Symetrické polynomy

Buď $\mathbb{R}[x_1, x_2, \dots, x_n]$ okruh všech polynomů n proměnných $x_1, x_2, \dots, x_n$ s koeficienty, jimiž jsou libovolné prvky tělesa $\mathbb{R}$ všech reálných čísel. Buď $p \in \mathbb{R}[x_1, x_2, \dots, x_n]$ libovolný takový polynom. Přejeme-li si zde zdůraznit, že p je polynom v proměnných $x_1, x_2, \dots, x_n$, píšeme obšírněji $p(x_1, x_2, \dots, x_n)$ místo pouhého p. Do takového polynomu můžeme dále dosadit libovolné polynomy $q_1, q_2, \dots, q_n$ z okruhu $\mathbb{R}[x_1, x_2, \dots, x_n]$ za jednotlivé proměnné $x_1, x_2, \dots, x_n$. Výsledkem takového dosazení je potom polynom z okruhu $\mathbb{R}[x_1, x_2, \dots, x_n]$, který zaznamenáváme zápisem $p(q_1, q_2, \dots, q_n)$. Řekneme, že polynom p z okruhu $\mathbb{R}[x_1, x_2, \dots, x_n]$ je symetrický, jestliže pro každou permutaci σ množiny čísel $\{1, 2, \dots, n\}$ platí rovnost $p(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) = p(x_1, x_2, \dots, x_n)$. Příklady symetrických polynomů jsou sumy $s_k = x_1^k + x_2^k + \cdots + x_n^k$ mocnin jednotlivých proměnných pro libovolná kladná celá čísla k. Je-li $p(x_1, x_2, \dots, x_n)$ libovolný polynom z okruhu $\mathbb{R}[x_1, x_2, \dots, x_n]$ a jsou-li $q_1, q_2, \dots, q_n$ libovolné symetrické polynomy z tohoto okruhu, pak polynom $p(q_1, q_2, \dots, q_n)$ vzniklý dosazením je symetrický polynom z tohoto okruhu.

Člen v proměnných $x_1, x_2, \ldots, x_n$ je libovolný součin mocnin proměnných tvaru $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$, kde $\alpha_1, \alpha_2, \ldots, \alpha_n$ jsou libovolná nezáporná celá čísla. Stupněm člene $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ pak rozumíme součet $\alpha_1 + \alpha_2 + \cdots + \alpha_n$ exponentů u všech jeho proměnných. Každý polynom p z okruhu $\mathbb{R}[x_1, x_2, \ldots, x_n]$ je pak součtem několika členů opatřených koeficienty, jimiž jsou nějaké prvky tělesa $\mathbb{R}$ vyjma nuly. Stupněm nenulového polynomu p pak rozumíme největší ze stupňů jeho jednotlivých členů. Řekneme, že nenulový polynom p z okruhu $\mathbb{R}[x_1, x_2, \ldots, x_n]$ je homogenní, jestliže všechny jeho členy mají tentýž stupeň. Stupněm homogenního polynomu je pak ovšem stupeň kteréhokoliv z jeho jednotlivých členů. Je vidět, že každý polynom p z okruhu $\mathbb{R}[x_1, x_2, \ldots, x_n]$ je pak součtem několika homogenních polynomů různých stupňů. Je-li tento polynom p symetrický, pak jednotlivé homogenní polynomy různých stupňů, které v součtu dají tento symetrický polynom p, jsou samy o sobě rovněž symetrickými polynomy. Dostáváme se tak k pojmu homogenních symetrických polynomů. Pro každé kladné celé číslo k označme symbolem $\Lambda_{\mathbb{R}}^k[x_1, x_2, \ldots, x_n]$ množinu všech homogenních symetrických polynomů stupně k s koeficienty, jimiž jsou libovolné prvky tělesa $\mathbb{R}$. Pak množina $\Lambda_{\mathbb{R}}^k[x_1, x_2, \ldots, x_n]$ tvoří vektorový podprostor ve vektorovém prostoru $\mathbb{R}[x_1, x_2, \ldots, x_n]$ nad tělesem $\mathbb{R}$ všech reálných čísel. Uvidíme, že $\Lambda_{\mathbb{R}}^k[x_1, x_2, \ldots, x_n]$ je vektorový prostor nad tělesem $\mathbb{R}$ konečné dimenze, a najdeme jeho bázi.

