Polynomy více proměnných

Poznámka. V Algebře I jsme k libovolnému okruhu R sestrojili okruh polynomů $R[x]$ nad okruhem R. Tuto konstrukci můžeme opakovat pro okruh $R[x]$ a sestrojit okruh polynomů nad ním, jen musíme odlišit původní a nově zaváděnou proměnnou.

Definice. Nechť R je okruh. Okruhem polynomů dvou proměnných nad okruhem R rozumíme okruh $R[x_1, x_2] = \big(R[x_1]\big)[x_2]$. Dále postupujeme indukcí: pro libovolné přirozené číslo n je okruhem polynomů n proměnných nad okruhem R okruh $R[x_1, \ldots, x_n] = \big(R[x_1, \ldots, x_{n-1}]\big)[x_n]$.

Prvky okruhu $R[x_1, \ldots, x_n]$ nazýváme polynomy n proměnných nad okruhem R, zřejmě je každý takový polynom možné zapsat jako konečný součet sčítanců tvaru $a x_{i_1}^{k_1} x_{i_2}^{k_2} \ldots x_{i_m}^{k_m}$, kde $a \in R$, $0 \leq m \leq n$, $1 \leq i_1 < i_2 < \cdots < i_m \leq n$ a $k_1, \ldots, k_m \in \mathbb{N}$. Pro usnadnění zápisu definujeme $x_i^0 = 1$ pro každé $i = 1, \ldots, n$, pak je tedy tento sčítanec možno psát ve tvaru $a x_1^{r_1} x_2^{r_2} \ldots x_n^{r_n}$, kde $a \in R$ a $r_1, \ldots, r_n \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

Stupeň polynomu více proměnných

Každý polynom $f \in R[x_1, \ldots, x_n]$ lze tedy zapsat jako konečný součet sčítanců tvaru $a x_1^{r_1} x_2^{r_2} \ldots x_n^{r_n}$, kde $a \in R$ a $r_1, \ldots, r_n \in \mathbb{N}_0$. Součinu $x_1^{r_1} x_2^{r_2} \ldots x_n^{r_n}$ říkáme člen, prvku a koeficient tohoto členu.

Je-li $f \neq 0$, lze při zápisu f navíc požadovat, aby se žádný člen neopakoval a koeficienty byly nenulové. V tom případě členy v tomto součtu použité nazýváme členy polynomu f, o použitém koeficientu takového členu mluvíme jako o koeficientu polynomu f u tohoto členu.

Stupněm členu $x_1^{r_1} x_2^{r_2} \ldots x_n^{r_n}$ rozumíme součet $r_1 + \cdots + r_n$.

Stupněm $\operatorname{st} f$ nenulového polynomu f rozumíme největší ze stupnů jeho členů, stupeň nulového polynomu klademe roven $-\infty$.

Mají-li všechny členy polynomu f stejný stupeň, hovoříme o homogenním polynomu (často se homogenním polynomům také říká forma, například lineární forma, kvadratická forma, ...).

Okruh polynomů více proměnných

Každý nenulový polynom $f \in R[x_1, \ldots, x_n]$ je tedy součtem několika členů vybavených koeficienty z okruhu R. Součet $f + g$ dvou takových polynomů provedeme sečtením těchto součtů, pokud nějaký člen je členem obou polynomů, úpravou $ax_1^{r_1}x_2^{r_2}\ldots x_n^{r_n} + bx_1^{r_1}x_2^{r_2}\ldots x_n^{r_n} = (a+b)x_1^{r_1}x_2^{r_2}\ldots x_n^{r_n}$ sečteme příslušné koeficienty v okruhu R. V případě $a + b = 0$ příslušný člen v zápisu polynomu $f + g$ neuvedeme.

