

# Algoritmy na polynomech, cvičení 4

borysek@karlin.mff.cuni.cz

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

13. listopadu 2025

1. 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  $(1 - z)J$ .

2. 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  $A \cup B$ .

3. Necht  $R$  je Gröbnerova báze ideálu  $I < T[x_1, \dots, x_k]$  vůči  $<_{LEX} x_1 < \dots < x_k$ . Eliminační lemma říká, že pro každé  $i = 1, \dots, k$  je

$$I \cap T[x_1, \dots, x_i] = \langle R \cap T[x_1, \dots, x_i] \rangle_{T[x_1, \dots, x_i]}.$$

Dokažte, že  $R \cap T[x_1, \dots, x_i]$  je navíc Gröbnerova báze ideálu  $I \cap T[x_1, \dots, x_i]$ .

4. Kolik řešení má následující soustava v  $\mathbb{Q}$  a v  $\mathbb{C}$ ? Řešte pomocí Gröberových bazí. Můžete si pomoci SageMath.

(a)

$$\begin{aligned} 1 + 2x^2 + y^2 + 4x^2y^2 + 2x^2y^4 &= 0 \\ xy^2 + xy^4 &= 0. \end{aligned}$$

(b)

$$\begin{aligned} x^2 - 2xy^2 + 1 &= 0 \\ xy - 2y^2 + x &= 0. \end{aligned}$$

5. Nalezněte všechna řešení nad  $\mathbb{Q}$  následující soustavy. Řešte pomocí Gröberových bazí s  $<_{LEX} x < y < z$ . Můžete si pomoci SageMath.

$$\begin{aligned} xy^2 - y^2 - xy + y + x^2 - x &= 0 \\ yz + xy^2 - y^2 - xy + y - 1 &= 0 \\ yz - 1 &= 0 \end{aligned}$$

6. 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  $\sum_{i=1}^n h_i f_i = g$ . S pomocí Gröbnerových bazí dokažte, 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  $g \in \langle f_1, \dots, f_n \rangle_{T[x_1, \dots, x_k]}$ . Speciálně  $1 \in \langle f_1, \dots, f_n \rangle_{S[x_1, \dots, x_k]} \iff 1 \in \langle f_1, \dots, f_n \rangle_{T[x_1, \dots, x_k]}$ .

7. Necht'  $T \leq S$  jsou tělesa a necht' navíc  $T$  je algebraicky uzavřené. Mějme  $f_1, \dots, f_n \in T[x_1, \dots, x_k]$ . Ukažte, že je-li  $V(f_1, \dots, f_n)_T = \emptyset$ , pak i  $V(f_1, \dots, f_n)_S = \emptyset$ . Tedy pokud soustava nemá řešení v algebraicky uzavřeném tělese, pak nemá řešení v žádném jiném nadtělese.

8. Ukažte, že problém určit zda polynom  $p(\bar{x})$  náleží danému ideálu  $I \leq \mathbb{Q}[\bar{x}]$  je NP-těžký, pomocí redukce SATu na tento problém. Náповěda: Nejprve si to rozmyslete pro situaci v  $\mathbb{C}[\bar{x}]$  a z toho odvoďte, i situaci v  $\mathbb{Q}[\bar{x}]$ . Může se hodit Důsledek 22.3 ze skript.

**Poznámka.** Poznamenejme, že problém nálezení ideálu je dokonce EXPSPACE-úplný, a proto neleží v NP.

9. Necht'  $T$  je algebraicky uzavřené těleso,  $R \subset T[x_1, \dots, x_k]$  Gröbnerova báze vzhledem k  $<_{LEX}$  s  $x_1 < \dots < x_k$ . Dokažte, že pak  $V(R)$  je konečná  $\iff$  pro každé  $i = 1, \dots, k$  existuje polynom  $f_i \in R$  tak, že  $\text{lt}(f_i) = x_i^n$  pro nějaké  $n \in \mathbb{N}_0$  (speciálně  $f \in T[x_1, \dots, x_i]$ ). Pozn.  $\Rightarrow$  je náročnější.

10. Necht'  $T$  je těleso a  $A \subset T^k$  konečná. Ukažte, že pak existují polynomy  $f_1, \dots, f_k$  tak, že  $f_i \in T[x_1, \dots, x_i]$  a  $A = V(f_1, \dots, f_k)$ . Tedy  $A$  lze popsat jako řešení soustavy rovnic

$$\begin{aligned} f_1(x_1) &= 0 \\ f_2(x_1, x_2) &= 0 \\ &\vdots \\ f_k(x_1, x_2, \dots, x_k) &= 0 \end{aligned}$$

Náповěda: interpolace ve více proměnných.

11. (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) Bez použití Gröbnerovýchází dokažte cvičení 6.