Rozkladem λ nezáporného celého čísla k rozumíme libovolnou posloupnost $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_s)$ kladných celých čísel takovou, že $\lambda_1 \geqslant \lambda_2 \geqslant \dots \geqslant \lambda_s$ a $\lambda_1 + \lambda_2 + \dots + \lambda_s = k$. Délkou rozkladu λ rozumíme počet s jeho kladných složek a značíme ji symbolem $\ell(\lambda)$. Někdy připouštíme, aby složkami rozkladu λ byly i nuly, a náš původní rozklad $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_s)$ pak ztotožňujeme s každou posloupností tvaru $(\lambda_1, \lambda_2, \dots, \lambda_s, 0, 0, \dots, 0)$. Značíme symbolem $\mathrm{Par}(k)$ množinu všech rozkladů čísla k. Jestliže $\lambda \in \mathrm{Par}(k)$, píšeme také $\lambda \vdash k$. Ještě pro každé $i \in \{1, 2, \dots, k\}$ označme symbolem $m_i = m_i(\lambda)$ počet těch složek rozkladu λ, které jsou rovny i. Pak ovšem platí $m_1 + m_2 + \dots + m_k = \ell(\lambda)$ a $1m_1 + 2m_2 + \dots + km_k = k$.

Pro každé nezáporné celé číslo k definujeme částečné uspořádání $\leqslant$ na množině rozkladů $\mathrm{Par}(k)$, nazývané uspořádání dominancí, následujícím způsobem. Jsou-li $\mu = (\mu_1, \mu_2, \dots, \mu_r)$ a $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_s)$ dva rozklady čísla k, pak klademe $\mu \leqslant \lambda$, jestliže platí

$$\mu_1 + \mu_2 + \dots + \mu_j \leqslant \lambda_1 + \lambda_2 + \dots + \lambda_j \qquad \text{pro všechna } j \geqslant 1.$$

Dostáváme tak částečně uspořádanou množinu $(\mathrm{Par}(k), \leqslant)$.

Budeme dále potřebovat nějaké lineární uspořádání množiny $\mathrm{Par}(k)$, které by bylo kompatibilní s tímto právě definovaným uspořádáním dominancí. Příkladem takového lineárního uspořádání je lexikografické uspořádání, které budeme značit symbolem $\preccurlyeq$. Toto uspořádání je definováno následovně. Jestliže $\mu = (\mu_1, \mu_2, \ldots, \mu_r)$ a $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_s)$ jsou dva rozklady čísla k, pak klademe $\mu \preccurlyeq \lambda$, jestliže buďto $\mu = \lambda$, anebo pro nějaké $j \geqslant 1$ platí

$$\mu_1 = \lambda_1,\ \mu_2 = \lambda_2,\ \ldots,\ \mu_{j-1} = \lambda_{j-1}, \qquad \mu_j < \lambda_j.$$

Dostáváme tak lineárně uspořádanou množinu $(\mathrm{Par}(k), \preccurlyeq)$. Je snadné se přesvědčit, že takto definované lexikografické uspořádání $\preccurlyeq$ je skutečně kompatibilní s částečným uspořádáním dominancí $\leqslant$, totiž že pro libovolné dva rozklady μ a λ čísla k splňující $\mu \leqslant \lambda$ platí $\mu \preccurlyeq \lambda$.

Je-li $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_s)$ rozklad čísla k a je-li splněno $\ell(\lambda) \leqslant n$, definujeme homogenní symetrický polynom $m_\lambda(x_1, x_2, \ldots, x_n)$ stupně k v proměnných $x_1, x_2, \ldots, x_n$ předpisem

$$m_\lambda(x_1, x_2, \ldots, x_n) = \sum_\alpha x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n},$$

kde suma běží přes všechny vzájemně různé permutace $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ složek posloupnosti $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_s, 0, 0, \ldots, 0)$, kterou bereme jako posloupnost délky n. Polynom $m_\lambda(x_1, x_2, \ldots, x_n)$ nazýváme monomiální symetrický polynom.

