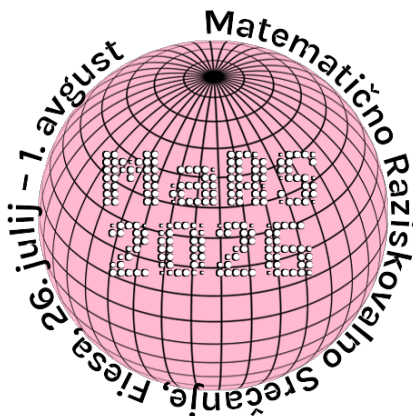


Simetrični polinomi

Katja Anzeljc, Lovro Kastelic, Živa Lenarčič

Mentor: Jure Kreže



Povzetek

V članku so obravnavani simetrični polinomi. Razložene so njihove lastnosti ter računske operacije. Definiran je pojem leksikografske urejenosti. Dokazan je osnovni izrek o simetričnih polinomih, ki pravi, da se vsak simetrični polinom lahko zapiše kot polinom v elementarnih simetričnih polinomih.

1 Uvod

Neverjetni svet števil in krivulj odpirajo polinomi v več spremenljivkah. Da ne prehitimo lastnih misli, obnovimo znanje polinomov v eni spremenljivki. Zapišemo jih kot formalno vsoto členov, ki so sestavljeni iz realnih koeficientov $a_0, a_1, a_2, \dots, a_n$ in formalne spremenljivke X , pri čemer velja $a_n \neq 0$. Definicija polinoma v eni spremenljivki z realnimi koeficienti f je

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0.$$

Množico polinomov v eni spremenljivki označimo z $\mathbb{R}[X]$. Oglejmo si polinome z več spremenljivkami. V njih poleg običajne X spremenljivke nastopajo tudi druge. Najprej definiramo polinome, ki imajo ob spremenljivki X še spremenljivko Y , potem pa posplošimo to definicijo na n spremenljivk. Množico polinomov z realnimi koeficienti v dveh spremenljivkah označimo z $\mathbb{R}[X, Y]$. Polinom z realnimi koeficienti v dveh spremenljivkah X in Y gledamo kot polinom v eni spremenljivki Y , ki ima za koeficiente polinome v spremenljivki X . Torej polinom $f \in \mathbb{R}[X, Y]$ lahko zapišemo kot

$$f(X, Y) = a_n(X)Y^n + \dots + a_1(X)Y + a_0,$$

pri čemer so koeficienti a_i polinomi z realnimi koeficienti v spremenljivki X . Podobno velja tudi za polinome z več spremenljivkami, namreč polinom f v spremenljivkah $X_1, \dots, X_n$ obravnavamo kot polinom v spremenljivki X_n , ki ima za koeficiente polinome v spremenljivkah $X_1, \dots, X_{n-1}$. Množico polinomov v n spremenljivkah označimo z $\mathbb{R}[X_1, \dots, X_n]$.

V članku definiramo leksikografsko urejenost, ki nam pomaga pri definiranju multistopenj in vzdolnih koeficientov polinomov več spremenljivk, ter se seznanimo z računskimi operacijami polinomov.

Spoznamo simetrične polinome, ki so posebna vrsta polinomov z več spremenljivkami. Definiramo elementarne simetrične polinome, ki so v določenem smislu osnovne gradbene enote simetričnih polinomov. Dokažemo osnovni izrek o simetričnih polinomih, ki pravi, da se lahko vsak simetrični polinom zapiše kot polinom v elementarnih simetričnih polinomih.

2 Leksikografska urejenost

2.1 Definicija

Označimo z $\mathbb{N}_0 = \mathbb{N} \cup \{0\} = \{0, 1, \dots\}$ množico nenegativnih celih števil. Z $\mathbb{N}_0^n$ označimo množico n -teric nenegativnih celih števil.