Při násobení polynomů roznásobujeme součty užitím distributivního zákona, je tedy pouze třeba si rozmyslet, jak upravit součin $ax_1^{r_1}x_2^{r_2}\ldots x_n^{r_n} \cdot bx_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$. Uvědomme si, že i v případě, kdy okruh R není komutativní, tak v okruhu $R[x]$ platí $a \cdot x = ax = x \cdot a$ pro každé $a \in R$. Každá proměnná tedy komutuje s každou konstantou, tedy v okruhu $R[x_1, \ldots, x_n]$ platí $a \cdot x_i = x_i \cdot a$, $x_j \cdot x_i = x_i \cdot x_j$ pro každé $a \in R$, $i, j \in \{1, \ldots, n\}$. Proto $ax_1^{r_1}x_2^{r_2}\ldots x_n^{r_n} \cdot bx_1^{k_1}x_2^{k_2}\ldots x_n^{k_n} = (a \cdot b)x_1^{r_1+k_1}x_2^{r_2+k_2}\ldots x_n^{r_n+k_n}$.

Součinem homogenních polynomů je homogenní polynom.

Vedoucí člen, vedoucí koeficient

Na množině $\mathbb{N}_0^n$ máme legikografické uspořádání definované takto: pro libovolné n-tice $[r_1, \ldots, r_n], [k_1, \ldots, k_n] \in \mathbb{N}_0^n$ klademe $[r_1, \ldots, r_n] < [k_1, \ldots, k_n]$, právě když existuje $j \in \{1, \ldots, n\}$ tak, že pro každé i, $1 \leq i < j$ platí $r_i = k_i$ a současně $r_j < k_j$.
Pak $[r_1, \ldots, r_n] \leq [k_1, \ldots, k_n]$ znamená $[r_1, \ldots, r_n] < [k_1, \ldots, k_n]$ nebo $[r_1, \ldots, r_n] = [k_1, \ldots, k_n]$.

Zřejmě $(\mathbb{N}_0^n, \leq)$ je řetězec.

Řekneme, že člen $x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ je před členem $x_1^{r_1} x_2^{r_2} \ldots x_n^{r_n}$, jestliže $[r_1, \ldots, r_n] < [k_1, \ldots, k_n]$.

Člen nenulového polynomu $f \in R[x_1, \ldots, x_n]$, který je před všemi ostatními členy polynomu f, se nazývá vedoucí člen polynomu f, jeho koeficientu říkáme vedoucí koeficient polynomu f.

Vedoucí člen ani vedoucí koeficient nulového polynomu nedefinujeme.

Může se stát, že stupeň vedoucího člene polynomu f je menší než stupeň polynomu f.

Vedoucí člen, vedoucí koeficient

Věta. *Nechť* $[r_1, \ldots, r_n] \leq [k_1, \ldots, k_n]$, $[r'_1, \ldots, r'_n] \leq [k'_1, \ldots, k'_n]$. *Pak* $[r_1 + r'_1, \ldots, r_n + r'_n] \leq [k_1 + k'_1, \ldots, k_n + k'_n]$.

Důkaz. Existují $j, j' \in \{1, \ldots, n\}$ tak, že
$r_j < k_j, \quad \forall i : 1 \leq i < j \implies r_i = k_i,$
$r'_{j'} < k'_{j'}, \quad \forall i : 1 \leq i < j' \implies r'_i = k'_i.$
Označme $\ell = \min\{j, j'\}$, pak
$r_\ell + r'_\ell < k_\ell + k'_\ell, \quad \forall i : 1 \leq i < \ell \implies r_i + r'_i = k_i + k'_i,$
což bylo třeba dokázat.

Důsledek. *Nechť* $f, g \in R[x_1, \ldots, x_n]$ *jsou nenulové polynomy. Je-li součin vedoucích koeficientů polynomů* f *a* g *nenulový, je vedoucí člen součinu* $f \cdot g$ *součinem vedoucích členů polynomů* f *a* g.

Poznámka. Pokud alespoň jeden z vedoucích koeficientů není dělitel nuly, je předpoklad o nenulovosti součinu vedoucích koeficientů splněn. Je-li R obor integrity, pak tento předpoklad bude splněn vždy.