Je-li nyní f libovolný homogenní symetrický polynom stupně k v proměnných $x_1, x_2, \ldots, x_n$, takže polynom f je prvkem vektorového podprostoru $\Lambda^k_{\mathbb{R}}[x_1, x_2, \ldots, x_n]$, a je-li navíc splněno $k \leqslant n$, pak f je očividně lineární kombinací monomiálních symetrických polynomů $m_\lambda(x_1, x_2, \ldots, x_n)$, kde λ probíhá všechny rozklady čísla k, přičemž koeficienty jsou nějaké prvky tělesa $\mathbb{R}$. Navíc takové vyjádření polynomu f ve tvaru lineární kombinace monomiálních symetrických polynomů je jediné. Odtud plyne, že množina monomiálních symetrických polynomů $\{m_\lambda(x_1, x_2, \ldots, x_n) : \lambda \vdash k\}$ tvoří bázi vektorového prostoru $\Lambda^k_{\mathbb{R}}[x_1, x_2, \ldots, x_n]$. Je tedy dimenze tohoto vektorového prostoru rovna počtu prvků množiny $\mathrm{Par}(k)$ všech rozkladů čísla k.

Definujme teď ještě jinou množinu homogenních symetrických polynomů, značme je $p_\lambda(x_1, x_2, \ldots, x_n)$, kde λ probíhá množinu $\mathrm{Par}(k)$ všech rozkladů čísla k, následujícím způsobem. Předpokládáme i nadále, že je splněno $k \leqslant n$. Začneme tím, že připomeneme, že pro každé kladné celé číslo h jsme definovali sumu mocnin proměnných s_h, anebo podrobněji $s_h(x_1, x_2, \ldots, x_n)$, předpisem

$$s_h = x_1^h + x_2^h + \cdots + x_n^h.$$

Pak pro každý rozklad $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_\varsigma)$ daného čísla k, kde $\varsigma = \ell(\lambda)$ je délka rozkladu λ, klademe

$$p_\lambda(x_1, x_2, \ldots, x_n) = s_{\lambda_1} s_{\lambda_2} \cdots s_{\lambda_\varsigma}.$$

Směřujeme nyní k tomu ukázat, že pak množina symetrických polynomů $\{p_\lambda(x_1, x_2, \ldots, x_n) : \lambda \vdash k\}$ tvoří jinou bázi našeho vektorového prostoru $\Lambda^k_{\mathbb{R}}[x_1, x_2, \ldots, x_n]$.

Buď M neprázdná konečná množina. Uspořádaným rozkladem této množiny M rozumíme každou posloupnost $\pi = (B_1, B_2, \ldots, B_\varkappa)$ neprázdných vzájemně disjunktních podmnožin množiny M, jejichž sjednocením je celá množina M, takže pak soubor podmnožin $\{B_1, B_2, \ldots, B_\varkappa\}$ tvoří obvyklý rozklad množiny M. Podmnožiny $B_1, B_2, \ldots, B_\varkappa$ nazýváme bloky uspořádaného rozkladu π.

Tvrzení.

Nechť $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_\varsigma)$ je rozklad čísla k, kde $\varsigma = \ell(\lambda)$ je délka tohoto rozkladu. Poněvadž množina polynomů $\{m_\mu : \mu \vdash k\}$ tvoří bázi vektorového prostoru $\Lambda^k_{\mathbb{R}}[x_1, x_2, \ldots, x_n]$, existují jednoznačně určená reálná čísla $r_{\lambda\mu}$, kde μ probíhá všechny rozklady čísla k, taková, že platí

$$p_\lambda = \sum_{\mu \vdash k} r_{\lambda\mu} m_\mu.$$

Buď $\mu = (\mu_1, \mu_2, \ldots, \mu_\varkappa)$ kterýkoliv z těchto rozkladů čísla k, kde $\varkappa = \ell(\mu)$ je délka tohoto rozkladu. Pak číslo $r_{\lambda\mu}$ je rovno počtu všech těch uspořádaných rozkladů $\pi = (B_1, B_2, \ldots, B_\varkappa)$ množiny čísel $\{1, 2, \ldots, \varsigma\}$, pro něž platí

$$\mu_j = \sum_{i\in B_j} \lambda_i \qquad \textit{pro všechna } j = 1, 2, \ldots, \varkappa.$$

Důkaz.