Primerjali bi radi dve n -terici nenegativnih celih števil $\mathbf{i} = (i_1, i_2, \dots, i_n)$ in $\mathbf{j} = (j_1, j_2, \dots, j_n)$, kjer so členi $i_t, j_t \in \mathbb{N}_0$. Pogost način urejanja n -teric¹ je leksikografska urejenost. Ta ureja števila podobno kot so urejene besede v slovarjih. Besede najprej razdelimo po prvih črkah glede na njihovo mesto v abecedi. Besede, ki se začnejo na isto črko, potem dalje razvrstimo glede na drugo črko, potem glede na tretjo in tako dalje, dokler se beseda ne konča. Leksikografsko urejanje enako poteka tudi pri n -tericah nenegativnih celih števil z razliko, da imamo namesto črk številke. Začnemo tako, da pogledamo števili na prvi koordinati obeh n -teric. Če se razlikujeta, n -terici primerjamo kot bi primerjali ti dve števili, torej če je število i_1 večje od števila j_1 , je tudi $\mathbf{i}$ večji od $\mathbf{j}$ in obratno. V primeru, da je število enako, pogledamo drugo koordinato, če velja $i_2 > j_2$, določimo $\mathbf{i} > \mathbf{j}$ in obratno. Ti dve števili potem že spet primerjamo, kot smo to storili za prvo koordinato. Če se tudi tukaj ne razlikujeta, se ponovno premaknemo na naslednje mesto. Postopek ponavljamo, dokler se števili ne razlikujeta oziroma dokler nam ne zmanjka mest. Če ugotovimo, da je $\mathbf{i}$ manjši od $\mathbf{j}$, to zapišemo kot $\mathbf{i} < \mathbf{j}$ oziroma $\mathbf{i} > \mathbf{j}$, če ugotovimo, da je $\mathbf{i}$ večji od $\mathbf{j}$. V nasprotnem primeru se zgodi, da so vse koordinate enake, potem sta tudi n -terici enaki, torej velja $\mathbf{i} = \mathbf{j}$. Če velja bodisi $\mathbf{i} < \mathbf{j}$ bodisi $\mathbf{i} = \mathbf{j}$, pišemo $\mathbf{i} \preceq \mathbf{j}$.

Za primer vzemimo 5-terici $\mathbf{i} = (1, 7, 3, 10, 5)$ in $\mathbf{j} = (1, 7, 6, 0, 2)$. Najprej pogledamo prvo koordinato, ta je pri obeh enaka številu 1. Števili na prvi koordinati sta enaki, zato pogledamo drugo koordinato, ki je v obeh 5-tericah enaka številu 7. Ker imamo dve enaki števili, pogledamo naslednjo koordinato. Na tretji koordinati ima $\mathbf{i}$ število 3, $\mathbf{j}$ pa število 6. Velja $3 < 6$, iz česar sledi $\mathbf{i} < \mathbf{j}$.

¹Mi primerjamo n -terice nenegativnih celih števil, enaka metoda pa deluje za primerjanje n -teric, ki vsebujejo druge matematične objekte, ki jih znamo med sabo primerjati.

2.2 Lastnosti leksikografske urejenosti

Za nas so pomembne naslednje tri lastnosti leksikografske urejenosti, pri čemer velja $n \in \mathbb{N}$ in $\mathbf{i}, \mathbf{j}, \mathbf{k}, \mathbf{i}', \mathbf{j}' \in \mathbb{N}_0^n$:

1. (Tranzitivnost) Iz $\mathbf{i} \preceq \mathbf{j}$ in $\mathbf{j} \preceq \mathbf{k}$ sledi $\mathbf{i} \preceq \mathbf{k}$.
2. (Monotonost seštevanja) Naj velja $\mathbf{i} \preceq \mathbf{i}'$ in $\mathbf{j} \preceq \mathbf{j}'$. Sledi, da je $\mathbf{i} + \mathbf{j} \preceq \mathbf{i}' + \mathbf{j}'$. V primeru, da je $\mathbf{i} \prec \mathbf{i}'$ ali $\mathbf{j} \prec \mathbf{j}'$, velja $\mathbf{i} + \mathbf{j} \prec \mathbf{i}' + \mathbf{j}'$.
3. (Totalnost) Za vsaki dve n -terici $\mathbf{i}$ in $\mathbf{j}$ velja natanko eden izmed sledečih izrazov

$$\mathbf{i} \prec \mathbf{j}, \quad \mathbf{i} \succ \mathbf{j}, \quad \mathbf{i} = \mathbf{j}.$$