Vlastnosti okruhu polynomů více proměnných

Okruh polynomů více proměnných vznikl iterováním konstrukce okruhu polynomů jedné proměnné. Proto některé výsledky o okruzích polynomů jedné proměnné nám dávají důsledky pro okruhy polynomů více proměnných:

Je-li R obor integrity, pak i $R[x_1, \ldots, x_n]$ je oborem integrity.

Máme posloupnost do sebe vnořených podokruhů:
$R \subsetneq R[x_1] \subsetneq R[x_1, x_2] \subsetneq \cdots \subsetneq R[x_1, x_2, \ldots, x_n]$.

Víme, že je-li R okruh s jednoznačným rozkladem, pak i $R[x]$ je okruh s jednoznačným rozkladem, a proto i $R[x_1, \ldots, x_n]$ je okruh s jednoznačným rozkladem.

Speciálně pro každé těleso T je okruh $T[x_1, \ldots, x_n]$ okruhem s jednoznačným rozkladem.

Hodnoty polynomů více proměnných

Je-li R podokruh okruhu K, pak pro libovolné prvky $c_1, \ldots, c_n \in K$ a libovolný polynom $f \in R[x_1, \ldots, x_n]$ máme hodnotu $f(c_1, \ldots, c_n) \in K$ polynomu f v $c_1, \ldots, c_n$.

Je-li K komutativní okruh, pak pro libovolné $c_1, \ldots, c_n \in K$ je zobrazení $\varphi : R[x_1, \ldots, x_n] \to K$ určené předpisem $\varphi(f) = f(c_1, \ldots, c_n)$ homomorfismus okruhů.

Předpoklad, že K je komutativní okruh, lze zeslabit:

Věta. *Nechť R je podokruh okruhu K, nechť $c_1, \ldots, c_n \in K$ splňují*

- *pro každé $a \in R$ a každé $i \in \{1, \ldots, n\}$ platí $a \cdot c_i = c_i \cdot a$,*
- *pro každé $i, j \in \{1, \ldots, n\}$ platí $c_i \cdot c_j = c_j \cdot c_i$.*

Pak zobrazení $\varphi : R[x_1, \ldots, x_n] \to K$ určené předpisem $\varphi(f) = f(c_1, \ldots, c_n)$ je homomorfismus okruhů.

Důkaz. Stačí pro libovolné $a, b \in R$, $r_1, \ldots, r_n, k_1, \ldots, k_n \in \mathbb{N}_0$ si uvědomit, že za těchto předpokladů $ac_1^{r_1} c_2^{r_2} \ldots c_n^{r_n} \cdot bc_1^{k_1} c_2^{k_2} \ldots c_n^{k_n} = (a \cdot b) c_1^{r_1+k_1} c_2^{r_2+k_2} \ldots c_n^{r_n+k_n}$.

Další teorie okruhu polynomů více proměnných

Studium ireducibilních polynomů či ideálů okruhu $R[x_1, \ldots, x_n]$ je podstatně složitější než v případě polynomů jedné proměnné. Přestože je tato teorie potřeba v algebraické geometrii při studiu ploch (tedy množin kořenů polynomů více proměnných), nebudeme ji nyní budovat.

Zaměříme se pouze na jeden aspekt teorie polynomů více proměnných: budeme studovat tzv. symetrické polynomy.

Symetrické polynomy

Definice. Nechť R je okruh. Polynom $f \in R[x_1, \ldots, x_n]$ nazýváme symetrický polynom (n proměnných), jestliže pro libovolnou permutaci α množiny $\{1, \ldots, n\}$ platí $f(x_1, \ldots, x_n) = f(x_{\alpha(1)}, \ldots, x_{\alpha(n)})$.

