Talvine õppesessioon (eliitrühm)

Polünoomide algebra
Aleksei Ganyukov

20. detsember 2025

1 Polünoomidest teooriat

Ühe muutuja polünoomi üldine kuju on $P(x) = a_n x^n + \cdots + a_1 x + a_0$, kus $a_n, \ldots, a_0$ nimetatakse *kordajateks*. Polünoomi $P \in \mathbb{C}[X]$ kordajad on kompleksarvud, aga polünoomide $Q \in \mathbb{R}[X]$, $R \in \mathbb{Q}[X]$, ning $S \in \mathbb{Z}[X]$ kordajad on vastavalt reaal-, ratsionaal- ja täisarvud. Selles materjalis me tähistame ka $\mathbb{N} = \mathbb{Z}^+$, $\mathbb{R}_{>0} = \mathbb{R}^+$ ja $\mathbb{R}_{\geq 0} = \mathbb{R}^+ \cup \{0\}$. Kui '$X$' ei kasutata, siis tähistatakse arvude hulka, mitte polünoomide hulka.

Liiget $a_n x^n$ nimetatakse *pealiikmeks* ning a_0 on *vabaliige*. Polünoomi, millel $a_n = 1$, nimetatakse *unitaarseks* polünoomiks. Polünoomi P *aste* $\deg(P)$ on suurim indeks n, mille korral $a_n \neq 0$. Arvu z nimetatakse polünoomi P *juureks* (või nullkohaks), kui $P(z) = 0$.

Teoreem 1 (Algebra põhiteoreem)**.** $n \geq 1$ astme polünoomil on täpselt n kompleksarvulist juurt, arvestades kordsust (ülimalt n reaalarvulist juurt).

Rääkides, et võrrandil on n lahendit, peetakse tavaliselt silmas, et lahendid on erinevad; polünoomil võivad siiski olla kordsed juured.

Polünoomide jaguvus on sarnane täisarvude jaguvusega. Kui P ja Q on polünoomid ning $\deg(Q) > 0$, siis leiduvad polünoomid A, R nii, et $P(x) = A(x)Q(x) + R(x)$ ja $\deg(R) < \deg(Q)$. Kui $R(x) = 0$, ütleme, et $Q(x)$ jagab $P(x)$, ning kirjutame $Q(x) \mid P(x)$ (või $Q \mid P$). Samas kuuluvad A ja R samasse ringi nagu P ja Q (nt $\mathbb{Z}[X]$, $\mathbb{R}[X]$ jne).

Fakt 1.1. Kui a on $P(x)$ juur, siis $x - a \mid P(x)$.

Fakt 1.2. Kui $x_1, \ldots, x_n$ on polünoomi $P(x)$ juured ning a_n on pealiikme kordaja, siis $P(x) = a_n(x-x_1)\cdots(x-x_n)$.

Oluline omadus $x - a \mid P(x) - P(a)$ kandub täisarvude jagatavuselt üle ka polünoomidele: siin võivad x ja a olla nii konstandid kui ka muutujad (isegi polünoomid). Seega leidub mingi $Q \in \mathbb{R}[X]$ nii, et $P(x) - P(a) = (x-a)Q(x)$.

Lause 1.3 (Lagrange'i interpolatsioonipolünoom)**.** Olgu antud $n+1$ erinevat punkti (x_i, y_i), $i = 0, 1, \ldots, n$, kusjuures $x_i \neq x_j$ kõigi $i \neq j$ korral. Siis leidub täpselt üks ülimalt n astme polünoom $P(x)$, mis läbib kõiki neid punkte. See on antud valemiga

$$P(x) = \sum_{i=0}^{n} y_i \frac{\prod\limits_{\substack{k=0 \\ k\neq i}}^{n} (x - x_k)}{\prod\limits_{\substack{k=0 \\ k\neq i}}^{n} (x_i - x_k)}.$$

Järeldus 1.4. Kui $P \in \mathbb{R}[X]$ on astmega $\leq n$ ning võtab täisarvulistes/ratsionaalarvulistes punktides $n+1$ täisarvulist/ratsionaalarvulist väärtust, siis $P \in \mathbb{Q}[X]$. Märkus: täisarvulised punktid-väärtused tagavad ratsionaalarvulisuse, kuid ei taga tingimata täisarvulisi kordajaid.