Dokaz. Najprej dokažimo tranzitivnost. Naj bodo $\mathbf{i} = (i_1, i_2, \dots, i_n)$, $\mathbf{j} = (j_1, j_2, \dots, j_n)$, $\mathbf{k} = (k_1, k_2, \dots, k_n) \in \mathbb{N}_0^n$, kjer so členi $i_t, j_t, k_t \in \mathbb{N}_0$. Brez škode za splošnost naj velja $\mathbf{i} \prec \mathbf{j}$ in $\mathbf{j} \prec \mathbf{k}$. Prvi različni člen med $\mathbf{j}$ in $\mathbf{i}$ je večji pri $\mathbf{j}$ oziroma $i_m < j_m$, kjer je $m \in \mathbb{N}$ zaporedno število prvega različnega člena. Ker so vsi členi pred m -tima členoma enaki, velja zapis

$$\mathbf{j} = (i_1, i_2, \dots, i_{m-1}, j_m, j_{m+1}, j_{m+2}, \dots, j_n).$$

Enak razmislek ponovimo z neenakostjo $\mathbf{j} \prec \mathbf{k}$. Označimo s $p \in \mathbb{N}$ zaporedno število prvega različnega člena n -teric $\mathbf{j}$ in $\mathbf{k}$ ter ločimo dva primera.

Najprej predpostavimo, da je $m \leq p$. V tem primeru zapišemo

$$\mathbf{k} = (i_1, \dots, i_{m-1}, j_m, j_{m+1}, \dots, j_{p-1}, k_p, k_{p+1}, \dots, k_n),$$

in opazimo, da se prvih $m-1$ mest n -terice $\mathbf{k}$ ujema s prvimi $m-1$ mesti n -terice $\mathbf{i}$, za naslednje mesto pa že velja $i_m < k_m$, iz česar sledi $\mathbf{i} \prec \mathbf{k}$.

Zdaj pa predpostavimo, da je $p < m$. V tem primeru zapišemo

$$\mathbf{k} = (i_1, \dots, i_{p-1}, k_p, k_{p+1}, \dots, k_n),$$

in opazimo, da se prvih $p-1$ členov n -teric $\mathbf{i}$ in $\mathbf{k}$ ujema, za naslednji člen pa že velja $j_p < k_p$ in $i_p = j_p$, torej $i_p < k_p$, iz česar sledi $\mathbf{i} \prec \mathbf{k}$.

Dokažimo še totalnost. Vzemimo n -terici $\mathbf{i} = (i_1, i_2, \dots, i_n)$ in $\mathbf{j} = (j_1, j_2, \dots, j_n)$. Predpostavimo najprej, da se n -terici ne razlikujeta v nobenem členu, potem velja $\mathbf{i} = \mathbf{j}$. V nasprotnem primeru naj bo p zaporedno število prvega člena z različnim številom. Člena j_p in i_p primerjamo. Primerjamo dve naravni števili, zato lahko velja samo $i_p < j_p$, iz česar sledi $\mathbf{i} \prec \mathbf{j}$, ali pa $i_p > j_p$, iz česar sledi $\mathbf{i} \succ \mathbf{j}$. $\square$

Dokaz monotonosti seštevanja prepuščamo bralcu. Za dokaz osnovnega izreka o simetričnih polinomih potrebujemo še naslednji izrek.

Izrek 1. Vsako strogo padajoče zaporedje n -teric $\mathbf{d}_1 \succ \mathbf{d}_2 \succ \dots$ je končno.

Pri dokazu izreka nam bo pomagala naslednja lema, v kateri za n -terico $\mathbf{b} \in \mathbb{N}_0^n$ in $a \in \mathbb{N}_0$ uvedemo zapis

$$\mathbf{b} = (b_1, \dots, b_n),$$

$$(a, \mathbf{b}) = (a, b_1, \dots, b_n) \in \mathbb{N}_0^{n+1}.$$

Lema 1. Vsaka neprazna podmnožica $\mathbb{N}_0^n$ ima najmanjši element.

Dokaz. Trditev dokažimo z indukcijo.

Brez dokaza uporabimo, da lema velja v primeru $n = 1$, saj je to znano dejstvo. Ta lastnost se imenuje načelo dobre urejenosti, njen dokaz je dostopen na spletu.