Připomeňme, že podle našeho předpokladu je $k \leqslant n$. Pak ovšem máme $\ell(\mu) \leqslant n$, čili $\varkappa \leqslant n$. Je jasné, že pak číslo $r_{\lambda\mu}$ je koeficientem člene $x_1^{\mu_1} x_2^{\mu_2} \ldots x_\varkappa^{\mu_\varkappa}$ v součinu $p_\lambda = s_{\lambda_1} s_{\lambda_2} \cdots s_{\lambda_\varsigma}$, to jest v součinu $\left(\sum x_i^{\lambda_1}\right)\left(\sum x_i^{\lambda_2}\right) \cdots \left(\sum x_i^{\lambda_\varsigma}\right)$. Abychom dostali člen $x_1^{\mu_1} x_2^{\mu_2} \ldots x_\varkappa^{\mu_\varkappa}$ v rozvoji tohoto součinu, vybereme pro každé $j = 1, 2, \ldots, \varsigma$ sčítanec $x_{i_j}^{\lambda_j}$ z činitele $\sum x_i^{\lambda_j}$ takovým způsobem, aby bylo splněno $\prod_j x_{i_j}^{\lambda_j} = x_1^{\mu_1} x_2^{\mu_2} \ldots x_\varkappa^{\mu_\varkappa}$. Pro každé $t = 1, 2, \ldots, \varkappa$ pak položme $B_t = \{j \in \{1, 2, \ldots, \varsigma\} : i_j = t\}$. Potom $\pi = (B_1, B_2, \ldots, B_\varkappa)$ bude uspořádaným rozkladem množiny čísel $\{1, 2, \ldots, \varsigma\}$ splňujícím poslední výše uvedenou podmínku. Naopak zase každý takový uspořádaný rozklad π dá popsaným způsobem vzniknout členu $x_1^{\mu_1} x_2^{\mu_2} \ldots x_\varkappa^{\mu_\varkappa}$. $\square$

Věta.

Nechť $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_\varsigma)$ je rozklad čísla k, kde $\varsigma = \ell(\lambda)$ je délka tohoto rozkladu. Pak, jak už bylo řečeno výše, existují jednoznačně určená reálná čísla $r_{\lambda\mu}$, kde μ probíhá všechny rozklady čísla k, taková, že platí

$$p_\lambda = \sum_{\mu \vdash k} r_{\lambda\mu} m_\mu.$$

Pak platí $r_{\lambda\mu} = 0$ s případnou výjimkou těch rozkladů μ čísla k, pro něž je $\lambda \leqslant \mu$. Naproti tomu máme

$$r_{\lambda\lambda} = m_1(\lambda)!\, m_2(\lambda)! \cdots m_k(\lambda)!,$$

kde pro každé $i \in \{1, 2, \ldots, k\}$ je $m_i(\lambda)$ počet těch složek rozkladu λ, které jsou rovny i. Odtud plyne, že množina polynomů $\{p_\lambda : \lambda \vdash k\}$ tvoří bázi vektorového prostoru $\Lambda^k_{\mathbb{R}}[x_1, x_2, \ldots, x_n]$.

Důkaz.

Jestliže $\mu = (\mu_1, \mu_2, \ldots, \mu_\varkappa)$ je rozklad čísla k takový, že $r_{\lambda\mu} \neq 0$, pak podle předchozího tvrzení existuje alespoň jeden uspořádaný rozklad $\pi = (B_1, B_2, \ldots, B_\varkappa)$ množiny čísel $\{1, 2, \ldots, \varsigma\}$ takový, že platí $\mu_j = \sum_{i \in B_j} \lambda_i$ pro všechna $j = 1, 2, \ldots, \varkappa$. Vezměme kterékoliv číslo $t \in \{1, 2, \ldots, \varsigma\}$.