Poznámka. V předchozí definici znamená $f(x_{\alpha(1)}, \ldots, x_{\alpha(n)})$ hodnotu polynomu f v prvcích $x_{\alpha(1)}, \ldots, x_{\alpha(n)} \in R[x_1, \ldots, x_n]$. Vzhledem k tomu, že R je podokruhem okruhu $R[x_1, \ldots, x_n]$, má tato hodnota smysl. Poznamenejme, že $f(x_1, \ldots, x_n) = f$.

Příklad. Každý konstantní polynom $f \in R$ je symetrický. Polynom $x_1^2 + x_2^2$ je symetrický polynom dvou proměnných, není však symetrický jako polynom tří proměnných.

Věta. *Nechť R je okruh, $f \in R[x_1, \ldots, x_n]$. Polynom f je symetrický, právě když pro každé $i \in \{2, \ldots, n\}$ platí $f(x_i, x_2, \ldots, x_{i-1}, x_1, x_{i+1}, \ldots, x_n) = f$.*

Důkaz. Plyne z toho, že množina transpozic $\{(1,2), (1,3), \ldots, (1,n)\}$ generuje grupu $\mathbb{S}_n$.

Elementární symetrické polynomy

Definice. Nechť R je okruh. Následující polynomy $s_1, \ldots, s_n \in R[x_1, \ldots, x_n]$ nazýváme elementární symetrické polynomy n proměnných:

$$
\begin{aligned}
s_1 &= x_1 + x_2 + \cdots + x_n, \\
s_2 &= x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \cdots + x_{n-1}x_n, \\
&\vdots \\
s_k &= \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} x_{i_1}x_{i_2}\ldots x_{i_k}, \\
&\vdots \\
s_n &= x_1x_2\ldots x_n.
\end{aligned}
$$

Poznámka. Zřejmě jsou elementární symetrické polynomy n proměnných skutečně symetrické polynomy n proměnných. Ukážeme, že naopak jakýkoli symetrický polynom n proměnných lze vyjádřit pomocí nich.

Podokruh symetrických polynomů

Věta. *Nechť R je okruh, $n \in \mathbb{N}$. Pak množina S všech symetrických polynomů n proměnných tvoří podokruh okruhu $R[x_1, \ldots, x_n]$ a platí $R \subseteq S$.*

Důkaz. Konstantní polynomy $a \in R$ jsou symetrické, tedy $R \subseteq S$. Nechť $f, g \in S$ jsou symetrické polynomy. Protože proměnné komutují s libovolným prvkem okruhu R i mezi sebou, pro libovolné $\alpha \in \mathbb{S}_n$ platí
$(f \cdot g)(x_{\alpha(1)}, \ldots, x_{\alpha(n)}) = f(x_{\alpha(1)}, \ldots, x_{\alpha(n)}) \cdot g(x_{\alpha(1)}, \ldots, x_{\alpha(n)}) =$
$= f(x_1, \ldots, x_n) \cdot g(x_1, \ldots, x_n) = (f \cdot g)(x_1, \ldots, x_n)$,
a tedy $f \cdot g \in S$. Proto také $-f = (-1) \cdot f \in S$. Podobně
$(f+g)(x_{\alpha(1)}, \ldots, x_{\alpha(n)}) = f(x_{\alpha(1)}, \ldots, x_{\alpha(n)}) + g(x_{\alpha(1)}, \ldots, x_{\alpha(n)}) =$
$f(x_1, \ldots, x_n) + g(x_1, \ldots, x_n) = (f + g)(x_1, \ldots, x_n)$,
a tedy $f + g \in S$.

Důsledek. *Pro libovolný $h \in R[x_1, \ldots, x_n]$ platí, že hodnota $h(s_1, \ldots, s_n)$ polynomu h v elementárních symetrických polynomech $s_1, \ldots, s_n$ je symetrický polynom.*

Vedoucí člen symetrického polynomu

Poznámka. Elementární symetrické polynomy komutují s konstantními polynomy i mezi sebou. Proto je zobrazení $\Phi : R[x_1, \ldots, x_n] \to S$ určené předpisem $\Phi(f) = f(s_1, \ldots, s_n)$ homomorfismus okruhů.
Naším cílem je ukázat, že Φ je izomorfismus.
Ekvivalentně: každý symetrický polynom je hodnotou právě jednoho polynomu v elementárních symetrických polynomech.