Predpostavimo, da trditev velja za poljubno neprazno podmnožico $\mathbb{N}_0^n$. Trdimo, da velja tudi za vse neprazne podmnožice $\mathbb{N}_0^{n+1}$. Naj bo S neprazna podmnožica $\mathbb{N}_0^{n+1}$. Naj bo $S_0 \subseteq \mathbb{N}_0$ množica prvih koordinat elementov množice S . Po indukcijski predpostavki obstaja najmanjši element v S_0 , saj je neprazna podmnožica naravnih števil. Označimo ga z a . Definirajmo še množico $T \subseteq \mathbb{N}_0^n$, za

katero velja $\mathbf{k} \in T$, če velja $(a, \mathbf{k}) \in S$. Po definiciji množice S_0 je T neprazna, zato ima po induksijski predpostavki T najmanjši element, ki ga poimenujemo $\mathbf{b}$. Trdimo, da je $(a, \mathbf{b})$ najmanjši element množice S . Naj bo $\mathbf{j} = (j_0, j_1, \dots, j_n) \in S$. Po definiciji velja $j_0 \in S_0$, zato vemo, da je $a \leq j_0$. Iz $a < j_0$ sledi, da je $(a, \mathbf{b}) \prec \mathbf{j}$, zato predpostavimo, da je $a = j_0$. Posledično je $(j_1, \dots, j_n) \in T$ in velja $(j_1, \dots, j_n) \leq \mathbf{b}$, kar pomeni, da velja neenakost $\mathbf{j} \preceq (a, \mathbf{b})$. Element $(a, \mathbf{b})$ je torej najmanjši element množice S , kar zaključimo induksijski korak. $\square$

Dokaz izreka. Predpostavimo, da obstaja neskončno strogo padajoče zaporedje elementov $\mathbf{d}_1 \succ \mathbf{d}_2 \succ \dots$ v $\mathbb{N}_0^n$. Množica vseh n -teric v zaporedju je neprazna podmnožica $\mathbb{N}_0^n$, ki nima najmanjšega elementa. Z uporabo zgornje leme to vodi v protislovje. Zato drži nasprotno, in sicer da je vsako strogo padajoče zaporedje $\mathbf{d}_1 \succ \mathbf{d}_2 \succ \dots$ končno. $\square$

3 Polinomi

3.1 Zapis z vsoto

Polinom z več spremenljivkami lahko zapišemo tako, da vsak člen izrazimo kot $C_{\mathbf{d}}X^{\mathbf{d}} = C_{\mathbf{d}}X_1^{d_1}X_2^{d_2}\dots X_n^{d_n}$, pri čemer je $\mathbf{d} \in \mathbb{N}_0^n$ in $C_{\mathbf{d}} \in \mathbb{R}$.

Če uporabimo takšen zapis za vse člene, lahko zapišemo polinom f v obliki

$$f = \sum_{\mathbf{a} \in \mathbb{N}_0^n} C_{\mathbf{a}}X^{\mathbf{a}},$$

pri čemer so $C_{\mathbf{a}} \in \mathbb{R}$, med katerimi je končno mnogo neničelnih.

3.2 Osnovne definicije

V uvodu so definirani polinomi, definirajmo nekaj osnovnih pojmov, ki opisujejo polinome. Stopnja neničelnega polinoma v eni spremenljivki je najvišja potenca neničelnih členov polinoma in jo označimo z $\deg(f)$. Stopnja ničelnega polinoma ni definirana.² Za neničelni polinom stopnje n je vodilni člen $a_n x^n$. Koeficient pri vodilnem členu imenujemo vodilni koeficient in ga označimo z $\text{lead}(f)$.

Zgled 1. Naj bo $f \in \mathbb{R}[X]$ polinom, dan s predpisom

$$f(X) = 3X^4 + 2X^3 + 5X - 7,$$

potem velja, da je $\deg(f) = 4$, $\text{lead}(f) = 3$.

Tako kot imamo pri polinomih z eno spremenljivko vodilni člen, ki določa stopnjo polinoma, imamo pri polinomih z več spremenljivkami vodilni člen, ki določa tako imenovano multistopnjo.

Definicija 1. Naj bo $f \in \mathbb{R}[X_1, \dots, X_n]$ neničelni polinom, zapišimo $f = \sum_{\mathbf{a} \in \mathbb{N}_0^n} c_{\mathbf{a}}X^{\mathbf{a}}$. Multistopnja polinoma f je leksikografsko največja n -terica $\mathbf{d}$, pri kateri je koeficient $c_{\mathbf{d}}$ neničeln in se označi z $\text{mdeg}(f)$. Pri tem imenujemo $c_{\mathbf{d}}X^{\mathbf{d}}$ vodilni člen. Multistopnja ničelnega polinoma ni definirana.