Nechť $B_{i_1}, \dots, B_{i_\nu}$ jsou všechny ty vzájemně různé bloky uspořádaného rozkladu π, které obsahují alespoň jedno z čídel $1, 2, \dots, t$. Z poslední podmínky uvedené výše v tomto důkazu plyne, že $\mu_{i_1} + \dots + \mu_{i_\nu} \geqslant \lambda_1 + \lambda_2 + \dots + \lambda_t$. Kromě toho z faktu, že $t \geqslant \nu$ a $\mu_1 \geqslant \mu_2 \geqslant \dots \geqslant \mu_\varkappa$, zřejmě plyne, že $\mu_1 + \mu_2 + \dots + \mu_t \geqslant \mu_{i_1} + \dots + \mu_{i_\nu}$. Dohromady tedy dostáváme, že $\mu_1 + \mu_2 + \dots + \mu_t \geqslant \lambda_1 + \lambda_2 + \dots + \lambda_t$. Poněvadž t bylo libovolné číslo z množiny $\{1, 2, \dots, \varsigma\}$, celkem to dává, že $\lambda \leqslant \mu$ v uspořádání dominancí.

Pokud jde o hodnotu $r_{\lambda\lambda}$, pak v úvahách z předchozího odstavce pro případ, že $\mu = \lambda$, zřejmě musí být všechny bloky $B_1, B_2, \dots, B_\varkappa$ uspořádaného rozkladu π jednoprvkovými množinami (poznamenejme zde, že pak totiž $\varkappa = \varsigma$). Navíc pro každé $j \in \{1, 2, \dots, \varkappa\}$ má platit, že $\mu_j = \lambda_i$, kde $i \in \{1, 2, \dots, \varsigma\}$ je to číslo, pro něž $B_j = \{i\}$. Poněvadž nyní $\mu = \lambda$ a navíc máme $\lambda_1 \geqslant \lambda_2 \geqslant \dots \geqslant \lambda_\varsigma$, plyne odtud, že uspořádaný rozklad $\pi = (B_1, B_2, \dots, B_\varkappa)$ množiny čísel $\{1, 2, \dots, \varsigma\}$ se od uspořádaného souboru množin $(\{1\}, \{2\}, \dots, \{\varsigma\})$ může lišit nanejvýš nějakou permutací prvních $m_k(\lambda)$ položek tvaru $\{i\}$, pro něž $\lambda_i = k$, potom nějakou permutací následujících $m_{k-1}(\lambda)$ položek tvaru $\{i\}$, pro něž $\lambda_i = k - 1$, atd., až nakonec nějakou permutací posledních $m_1(\lambda)$ položek tvaru $\{i\}$, pro něž $\lambda_i = 1$. Celkem to dává $m_1(\lambda)!\, m_2(\lambda)! \cdots m_k(\lambda)!$ možností, jak může vypadat uspořádaný rozklad π, a tomuto počtu je pak také rovno číslo $r_{\lambda\lambda}$.

Konečně uvažme matici $R = \left(r_{\lambda\mu}\right)_{\lambda,\mu\in\mathrm{Par}(k)}$. Indexy řádků a sloupců v této matici nechť jsou lineárně uspořádány lexikografickým uspořádáním $\preccurlyeq$ množiny rozkladů $\mathrm{Par}(k)$. Viděli jsme dříve, že toto uspořádání je zúplněním částečného uspořádání $\leqslant$ dominancí na této množině $\mathrm{Par}(k)$. Z prvního odstavce tohoto důkazu tak plyne, že R je horní trojúhelníková matice. Z druhého odstavce tohoto důkazu pak plyne, že všechny prvky na hlavní diagonále matice R jsou nenulové. Dohromady to ukazuje, že R je regulární matice. Z definice prvků $r_{\lambda\mu}$ matice R je patrno, že matice R je maticí přechodu od soustavy polynomů $\{p_\lambda : \lambda \vdash k\}$ k soustavě polynomů $\{m_\lambda : \lambda \vdash k\}$. Ale, jak jsme už dříve viděli, množina polynomů $\{m_\lambda : \lambda \vdash k\}$ tvoří bázi vektorového prostoru $\Lambda^k_{\mathbb{R}}[x_1, x_2, \ldots, x_n]$. Z tohoto důvodu také množina polynomů $\{p_\lambda : \lambda \vdash k\}$ tvoří bázi vektorového prostoru $\Lambda^k_{\mathbb{R}}[x_1, x_2, \ldots, x_n]$. $\square$

Z právě uvedené věty odvodíme ještě následující důsledek. Připomeňme, že až dosud jsme předpokládali, že $k \leqslant n$. Nyní ale budeme pracovat se silnějším předpokladem. Budeme žádat, aby platilo $k^2 \leqslant n$. Pak obdržíme následující fakt.

