3 + t + 1$ nesvodljiv

$\mathbb{Q}$ $\mathbb{R}$ $\mathbb{C}$ $\mathbb{Z}_2$ $\mathbb{Z}_3$ $\mathbb{Z}_5$ $\mathbb{Z}_7$

$\mathbb{Q}$: Potencijalni racionalni koreni su oblika $\frac{p}{q}$ gde $p \mid 1$ i $q \mid 1$. Zato $\frac{p}{q} \in \{1, -1\}$, pa proverom dobijamo $P(1) \neq 0$ i $P(-1) \neq 0$.

Primer

Zaokruži oznaku polja nad kojima je polinom $P = t^3 + t + 1$ nesvodljiv

$\mathbb{Q}$ $\mathbb{R}$ $\mathbb{C}$ $\mathbb{Z}_2$ $\mathbb{Z}_3$ $\mathbb{Z}_5$ $\mathbb{Z}_7$

$\mathbb{Q}$: Potencijalni racionalni koreni su oblika $\frac{p}{q}$ gde $p \mid 1$ i $q \mid 1$. Zato $\frac{p}{q} \in \{1, -1\}$, pa proverom dobijamo $P(1) \neq 0$ i $P(-1) \neq 0$.

$\mathbb{R}$: Svodljiv jer je stepena većeg od 2

Primer

Zaokruži oznaku polja nad kojima je polinom $P = t^3 + t + 1$ nesvodljiv

$\mathbb{Q}$ $\mathbb{R}$ $\mathbb{C}$ $\mathbb{Z}_2$ $\mathbb{Z}_3$ $\mathbb{Z}_5$ $\mathbb{Z}_7$

$\mathbb{Q}$: Potencijalni racionalni koreni su oblika $\frac{p}{q}$ gde $p \mid 1$ i $q \mid 1$. Zato $\frac{p}{q} \in \{1, -1\}$, pa proverom dobijamo $P(1) \neq 0$ i $P(-1) \neq 0$.

$\mathbb{R}$: Svodljiv jer je stepena većeg od 2

$\mathbb{C}$: Svodljiv jer je stepena većeg od 1

Primer

Zaokruži oznaku polja nad kojima je polinom $P = t^3 + t + 1$ nesvodljiv

$\mathbb{Q}$ $\quad$ $\mathbb{R}$ $\quad$ $\mathbb{C}$ $\quad$ $\mathbb{Z}_2$ $\quad$ $\mathbb{Z}_3$ $\quad$ $\mathbb{Z}_5$ $\quad$ $\mathbb{Z}_7$

$\mathbb{Q}$: Potencijalni racionalni koreni su oblika $\frac{p}{q}$ gde $p \mid 1$ i $q \mid 1$. Zato $\frac{p}{q} \in \{1, -1\}$, pa proverom dobijamo $P(1) \neq 0$ i $P(-1) \neq 0$.

$\mathbb{R}$: Svodljiv jer je stepena većeg od 2

$\mathbb{C}$: Svodljiv jer je stepena većeg od 1

$\mathbb{Z}_2$: Nesvodljiv jer je $P(0) = 1, P(1) = 1$

Primer

Zaokruži oznaku polja nad kojima je polinom $P = t^3 + t + 1$ nesvodljiv

$\mathbb{Q}$ $\quad$ $\mathbb{R}$ $\quad$ $\mathbb{C}$ $\quad$ $\mathbb{Z}_2$ $\quad$ $\mathbb{Z}_3$ $\quad$ $\mathbb{Z}_5$ $\quad$ $\mathbb{Z}_7$

$\mathbb{Q}$: Potencijalni racionalni koreni su oblika $\frac{p}{q}$ gde $p \mid 1$ i $q \mid 1$. Zato $\frac{p}{q} \in \{1, -1\}$, pa proverom dobijamo $P(1) \neq 0$ i $P(-1) \neq 0$.

$\mathbb{R}$: Svodljiv jer je stepena većeg od 2

$\mathbb{C}$: Svodljiv jer je stepena većeg od 1

$\mathbb{Z}_2$: Nesvodljiv jer je $P(0) = 1, P(1) = 1$

$\mathbb{Z}_3$: Svodljiv jer je $P(1) = 0$, odakle je $t^3 + t + 1 = (t + 2)(t^2 + t + 2)$

Primer

Zaokruži oznaku polja nad kojima je polinom $P = t^3 + t + 1$ nesvodljiv

$\mathbb{Q}$ $\quad$ $\mathbb{R}$ $\quad$ $\mathbb{C}$ $\quad$ $\mathbb{Z}_2$ $\quad$ $\mathbb{Z}_3$ $\quad$ $\mathbb{Z}_5$ $\quad$ $\mathbb{Z}_7$

$\mathbb{Q}$: Potencijalni racionalni koreni su oblika $\frac{p}{q}$ gde $p \mid 1$ i $q \mid 1$. Zato $\frac{p}{q} \in \{1, -1\}$, pa proverom dobijamo $P(1) \neq 0$ i $P(-1) \neq 0$.