Zgled 2. Pri polinomu $f(X_1, X_2, X_3, X_4) = 5X_1^3 + 3X_1X_2X_3X_4^6 + 7X_2^5$ so 4-terice potenc pri členih $5X_1^3, 3X_1X_2X_3X_4^6$ ter $7X_2^5$ zaporedoma enake $(3, 0, 0, 0)$, $(1, 1, 1, 6)$ ter $(0, 5, 0, 0)$, multistopnja je torej $\text{mdeg}(f) = (3, 0, 0, 0)$.

Tudi polinomom z več spremenljivkami lahko določimo vodilni koeficient.

Definicija 2. Vodilni koeficient neničelnega polinoma f v več spremenljivkah je koeficient pred vodilnim členom. Označimo ga z $\text{lead}(f)$. Vodilni koeficient ničelnega polinoma ni definiran.

Pri prejšnjem zgledu je $\text{lead}(f) = 5$.

²Pogosto se definira $\deg 0 = -\infty$.

Zgled 3. Naj bo $f \in \mathbb{R}[X, Y, Z]$ polinom, podan s predpisom

$$f(X, Y, Z) = 3X^4 + 2XYZ + 5Y^2 + Z.$$

Velja $\text{mdeg}(f) = (4, 0, 0)$ in $\text{lead}(f) = 3$. Pri tem privzamemo naravno leksikografsko urejenost, ki je po vrstnem redu navedbe spremenljivk, torej $X \succ Y \succ Z$.

Definirajmo podmnožico polinomov z več spremenljivkami imenovani simetrični polinomi. Označimo z $[n] = \{1, 2, \dots, n\}$. Bijekcijo $\pi : [n] \rightarrow [n]$ imenujemo permutacija. Polinom $f \in \mathbb{R}[X_1, \dots, X_n]$ je simetrični, če za vsako permutacijo $\pi : [n] \rightarrow [n]$ velja $f(X_{\pi(1)}, X_{\pi(2)}, \dots, X_{\pi(n)}) = f(X_1, X_2, \dots, X_n)$. To pomeni, da lahko zamenjamo spremenljivke na poljuben način in zmeraj dobimo enak polinom. Na primer polinom $p(x, y) = x + y$ je simetrični polinom, saj velja $p(x, y) = x + y = y + x = p(y, x)$. Kasneje bomo dokazali, da lahko vsak simetrični polinom zapišemo kot polinom v tako imenovanih elementarnih simetričnih polinomih.

Definicija 3. Polinom $S_{n,k} \in \mathbb{R}[X_1, \dots, X_n]$, ki ga imenujemo k -ti elementarni simetrični polinom v n spremenljivkah, je vsota vseh možnih produktov k spremenljivk izmed $X_1, \dots, X_n$. Predpis je dan s

$$S_{n,k} = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} X_{i_1} X_{i_2} \cdots X_{i_k}.$$

Zgled 4. Za $n = 3$ so elementarni simetrični polinomi

$$\begin{aligned} S_{3,0}(X, Y, Z) &= 1, \\ S_{3,1}(X, Y, Z) &= X + Y + Z, \\ S_{3,2}(X, Y, Z) &= XY + YZ + XZ, \\ S_{3,3}(X, Y, Z) &= XYZ. \end{aligned}$$

3.3 Vietove formule

Kot primer uporabe simetričnih polinomov prikažemo Vietove formule. Če kubični polinom $f(X) = aX^3 + bX^2 + cX + d$ z ničlami $X_1, X_2, X_3 \in \mathbb{R}$ zapišemo v ničelni obliki kot $f(X) = a(X - X_1)(X - X_2)(X - X_3)$ in zmnožimo vse faktorje ničelne oblike, dobimo

$$\begin{aligned} f(X) &= a(X - X_1)(X - X_2)(X - X_3) = \\ &= aX^3 - a(X_1 + X_2 + X_3)X^2 + a(X_1X_2 + X_1X_3 + X_2X_3)X - aX_1X_2X_3. \end{aligned}$$

Opazimo, da lahko enačimo koeficiente pri istoležnih členih, da dobimo dobro znane Vietove formule

$$\begin{aligned} 1 &= \frac{a}{a}, \\ X_1 + X_2 + X_3 &= -\frac{b}{a}, \\ X_1X_2 + X_3X_2 + X_1X_3 &= \frac{c}{a}, \\ X_1X_2X_3 &= -\frac{d}{a}. \end{aligned}$$