Kui A ja B on n-astme polünoomid ning võrdus $A(x) = B(x)$ kehtib vähemalt $n+1$ erineva x väärtuse korral, siis $C(x) \coloneqq A(x) - B(x)$ on nullpolünoom ja seega $A(x) \equiv B(x)$ (st polünoomide A ja B kõik kordajad ja juured on samad).

Polünoomi P tuletis on $P'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1$. Tuletise nullkohad vastavad P lokaalsele ekstreemumile. Polünoomi kordne juur on alati ka P' juur, ning kui $x_1, x_2 \in \mathbb{R}$ on P juured, $x_1 < x_2$, siis leidub $x_3 \in (x_1, x_2)$ nii, et $P'(x_3) = 0$ (Rolle'i teoreem). Kui $a < b$ ja $P(a) < P(b)$, siis leiduvad $c \in (a, b)$ ja $d \in (a, b)$ nii, et $P(a) < P(c) < P(b)$ ning $P'(d) = \frac{P(b)-P(a)}{b-a}$ (keskväärtusteoreem).

(Cauchy–Schwarzi võrratus) Olgu $a_1, \ldots, a_n$ ja $b_1, \ldots, b_n$ reaalarvud, siis

$$(a_1^2 + \cdots + a_n^2)(b_1^2 + \cdots + b_n^2) \geq (a_1 b_1 + \cdots + a_n b_n)^2.$$

2 Ülesanded

Osa 1

1. (Folkloor) Olgu $P \in \mathbb{R}_{>0}[X]$. Tõesta, et kui tingimus $P\left(\frac{1}{x}\right) \geq \frac{1}{P(x)}$ kehtib $x = 1$ korral, siis see kehtib iga $x > 0$ korral. (Vihje: C-S)

2. (AOPS) Iseloomusta kõik $P \in \mathbb{R}_{\geq 0}[X]$, mille korral $P(0) = 0$, $P(1) = 1$ ja $P(x) \geq x^{2025}$ iga $x \geq 0$ korral.

3. (Valgevene) Polünoomi $P \in \mathbb{R}[X]$, $P(x) = a_{2n}x^{2n} + a_{2n-1}x^{2n-1} + \ldots + a_1x + a_0$ juured pole reaalarvud. Tõesta, et järgmise polünoomi juured pole ka reaalavud:

$$Q(x) = a_{2n}x^{2n} + a_{2n-2}x^{2n-2} + \ldots + a_2x^2 + a_0.$$

4. (Poola) Olgu $P, Q \in \mathbb{R}[X]$, $P \not\equiv Q$, ning $P(Q(x)) \equiv Q(P(x))$. Tõesta, et iga $n \in \mathbb{N}$ korral jagab polünoom $P(x) - Q(x)$ polünoomi

$$\underbrace{P(P(\ldots P(P}_{n}(x))\ldots)) - \underbrace{Q(Q(\ldots Q(Q}_{n}(x))\ldots)).$$

5. Ütleme, et $S(x) \in \mathbb{R}[X]$ on *kena*, kui $x||S(x)$, s.t. $x \mid S(x)$, kuid $x^2 \nmid S(x)$. Antud on $P \in \mathbb{R}[X]$ ning on teada, et leidub kena $Q \in \mathbb{R}[X]$ nii, et $x^2 \mid P(Q(x)) - Q(2x)$. Tõesta, et leidub kena polünoom $R \in \mathbb{R}[X]$ nii, et $P(R(x)) - R(2x)$ jagub x^{67}-ga.

6. (AOPS) Olgu $P \in \mathbb{Z}[X]$, $P \not\equiv 0$ ning $P(r) = P(s) = 0$ mingite täisarvude $0 < r < s$ korral. Tõesta, et leidub $k \geq 0$ nii, et $a_k \leq -s$.