Lemma 1. *Nechť R je okruh a $f \in R[x_1, \ldots, x_n]$, $f \neq 0$, je symetrický polynom n proměnných. Pak vedoucí člen $x_1^{r_1} x_2^{r_2} \ldots x_n^{r_n}$ polynomu f splňuje $r_1 \geq r_2 \geq \cdots \geq r_n$.*

Důkaz. Předpokládejme, že $x_1^{r_1} x_2^{r_2} \ldots x_n^{r_n}$ je člen polynomu f, přičemž platí $r_i < r_{i+1}$ pro nějaké $i \in \{1, \ldots, n-1\}$. Protože f je symetrický, aplikací transpozice $(i, i+1)$ dostaneme, že f má také člen

$$x_1^{r_1} \ldots x_{i-1}^{r_{i-1}} x_i^{r_{i+1}} x_{i+1}^{r_i} x_{i+2}^{r_{i+2}} \cdots x_n^{r_n},$$

který je před členem $x_1^{r_1} x_2^{r_2} \ldots x_n^{r_n}$. Člen $x_1^{r_1} x_2^{r_2} \ldots x_n^{r_n}$ není vedoucí.

Zobrazení Φ je surjektivní

Lemma 2. *Homomorfismus Φ je surjekce, tj. pro každý symetrický polynom $f \in R[x_1, \ldots, x_n]$ existuje polynom $h \in R[x_1, \ldots, x_n]$ tak, že $\Phi(h) = f$.*

Důkaz. Je-li $f = 0$, věta platí pro $h = 0$. Předpokládejme, že $f \neq 0$.

Podle lemmatu 1 vedoucí člen $x_1^{r_1} x_2^{r_2} \ldots x_n^{r_n}$ polynomu f splňuje $r_1 \geq r_2 \geq \cdots \geq r_n$. Označme $t = s_1^{r_1 - r_2} s_2^{r_2 - r_3} \ldots s_{n-1}^{r_{n-1} - r_n} s_n^{r_n}$. Protože vedoucí člen polynomu s_k je $x_1 \ldots x_k$, je vedoucí člen polynomu t roven $x_1^{r_1} x_2^{r_2} \ldots x_n^{r_n}$, tedy stejný jako polynomu f. Označíme-li a vedoucí koeficient polynomu f, je $g = f - at$ symetrický polynom. Pokud $g \neq 0$, je vedoucí člen polynomu f před vedoucím členem polynomu g. Protože $at = \Phi(a x_1^{r_1 - r_2} x_2^{r_2 - r_3} \ldots x_{n-1}^{r_{n-1} - r_n} x_n^{r_n})$, z platnosti věty pro polynom g plyne její platnost pro polynom f.

Protože za vedoucím členem polynomu t podle lemmatu 1 může být jen konečně mnoho vedoucích členů symetrických polynomů, po konečně mnoha těchto redukcích dostaneme nulový polynom.

Zobrazení Φ je injektivní

Lemma 3. *Homomorfismus Φ je injekce.*

Důkaz. Ukážeme, že $\ker \Phi = \{0\}$, a to tak, že pro libovolný nenulový $h \in R[x_1, \ldots, x_n]$ dokážeme, že platí $\Phi(h) \neq 0$.

Pro každý člen $x_1^{r_1} x_2^{r_2} \ldots x_n^{r_n}$ je $\Phi(x_1^{r_1} x_2^{r_2} \ldots x_n^{r_n}) = s_1^{r_1} s_2^{r_2} \ldots s_n^{r_n}$. Vedoucí člen tohoto polynomu je $x_1^{r_1+r_2+\cdots+r_n} x_2^{r_2+r_3+\cdots+r_n} \ldots x_{n-1}^{r_{n-1}+r_n} x_n^{r_n}$.