Zapišemo vse elementarne simetrične polinome v treh spremenljivkah in opazimo, da se pojavijo v Vietovih formulah.

$$\begin{aligned} S_{3,0}(X_1, X_2, X_3) &= 1, \\ S_{3,1}(X_1, X_2, X_3) &= X_1 + X_2 + X_3, \\ S_{3,2}(X_1, X_2, X_3) &= X_1X_2 + X_1X_3 + X_2X_3, \\ S_{3,3}(X_1, X_2, X_3) &= X_1X_2X_3. \end{aligned}$$

Multistopnja polinoma $S_{n,k}$ je enaka $(\underbrace{1, \dots, 1}_k, 0, \dots, 0)$, pri čemer je na prvih k mestih število 1, na vseh ostalih pa 0.

3.4 Trditve o polinomih

V tem poglavju predstavimo tri trditve o polinomih v več spremenljivkah, ki jih uporabljamo pri računanju. Za množenje neničelnih polinomov več spremenljivk veljata trditvi $\text{mdeg}(f \cdot g) = \text{mdeg}(f) + \text{mdeg}(g)$ in $\text{lead}(f \cdot g) = \text{lead}(f) \cdot \text{lead}(g)$, pri čemer prva razloži, kako izračunamo multistopnjo pri množenju, druga pa pri istem postopku opisuje nastanek vodilnega koeficienta. Za seštevanje polinomov v več spremenljivkah velja bodisi $f + g = 0$ bodisi $\text{mdeg}(f + g) \preceq \max\{\text{mdeg}(f), \text{mdeg}(g)\}$.

Dokaz prvih dveh trditev. Označimo $\text{mdeg}(f) = \mathbf{n}$ in $\text{mdeg}(g) = \mathbf{m}$. Oglejmo si njun produkt v strnjem zapisu, torej polinoma f in g zaporedoma zapišemo kot

$$f = c_{\mathbf{n}} \mathbf{X}^{\mathbf{n}} + \sum_{\mathbf{a} \prec \mathbf{n}} c_{\mathbf{a}} \mathbf{X}^{\mathbf{a}} \text{ in } g = b_{\mathbf{m}} \mathbf{X}^{\mathbf{m}} + \sum_{\mathbf{a} \prec \mathbf{m}} b_{\mathbf{a}} \mathbf{X}^{\mathbf{a}}.$$

Množenje polinomov poteka po členih. Velja

$$f \cdot g = c_{\mathbf{n}} b_{\mathbf{m}} \mathbf{X}^{\mathbf{n}} \mathbf{X}^{\mathbf{m}} + \text{členi nižje multistopnje},$$

kar argumentiramo v nadaljevanju. Po definiciji velja enakost $c_{\mathbf{a}} \mathbf{X}^{\mathbf{a}} c_{\mathbf{b}} \mathbf{X}^{\mathbf{b}} = c_{\mathbf{a} + \mathbf{b}} \mathbf{X}^{\mathbf{a} + \mathbf{b}}$. Spomnimo se na monotonost leksikografske urejenosti. Iz te sledi, da je vsota multistopenj dveh členov, med katerima vsaj eden ni vodilni, strogo manjša kot vsota multistopenj vodilnih členov. Sledi, da je vodilni člen produkta produkt vodilnih členov faktorjev. S tem smo pokazali, da je $\text{mdeg}(f \cdot g) = \text{mdeg}(f) + \text{mdeg}(g)$ in, da je

$$\text{lead}(f \cdot g) = \text{lead}(f) \cdot \text{lead}(g).$$

□

Dokaz trditve o multistopnji polinoma pri seštevanju prepustimo bralcu.

4 Osnovni izrek o simetričnih polinomih

Trdimo, da je vsak simetrični polinom mogoče zapisati kot polinom v elementarnih simetričnih polinomih.