Osa 2

7. (Folkloor) Olgu $P \in \mathbb{R}[X]$ unitaarne ning $\deg P = n$. Tõesta, et leidub $k \in \{0, 1, \ldots, n\}$ nii, et $|P(k)| \geq \frac{n!}{2^n}$.

8. Olgu $n \geq 2$ ja reaalarvud $x_1 < x_2 < \cdots < x_n$. Defineerime funktsiooni $f : \mathbb{R} \to \mathbb{R}$ valemiga

$$f(x) = \left|\frac{(x-x_2)(x-x_3)\cdots(x-x_n)}{(x_1-x_2)(x_1-x_3)\cdots(x_1-x_n)}\right| + \cdots + \left|\frac{(x-x_1)(x-x_2)\cdots(x-x_{n-1})}{(x_n-x_1)(x_n-x_2)\cdots(x_n-x_{n-1})}\right|.$$

Tõesta, et leidub $i \in \{1, 2, \cdots, n-1\}$ nii, et iga $x \in (x_i, x_{i+1})$ korral kehtib $f(x) < \sqrt{n}$. (Vihje: C-S)

9. (Šveits) Leia kõik unitaarsed $P \in \mathbb{Z}[X]$, mille korral kõigi $a, b \in \mathbb{Z}$ jaoks leidub $c \in \mathbb{Z}$ nii, et $P(a)P(b) = P(c)$.

10. Olgu $a, b \in \mathbb{R}$ ning defineerime hulgad $A = \{a^n \mid n \in \mathbb{N}\}$ ja $B = \{b^n \mid n \in \mathbb{N}\}$. Leia kõik $a, b > 1$, mille korral leiduvad kaks mittekonstantset polünoomi $P, Q \in \mathbb{R}[X]$, mille pealiikmete kordajad on positiivsed, nii et iga $r \in \mathbb{R}$ korral

$$P(r) \in A \iff Q(r) \in B.$$

11. (AOPS) Olgu n naturaalarv ning olgu $a_1, a_2, \ldots, a_n$ positiivsed reaalarvud. Vaatleme polünoomi

$$P(x) = (x-a_1)(x-a_2)\cdots(x-a_n) + (x+a_1)(x+a_2)\cdots(x+a_n).$$

Tõesta, et polünoomil P puuduvad kordsed juured üle $\mathbb{C}$.

12. Olgu $n \geq 2$. Aleksei ja vastasmängija mängivad kordamööda järgmist mängu. Igal käigul valib aktiivne mängija varem valimata indeksi $i \in \{0, \ldots, n\}$ ja nullist erineva $a_i \in \mathbb{Q}$; Aleksei alustab. Mäng lõpeb, kui kõik indeksid on valitud. Seejärel moodustatakse polünoom $P(x) = a_nx^n + \cdots + a_0$. Aleksei võidab, kui polünoomil P leidub ratsionaaljuur, ning vastasmängija püüab seda vältida. Leia kõik $n \geq 2$, mille korral Aleksei saab kindlasti võita sõltumata vastasmängija käikudest.

13. Olgu $P \in \mathbb{R}[X]$, $P \not\equiv 0$, ja $P(0) = 0$. Tõesta, et iga $M \in \mathbb{R}^+$ korral leidub $d \in \mathbb{Z}^+$ nii, et iga unitaarse $Q \in \mathbb{R}[X]$ korral, millel $\deg Q \geq d$, leidub ülimalt $\deg Q$ täisarvu k nii, et $|P(Q(k))| \leq M$.

14. Leia kõik $P \in \mathbb{R}[X, Y]$, mille korral kõigi $x, y > 2025$ korral kehtib

$$P(\{x\}, \{y\}) = \{P(x, y)\}.$$

15. (Bulgaaria) Kas leidub ühe muutuja reaalsete kordajatega polünoom P, nii et võrrandil $P(xy) = P(x)P(y)$ on täpselt 2025 järjestatud lahendit (x, y) $(x \leq y)$?

Kui pole öeldud teisiti, siis ülesande allikas on tõenäoliselt Iraani algebraeksam.