Důsledek.

Ke každému symetrickému polynomu f z okruhu polynomů $\mathbb{R}[x_1, x_2, \ldots, x_n]$ stupně nejvýše k existuje jediný polynom q v okruhu polynomů $\mathbb{R}[x_1, x_2, \ldots, x_k]$ stupně nejvýše k takový, že platí $f = q(s_1, s_2, \ldots, s_k)$.

Důkaz.

Již jsme viděli, že symetrický polynom f je součtem konečného počtu homogenních symetrických polynomů různých stupňů, které nepřevyšují hodnotu k. Pokud dokážeme, že uvedený důsledek platí pro všechny sčítance v tomto součtu, budeme mít tento důsledek dokázán i pro samotný symetrický polynom f. Můžeme tedy dále předpokládat, že f je homogenní symetrický polynom stupně h, kde $h \leqslant k$. Kvůli jednoduchosti provedeme důkaz pouze v případě, kdy $h = k$. Pro menší hodnoty h by se důkaz vedl obdobně. Je tedy nyní f prvkem vektorového prostoru $\Lambda^k_{\mathbb{R}}[x_1, x_2, \ldots, x_n]$.

Podle předchozí věty je množina polynomů $\{p_\lambda : \lambda \vdash k\}$ bází vektorového prostoru $\Lambda^k_{\mathbb{R}}[x_1, x_2, \ldots, x_n]$. Existují tedy jednoznačně určené prvky c_λ tělesa $\mathbb{R}$, kde λ probíhá všechny rozklady čísla k, takové, že platí

$$f = \sum_{\lambda \vdash k} c_\lambda p_\lambda.$$

Ovšem polynomy p_λ jsou podle definice rovny polynomům

$$p_\lambda = s_{\lambda_1} s_{\lambda_2} \cdots s_{\lambda_\varsigma},$$

kde $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_\varsigma)$ a $\varsigma = \ell(\lambda)$ je délka rozkladu λ. Poněvadž λ je rozklad čísla k, máme $\lambda_1 \leqslant k$, $\lambda_2 \leqslant k$, ..., $\lambda_\varsigma \leqslant k$. Vznikne tedy polynom $s_{\lambda_1} s_{\lambda_2} \cdots s_{\lambda_\varsigma}$ dosazením polynomů $s_1, s_2, \ldots, s_k$ za proměnné $x_1, x_2, \ldots, x_k$ do člene $x_{\lambda_1} x_{\lambda_2} \cdots x_{\lambda_\varsigma}$. Tento poslední člen je ovšem prvkem okruhu polynomů $\mathbb{R}[x_1, x_2, \ldots, x_k]$ stupně nejvýše k. Celkem to tedy znamená, že samotný polynom f vznikne dosazením polynomů $s_1, s_2, \ldots, s_k$ za proměnné $x_1, x_2, \ldots, x_k$ do polynomu

$$q = \sum_{\lambda \vdash k} c_\lambda \, x_{\lambda_1} x_{\lambda_2} \cdots x_{\lambda_\varsigma},$$

což je ale prvek okruhu polynomů $\mathbb{R}[x_1, x_2, \ldots, x_k]$ stupně nejvýše k. Zbývá ozřejmit, že tento polynom q je určen jednoznačně.

Buď tedy $\bar{q}$ libovolný polynom z okruhu $\mathbb{R}[x_1, x_2, \ldots, x_k]$ stupně nejvýše k takový, že platí $f = \bar{q}(s_1, s_2, \ldots, s_k)$. Uvažme libovolný člen $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_k^{\alpha_k}$ tohoto polynomu; tento člen je ovšem stupně nejvýše k. Dosaďme do tohoto člene polynomy $s_1, s_2, \ldots, s_k$ za proměnné $x_1, x_2, \ldots, x_k$. Tak obdržíme polynom $s_1^{\alpha_1} s_2^{\alpha_2} \cdots s_k^{\alpha_k}$ stupně nejvýše k^2.

