

Algoritmy na polynomech, cvičení 3

borysek@karlin.mff.cuni.cz

<https://karlin.mff.cuni.cz/~borysek/>

30. října 2025

1 Teoretická část

1. Mějme $I = \langle f_1, f_2, \dots, f_n \rangle$ ideál v $T[x_1, \dots, x_k]$ a nějaké přípustné uspořádání na termtech a odvozené ostré uspořádání na polynomech $\gg$ v $T[x_1, \dots, x_k]$. Dále mějme faktor $R = T[x_1, \dots, x_k]/I$. Uvědomte si, že pro každou rozkladovou třídu $g+I \in R$ existuje právě jeden prvek $h \in T[x_1, \dots, x_k]$ tak, že $g+I = h+I$ a h je terminál vůči $\gg$. Navíc si uvědomte, jak lze výše uvedený prvek h s pomocí Gröbnerovy báze najít. (Speciálně si uvědomte, že pokud $g_1 \xrightarrow[\ast]{I} g_2$, pak $g_1 + I = g_2 + I$.)

2. Najděte normovanou redukovanou Gröbnerovu bázi ideálu

$$\langle xy - x + 1, xy^2 + y \rangle \leq \mathbb{Q}[x, y]$$

pro $\leq_{\text{GLEX}}, x > y$. Patří $x^3y^2 - 2xy + 3x$ do tohoto ideálu?

3. Najděte normovanou redukovanou Gröbnerovu bázi ideálu

$$\langle x^2 - y, xy - 1 \rangle \leq \mathbb{Q}[x, y]$$

pro $\leq_{\text{LEX}}, x > y$. Patří $2y^3 - x + 3$ do tohoto ideálu?

4. Necht $I = \langle f_1, \dots, f_n \rangle$, $J = \langle g_1, \dots, g_m \rangle$ jsou ideály z $T[x_1, \dots, x_k]$. Dokažte:

(a) $I + J = \langle f_1, \dots, f_n, g_1, \dots, g_m \rangle$,

(b) $IJ = \langle f_i g_j \mid 1 \leq i \leq n, 1 \leq j \leq m \rangle$,

(c) $I \cap J = (zI + (1-z)J) \cap T[x_1, \dots, x_k]$, kde z je nová proměnná a zI a $(1-z)J$ chápeme jako ideály v $(T[x_1, \dots, x_k])[z]$ generované množinami zI a $(1-z)J$. Tedy dle předchozí části jako $zI = \langle z f_1, \dots, z f_n \rangle_{T[x_1, \dots, x_k, z]}$ a analogicky $(1-z)J$.

5. Necht jsou I, J ideály v $T[x_1, \dots, x_k]$, dokažte:

(a) $V(I) \cap V(J) = V(I + J)$,

(b) $V(I) \cup V(J) = V(IJ)$.

Na základě těchto pozorování formulujte algoritmus, který pro dané algebraické množiny A, B a jejich algebraická vyjádření $A = V(f_1, \dots, f_n)$ a $B = V(g_1, \dots, g_m)$ spočítá algebraické vyjádření $A \cap B$ a $A \cup B$.

6. Dokažte, že R je Gröbnerova báze ideálu $I = \langle R \rangle$ právě tehdy, když $\langle \text{lt}(R) \rangle = \langle \text{lt}(I) \rangle$. Rozumí se $\text{lt}(U) = \{\text{lt}(u) : u \in U\}$. Dokažte tuto větu bez použití věty 21.1. Může se hodit dokázat nejprve tvrzení 7.
7. Necht $R \subseteq T[x_1, \dots, x_n]$. Necht pro každý polynom $f \in \langle R \rangle$ platí $f \xrightarrow[\ast]{R} 0$. Dokažte, že pak R je Gröbnerova báze ideálu $\langle R \rangle$. Dokažte tohle tvrzení bez použití věty 21.1.
8. Ukažte, že $T[x_1, x_2, \dots, x_k]$ není obor hlavních ideálů pro $k \geq 2$, a tedy že speciálně zde nutně neplatí rovnost, která platí v $T[x]$, tedy $\langle f, g \rangle = \langle \text{gcd}(f, g) \rangle$.
9. Necht T je algebraicky uzavřené těleso a necht $f \in T[x, y]$. Ukažte, že pak $V(f)$ je buď prázdná, nebo nekonečná.

10. (a) Necht' T je těleso a $M \in T^{m \times n}$ je matice. Ukažte, že $\text{rank}(M) = k \iff M$ obsahuje regulární $k \times k$ podmatici a neobsahuje žádnou větší takovou.
- (b) Necht' $T \leq S$ jsou tělesa, $M \in T^{m \times n}$, $b \in T^m$ a necht' má soustava lineárních rovnic $Mx = b$ řešení nad S . Ukažte, že pak má řešení i nad T .
- (c) Necht' $f_1, \dots, f_k \in T[x_1, \dots, x_m]$, $T \leq S$ tělesa a $s_1, \dots, s_k \in S$ tak, že $\sum_{i=1}^k s_i f_i = 1$. Platí potom, že existují $t_1, \dots, t_k \in T$ tak, že:

$$\sum_{i=1}^k t_i f_i = 1?$$

(Pozn. s_i i t_i jsou prvky příslušného tělesa, nikoli polynomy.)

- (d) Necht' $T \leq S$ jsou tělesa. Necht' $g, f_1, \dots, f_n \in T[x_1, \dots, x_k]$ a necht' existují $h_1, \dots, h_n \in S[x_1, \dots, x_k]$ tak, že $\sum_{i=1}^n h_i f_i = g$. Ukažte, že pak existují $c_1, \dots, c_n \in T[x_1, \dots, x_k]$ tak, že $\sum_{i=1}^n c_i f_i = g$. Tedy že pokud $g \in \langle f_1, \dots, f_n \rangle_{S[x_1, \dots, x_k]}$, pak i $g \in \langle f_1, \dots, f_n \rangle_{T[x_1, \dots, x_k]}$.
- (e) Dokažte část 10d bez použití Gröbnerovýchází.

2 Výpočetní část

1. Zopakujte si, jakým způsobem funguje uspořádání na termech v **SageMath**.
https://doc.sagemath.org/html/en/reference/polynomial_rings/sage/rings/polynomial/term_order.html
2. Nastudujte si, jakým způsobem fungují ideály a Gröbnerovy báze v **SageMath**.
https://doc.sagemath.org/html/en/reference/polynomial_rings/sage/rings/polynomial/multi_polynomial_ideal.html
3. Ověřte 2, 3 pomocí **SageMath**.
4. Své výsledky samotného Buchbergerova algoritmu u 2, 3 si můžete ověřit také pomocí **SageMath**.
https://doc.sagemath.org/html/en/reference/polynomial_rings/sage/rings/polynomial/toy_buchberger.html