$\mathbb{R}$: Svodljiv jer je stepena većeg od 2

$\mathbb{C}$: Svodljiv jer je stepena većeg od 1

$\mathbb{Z}_2$: Nesvodljiv jer je $P(0) = 1, P(1) = 1$

$\mathbb{Z}_3$: Svodljiv jer je $P(1) = 0$, odakle je $t^3 + t + 1 = (t + 2)(t^2 + t + 2)$

$\mathbb{Z}_5$: Nesvodljiv jer je $P(0) = 1, P(1) = 3, P(2) = 1, P(3) = 1, P(4) = 4$

Primer

Zaokruži oznaku polja nad kojima je polinom $P = t^3 + t + 1$ nesvodljiv

$\mathbb{Q}$ $\quad$ $\mathbb{R}$ $\quad$ $\mathbb{C}$ $\quad$ $\mathbb{Z}_2$ $\quad$ $\mathbb{Z}_3$ $\quad$ $\mathbb{Z}_5$ $\quad$ $\mathbb{Z}_7$

$\mathbb{Q}$: Potencijalni racionalni koreni su oblika $\frac{p}{q}$ gde $p \mid 1$ i $q \mid 1$. Zato $\frac{p}{q} \in \{1, -1\}$, pa proverom dobijamo $P(1) \neq 0$ i $P(-1) \neq 0$.

$\mathbb{R}$: Svodljiv jer je stepena većeg od 2

$\mathbb{C}$: Svodljiv jer je stepena većeg od 1

$\mathbb{Z}_2$: Nesvodljiv jer je $P(0) = 1, P(1) = 1$

$\mathbb{Z}_3$: Svodljiv jer je $P(1) = 0$, odakle je $t^3 + t + 1 = (t + 2)(t^2 + t + 2)$

$\mathbb{Z}_5$: Nesvodljiv jer je $P(0) = 1, P(1) = 3, P(2) = 1, P(3) = 1, P(4) = 4$

$\mathbb{Z}_7$: Nesvodljiv jer je
$P(0) = 1, P(1) = 3, P(2) = 4, P(3) = 3, P(4) = 6, P(5) = 5, P(6) = 6$

Višestruki koreni polinoma nad $\mathbb{C}$

Podsećanje: Polinom n-tog stepena nad $\mathbb{C}$ ima n korena. Neki od tih korena se mogu ponavljati - višestruki koreni.

Teorema

Neka su $P, Q \in \mathbb{C}$. Ako svaki koren od P, višestrukosti k, jeste i koren polinoma Q, višestrukosti veće ili jednake od k, tada polinom P deli polinom Q.

Napomena: Traženje višestrukih korena može se uraditi deljenjem (ili Hornerovom šemom). Za polinome sa realnim koeficijentima može i pomoću izvoda polinomske funkcije $\psi(P)(x)$.

Teorema

Koren α reda $k > 2$ polinoma P sa realnim koeficijentima jeste koren reda $k-1$ polinoma P', a takođe je i zajednički koren polinoma $P, P', P'', \ldots, P^{(k-1)}$ i nije koren polinoma $P^{(k)}$.

Dokaz

Direktna posledica činjenice da je $P(x) = (x-\alpha)^k Q(x)$, gde α nije koren polinoma $Q(x)$, i $P'(x) = (x-\alpha)^{k-1}\big(kQ(x) + (x-\alpha)Q'(x)\big)$.

Vijetove formule

Vijetove formule

Za polinom drugog stepena $P = at^2 + bt + c$ nad prozivoljnim poljem imamo da ako su mu koreni t_1 i t_2 tada je $at^2 + bt + c = a(t - t_1)(t - t_2) = at^2 - a(t_1 + t_2)t + at_1t_2$, odakle dobijamo Vijetove formule: $t_1 + t_2 = -\frac{b}{a}$ i $t_1 t_2 = \frac{c}{a}$. Ovaj rezultat može se uopštiti na polinome proizvoljnog stepena većeg od 2.

Teorema

Neka je $P = a_n t^n + a_{n-1} t^{n-1} + \ldots + a_1 t + a_0 \in F[t]$ *i neka su* $t_1, t_2, \ldots, t_n$ *svi koreni polinoma* P *(koreni se mogu ponavljati), tada važi*

$$t_1 + t_2 + \ldots + t_n = -\frac{a_{n-1}}{a_n}$$

$$t_1 t_2 + t_1 t_3 + \ldots + t_{n-1} t_n = \frac{a_{n-2}}{a_n}$$

$$\vdots$$

$$t_1 t_2 \ldots t_n = (-1)^n \frac{a_1}{a_n}$$

Primer

Neka je $f(x) = x^3 + ax^2 + bx + c$ polinom nad poljem $\mathbb{R}$ i neka je skup svih njegovih korena $\{1, 2\}$. Odrediti sve moguće vrednosti za a, b i c.
Rešenje. Vijetove formule za $f(x) = x^3 + ax^2 + bx + c$ glase

$$\begin{aligned} x_1 + x_2 + x_3 &= -a \\ x_1x_2 + x_1x_3 + x_2x_3 &= b \\ x_1x_2x_3 &= -c \end{aligned}$$

S obzirom da su koreni 1 i 2 imamo dve mogućnosti:

- Dvostruki koren je 1. Tada je $a = -4, b = 5, c = -2$.
- Dvostruki koren je 2. Tada je $a = -5, b = 8, c = -4$.

Šta smo danas radili

- Svodljivost i nesvodljivost
- Osnovni stav algebre i faktorizacija nad $\mathbb{C}$, $\mathbb{R}$ i $\mathbb{Q}$
- Vijetove formule