Pro každé celé číslo $i \in \{0, 1, 2, \ldots, k^2\}$ označme symbolem r_i polynom, který vznikne tím způsobem, že z polynomu $\bar{q}$ vybereme sumu všech těch jeho členů $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_k^{\alpha_k}$ i s jejich koeficienty, pro něž stupeň polynomu $s_1^{\alpha_1} s_2^{\alpha_2} \cdots s_k^{\alpha_k}$ je roven právě i. Pak jistě platí $\bar{q} = r_0 + r_1 + r_2 + \cdots + r_{k^2}$. Poněvadž $f = \bar{q}(s_1, s_2, \ldots, s_k)$ je homogenní symetrický polynom stupně k, plyne odtud, že pro každé $i \in \{0, 1, 2, \ldots, k-1, k+1, \ldots, k^2\}$ platí $r_i(s_1, s_2, \ldots, s_k) = 0$, zatímco $r_k(s_1, s_2, \ldots, s_k) = f$. Uvažme znovu kterýkoliv člen $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_k^{\alpha_k}$ jednoho z polynomů r_i pro $i \in \{0, 1, 2, \ldots, k^2\}$. Pak dostáváme

$$s_1^{\alpha_1} s_2^{\alpha_2} \cdots s_k^{\alpha_k} = s_k^{\alpha_k} s_{k-1}^{\alpha_{k-1}} \cdots s_1^{\alpha_1} = s_{\mu_1} s_{\mu_2} \cdots s_{\mu_\varkappa},$$

kde $\mu = (\mu_1, \mu_2, \ldots, \mu_\varkappa)$ je ten rozklad čísla i, v němž prvních α_k složek je rovno k, dalších α_{k-1} složek je rovno $k-1$, atd., až posledních α_1 složek je rovno 1. To znamená, že $s_1^{\alpha_1} s_2^{\alpha_2} \cdots s_k^{\alpha_k}$ je polynom p_μ z vektorového prostoru $\Lambda^i_{\mathbb{R}}[x_1, x_2, \ldots, x_n]$. Je tedy polynom $r_i(s_1, s_2, \ldots, s_k)$ lineární kombinací polynomů p_μ pro nějaké rozklady μ čísla i. Přitom koeficienty v této lineární kombinaci jsou koeficienty odpovídajících členů $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_k^{\alpha_k}$ ve vyjádření polynomu r_i. Ovšem poněvadž $i \leqslant n$, podle předchozí věty množina polynomů $\{p_\mu : \mu \vdash i\}$ tvoří bázi vektorového prostoru $\Lambda^i_{\mathbb{R}}[x_1, x_2, \ldots, x_n]$. Je-li tedy $i \neq k$, takže $r_i(s_1, s_2, \ldots, s_k) = 0$, musí všechny koeficienty v dotyčné lineární kombinaci být nulové. To ale znamená, že všechny koeficienty v polynomu r_i jsou nulové, takže r_i je nulový polynom pro všechna $i \in \{0, 1, 2, \ldots, k-1, k+1, \ldots, k^2\}$.

Zbývá tak už jenom polynom r_k, pro nějž platí $r_k(s_1, s_2, \ldots, s_k) = f$. Analogická úvaha jako předtím ukazuje, že pak polynom $r_k(s_1, s_2, \ldots, s_k)$ je nějakou lineární kombinací polynomů p_λ pro některé rozklady λ čísla k. Přitom koeficienty v této lineární kombinaci jsou koeficienty odpovídajících členů $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_k^{\alpha_k}$ ve vyjádření polynomu r_k. Podle předchozí věty ale množina polynomů $\{p_\lambda : \lambda \vdash k\}$ tvoří bázi vektorového prostoru $\Lambda^k_{\mathbb{R}}[x_1, x_2, \ldots, x_n]$. To znamená, že dotyčné koeficienty ve zmíněné lineární kombinaci jsou určeny jednoznačně. Připomeňme znovu, že máme $r_k(s_1, s_2, \ldots, s_k) = f$. Vrátíme-li se nyní k úvahám provedeným v předchozím odstavci tohoto důkazu, vidíme, že tam jsme polynom f vyjádřili jako lineární kombinaci zmíněných polynomů p_λ s jistými koeficienty c_λ, které jsme následně použili v definici polynomu q. Teď z toho, že jsou tyto koeficienty určeny jednoznačně, plyne rovnost polynomů $r_k = q$. Celkem to nakonec dává potřebnou rovnost polynomů $\bar{q} = q$. $\square$