Izrek 2. *Naj bo f simetrični polinom v n spremenljivkah. Potem velja*

$$f \in \mathbb{R}[S_{n,1}, S_{n,2}, \dots, S_{n,n}].$$

To pomeni, da obstajajo takšna realna števila $c_{\mathbf{a}} \in \mathbb{R}$, med katerimi je največ končno mnogo neničelnih, da lahko z uporabo zapisa $\mathbf{S} = (S_{n,1}, S_{n,2}, \dots, S_{n,n})$ in $\mathbf{S}^{(a_1, a_2, \dots, a_n)} = S_{n,1}^{a_1} S_{n,2}^{a_2} \dots S_{n,n}^{a_n}$ zapišemo

$$f = \sum_{\mathbf{a} \in \mathbb{N}_0^n} c_{\mathbf{a}} \mathbf{S}^{\mathbf{a}}.$$

Dokaz. Naj bo $f \in \mathbb{R}[X_1, \dots, X_n]$ poljuben simetrični polinom z multistopnjo $\mathbf{d} = (d_1, d_2, \dots, d_n)$. Dokaza se lotimo tako, da postopoma iščemo polinome elementarnih simetričnih polinomov, ki vsoto v določenem smislu približujejo polinomu f . Najprej odštejemo tak polinom iz elementarnih simetričnih polinomov, ki ima enak vodilni člen kot f , in razliko poimenujemo f_1 . S tem je multistopnja novega polinoma manjša kot multistopnja prejšnjega in postopek ponavljamo, dokler ne pridemo do ničelnega polinoma. Uporabimo že znano lastnost multistopnje produkta simetričnih polinomov $\text{mdeg}(fg) = \text{mdeg}(f) + \text{mdeg}(g)$ ter zapišemo

$$\text{mdeg}(S_{n,1}^{a_1} S_{n,2}^{a_2} \dots S_{n,n}^{a_n}) = a_1 \text{mdeg}(S_{n,1}) + \dots + a_n \text{mdeg}(S_{n,n}).$$

Multistopnja je tako enaka $(a_1 + a_2 + \dots + a_n, a_2 + a_3 + \dots + a_n, \dots, a_n)$. Želimo, da je multistopnja enaka $\mathbf{d}$, torej $(d_1, d_2, \dots, d_n)$. Iz tega sledi, da je $d_n = a_n$ ter

$$\begin{aligned} d_{n-1} &= a_{n-1} + a_n, \\ a_{n-1} &= d_{n-1} - d_n. \\ d_{n-2} &= a_{n-2} + a_{n-1} + a_n, \\ a_{n-2} &= d_{n-2} - d_{n-1} + d_n = d_{n-2} - d_{n-1}. \end{aligned}$$

Enako lahko izrazimo vse ostale a -je z d -ji. Če $k \neq n$, nastavimo $a_k = d_k - d_{k+1}$. Če so te razlike negativne, pride do problema, zato moramo zagotoviti, da velja

$$d_1 \geq d_2 \geq d_3 \geq \dots \geq d_n \geq 0.$$

Hitro opazimo, da je problem le v nesimetričnih polinomih. Pri polinomu $f(X_1, X_2, X_3) = X_1 X_3^5 + X_2$ sta multistopnji posameznih členov (1,0,5) in (0,1,0), kjer za multistopnjo polinoma (1,0,5) zgornji pogoj ni izpolnjen. Pri simetričnih polinomih, kot je $f(X_1, X_2) = X_1^2 X_2 + X_1 X_2^2$, z multistopnjama členov (2, 1) in (1, 2), opazimo, da za multistopnjo polinoma (2,1) zgornji pogoj velja. Zaradi simetričnosti so koordinate multistopnje vedno v padajočem vrstnem redu. Če to ne bi držalo, bi lahko zamenjali spremenljivke polinoma in dobili polinom z večjo multistopnjo, kar je protislovje.

V nadaljevanju dokaza določimo vse a_i in produkt $S_{n,1}^{a_1} S_{n,2}^{a_2} \dots S_{n,n}^{a_n}$ pomnožimo z $\text{lead}(f)$, da dobimo g_1 , ki ga odštejemo od f . Tako se odštejeta vodilna člena, kar je tudi naš cilj. Za lažje razumevanje pogledjmo primer odštevanja dveh polinomov z eno spremenljivko.

Zgled 5. *Podana imamo polinoma*

$$\begin{aligned} f(X) &= 5X^6 + 7X^5 + 3X, \\ g(X) &= X^6 + X. \end{aligned}$$

Če ju odštejemo takoj, se členi s stopnjo polinoma ne odštejejo, saj ostane še $4X^6$. Zato g pomnožimo z vodilnim koeficientom f , pri odštevanju dobimo polinom $h(X) = 7X^5 - 2X$, torej znižamo stopnjo polinoma f .