Pro různé n-tice $[r_1, \ldots, r_n]$ a $[k_1, \ldots, k_n]$ tedy platí, že vedoucí členy polynomů $\Phi(x_1^{r_1} x_2^{r_2} \ldots x_n^{r_n})$ a $\Phi(x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n})$ jsou různé.

Nechť $x_1^{t_1} x_2^{t_2} \ldots x_n^{t_n}$ je ten člen polynomu h, jehož obraz v homomorfismu Φ má vedoucí člen před vedoucími členy obrazů ostatních členů. Pak vedoucí člen polynomu $\Phi(x_1^{t_1} x_2^{t_2} \ldots x_n^{t_n})$ je vedoucím členem polynomu $\Phi(h)$. Je proto $\Phi(h) \neq 0$.

Hlavní věta o symetrických polynomech

Věta. *Nechť R je okruh a $f \in R[x_1, \ldots, x_n]$ je symetrický polynom n proměnných. Pak existuje právě jeden polynom $h \in R[x_1, \ldots, x_n]$ splňující $\Phi(h) = f$, tj. $f = h(s_1, \ldots, s_n)$.*

Důkaz. Plyne z lemmat 2 a 3.

Protože důkaz lemmatu 2 je konstruktivní, dostáváme algoritmus na vyjadřování symetrického polynomu pomocí elementárních symetrických polynomů. Využijeme při něm i následující větu.

Věta. *Každý symetrický polynom je součtem několika homogenních symetrických polynomů.*

Důkaz. Plyne z toho, že pro každou permutaci α stupeň členu $x_1^{t_1} x_2^{t_2} \ldots x_n^{t_n}$ a členu $x_{\alpha(1)}^{t_1} x_{\alpha(2)}^{t_2} \ldots x_{\alpha(n)}^{t_n}$ je stejný. Proto součet členů daného symetrického polynomu pevně zvoleného stupně tvoří symetrický polynom.

Algoritmus

Je dán nenulový symetrický polynom $f \in R[x_1, \ldots, x_n]$.
Lze předpokládat, že f je homogenní stupně $s = \operatorname{st} f$
(jinak f napíšeme jako součet několika homogenních symetrických polynomů a každý sčítanec vyjadřujeme zvlášť).
Nechť $x_1^{r_1} x_2^{r_2} \ldots x_n^{r_n}$ je vedoucí člen polynomu f.
Víme, že $r_1 \geq r_2 \geq \cdots \geq r_n$, $r_1 + r_2 + \cdots + r_n = s$.
Vypíšeme všechny n-tice $[k_1, \ldots, k_n] \in \mathbb{N}_0^n$, které jsou lexikograficky menší než $[r_1, \ldots, r_n]$ a které splňují
$k_1 \geq k_2 \geq \cdots \geq k_n$, $k_1 + k_2 + \cdots + k_n = s$.
Nechť a je vedoucí koeficient polynomu f. Pak pro každou vypsanou n-tici $[k_1, \ldots, k_n]$ existuje $a_{[k_1,\ldots,k_n]} \in R$ tak, že platí

$$f = a s_1^{r_1 - r_2} \ldots s_{n-1}^{r_{n-1} - r_n} s_n^{r_n} + \sum_{[k_1,\ldots,k_n]} a_{[k_1,\ldots,k_n]} s_1^{k_1 - k_2} \ldots s_{n-1}^{k_{n-1} - k_n} s_n^{k_n}.$$

Koeficienty $a_{[k_1,\ldots,k_n]}$ určíme metodou neurčitých koeficientů: obě strany rovnosti jsou polynomy. Každým dosazením za proměnné dostaneme lineární rovnici pro neznámé koeficienty.