Nadaljujemo dokaz izreka 2. Ko odštejemo polinom $\text{lead}(f)g_1$ od f , se vodilna člena odštejeta in dobimo polinom f_1 s strogo nižjo multistopnjo od f .

Polinom f_1 je simetrični. Iz tega sledi, da lahko postopek ponovimo s f_1 namesto f . To dokažimo z računom

$$\begin{aligned} f_1(X_{\pi(1)}, \dots, X_{\pi(n)}) &= f(X_{\pi(1)}, \dots, X_{\pi(n)}) - g_1(X_{\pi(1)}, \dots, X_{\pi(n)}) = \\ &= f(X_1, \dots, X_n) - g_1(X_1, \dots, X_n) = f_1(X_1, \dots, X_n). \end{aligned}$$

Nadaljujemo tako, da po enakem postopku kot za iskanje g_1 poiščemo polinom g_2 z enako multistopnjo kot f_1 , tega pomnožimo z vodilnim koeficientom f_1 in razliko vzamemo za f_2 .

Ponovno velja $\text{mdeg}(f_1) \succ \text{mdeg}(f_2)$ in f_2 je simetrični polinom. Prikazan proces ponavljamo, dokler sčasoma ne dobimo $f_r = 0$. Zaporedje se mora zaključiti z ničelnim polinomom zaradi izreka (1). To lahko zapišemo tudi kot

$$\begin{aligned} 0 &= f_{r-1} - g_r = \\ &= f_{r-2} - g_{r-1} - g_r = \\ &\quad \vdots \\ &= f - g_1 - g_2 - \dots - g_r, \end{aligned}$$

iz česar sledi

$$f = g_1 + g_2 + \dots + g_r.$$

Ker so polinomi $g_1, \dots, g_r$ večkratniki produktov elementarnih simetričnih polinomov, smo s tem dokazali, da je vsak simetrični polinom vsota produktov elementarnih simetričnih polinomov. $\square$

4.1 Primer osnovnega izreka o simetričnih polinomih

Za primer uporabe osnovnega izreka o simetričnih polinomih izpeljimo postopek, opisan v dokazu, na konkretnem simetričnem polinomu. Obravnavajmo primer s tremi spremenljivkami X, Y, Z , ki so urejene s pravilom $X \succ Y \succ Z$. Vzamemo simetrični polinom $f(X, Y, Z) = X^2 + Y^2 + Z^2$, ki ga želimo izraziti kot polinom v elementarnih simetričnih polinomih.

Za začetek vzemimo $S_{3,1}^2 = (X + Y + Z)^2$, ki ga lahko zapišemo tudi kot

$S_{3,1}^2 = X^2 + 2XY + Y^2 + 2XZ + 2YZ + Z^2$ in ga odštejemo od polinoma f . Dobimo polinom f_1 s predpisom

$$\begin{aligned} f_1 &= (X^2 + Y^2 + Z^2) - (X^2 + 2XY + Y^2 + 2XZ + 2YZ + Z^2), \\ f_1 &= -2XY - 2XZ - 2YZ. \end{aligned}$$

Opazimo, da lahko polinomu f_1 preprosto prištejemo dvakratnik oblike $S_{3,2} = XY + YZ + XZ$, torej zapišemo izraz $f_2 = f_1 + 2S_{3,2}$. Če bi bila multistopnja simetričnega polinoma večja kot v tem primeru, bi postopek lahko trajal dlje in na enak način naprej, v tem primeru pa se konča pri $f_2 = 0$, kar pomeni, da smo bili uspešni.

Združimo te izraze in dobimo zapis polinoma f kot polinom v elementarnih simetričnih polinomih

$$\begin{aligned} f_1 &= f - S_{3,1}^2, \\ f_2 &= f_1 + 2S_{3,2} = 0, \\ 0 &= f - S_{3,1}^2 + 2S_{3,2}, \\ f &= S_{3,1}^2 - 2S_{3,2}. \end{aligned}$$

Literatura

- [1] K. Conrad, *Symmetric polynomials*, spletni zapiski, University of Connecticut. Dostopno na: <https://kconrad.math.uconn.edu/blurbs/galoistheory/symmfunction.pdf>