12. cvičení

Ve škole:

1. (Eisensteinovo kriterium) Nechť $a = \sum_{i=1}^{n} a_i x^i \in \mathbb{Z}[x]$ splňuje podmínku $\mathrm{NSD}(a_0, \ldots, a_n) = 1$ a nechť prvočíslo p dělí a_i pro všechna $i = 0, \ldots, n-1$ a p^2 nedělí a_0. Dokažte, že je polynom a v $\mathbb{Z}[x]$ ireducibilní.

2. Dokažte, že jsou v $\mathbb{Z}[x]$ ireducibilní polynomy
(a) $x^8 - 12$, (b) $2x^5 + 9x^3 - 6$, (c) $x^6 + 10x^5 - 4x^3 + 8x^2 - 2$.

3. Buď $\mathbf{R}$ obor, $f \in \mathbf{R}[x]$ a $a \in \mathbf{R}$. Dokažte, že je f ireducibilní v $\mathbf{R}[x]$ právě tehdy, když je $f(x+a)$ ireducibilní v $\mathbf{R}[x]$.

4. Dokažte, že jsou v $\mathbb{Z}[x]$ ireducibilní polynomy
(a) $x^6 + x^3 + 1$, (b) $x^{p-1} + x^{p-2} + \ldots + x + 1 = \frac{x^p - 1}{x-1}$ pro prvočíslo p.

Úlohy pro samostatné počítání:

5. Najděte generátor u všech ideálů, které jsou hlavní:
(a) $15\mathbb{Z} + 24\mathbb{Z}$ v $\mathbb{Z}$,
(b) $15\mathbb{Z} \cap 24\mathbb{Z}$ v $\mathbb{Z}$,
(c) $3\mathbb{Z}[x] + x\mathbb{Z}[x]$ v $\mathbb{Z}[x]$,
(d) $3\mathbb{Z}[x] \cap x\mathbb{Z}[x]$ v $\mathbb{Z}[x]$.

6. Pro každé $a, b \in \mathbb{Z}$ dokažte, že $\mathrm{NSD}(a,b)\mathbb{Z}$ je vzhledem k inkluzi nejmenší ideál okruhu celých čísel $\mathbb{Z}$ obsahující ideály $a\mathbb{Z}$ i $b\mathbb{Z}$ a že $\mathrm{NSN}(a,b)\mathbb{Z}$ je největší ideál okruhu $\mathbb{Z}$ obsažený v ideálech $a\mathbb{Z}$ i $b\mathbb{Z}$. Platí obdobné tvrzení v každém eukleidovském oboru?

Řešení:

1. Nechť $a = b \cdot c$, kde $b = \sum_{i=1}^{r} b_i x^i, c = \sum_{i=1}^{s} c_i x^i \in \mathbb{Z}[x]$. Pokud $\deg b = 0$, pak $b = b_0 x^0$ a $a = \sum_{i=1}^{s} b_0 c_i x^i$, proto b_0 dělí $\mathrm{NSD}(a_1, \ldots, a_n) = 1$, tedy $b = \pm 1$ je invertibilní polynom (symetricky pro c).

   Předpokládejme, že $\deg b > 0$ a $\deg c > 0$. Potom $\deg c < n$ a $\deg b < n$, a protože p dělí $a_0 = b_0 c_0$ a p^2 nedělí $a_0 = b_0 c_0$ platí, že buď p dělí b_0 a nedělí c_0 nebo p dělí c_0 a nedělí b_0, bez újmy na obecnosti předpokládejme, že p dělí b_0 a nedělí c_0. Indukcí dokážeme, že p dělí b_i pro všechna $i = 0, \ldots, r < n$. Pro $i = 0$ tvrzení předpokládáme. Nechť $i < n$ a p dělí b_j pro všechna $j = 0, \ldots, i-1$. Protože $a_i = \sum_{j=0}^{i} b_j c_{i-j}$ a p dělí a_i podle předpokladu, platí, že

   $$p \ \text{ dělí } \ (a_i - \sum_{j=0}^{i-1} b_j c_{i-j}) = b_i c_0.$$

   Protože p podle předpokladu nedělí c_0, musí dělit b_i. Protože p dělí všechny koeficienty b, dělí i všechny koeficienty $a = b \cdot c$, což je spor s předpokladem $\mathrm{NSD}(a_1, \ldots, a_n) = 1$.

2. Použijeme Eisensteinovo kriterium pro (a),(b) $p = 3$, (c) $p = 2$

3. Dokazujeme nepřímo: nechť $f(x) = g(x)h(x)$ pro neinvertibilní polynomy g a h, pak $f(x+a) = g(x+a)h(x+a)$. Obrácenou implikaci dostaneme použitím dokázaného tvrzení pro polynom $g(x) := f(x+a)$ a $g(x + (-a))$.

4. (a) Použijeme Eisensteinovo kriterium pro $(x+1)^6 + (x+1)^3 + 1 = x^6 + 6x^5 + 15x^4 + 21x^3 + 18x^2 + 9x + 3$ a prvočíslo 3,

   (b) použijeme Eisensteinovo kriterium pro $\frac{(x+1)^p - 1}{(x+1)-1} = \sum_{i=1}^{p} \binom{p}{i} x^{i-1}$ a prvočíslo p,

5. (a) $3 = \mathrm{NSD}(15, 24)$,

   (b) $120 = \mathrm{NSN}(15, 24)$,

   (c) Není hlavní: případný generátor hlavního ideálu by byl společný dělitel 3 a x v oboru $\mathbb{Z}[x]$, tedy 1 nebo -1, ovšem $\pm 1 \notin 3\mathbb{Z}[x] + x\mathbb{Z}[x]$,

   (d) $3x$.

6. Nejprve si všimněme, že $u/v \Leftrightarrow v\mathbb{Z} \subseteq u\mathbb{Z}$. Je-li $c := \mathrm{NSD}(a, b)$ a $d\mathbb{Z}$ ideál obsahující $a\mathbb{Z} \cup b\mathbb{Z}$ ($\mathbb{Z}$ je obor hlavních ideálů), pak $d/a, b$, a protože je d největší společný dělitel, dostáváme, že d/c, a proto $c\mathbb{Z} \subseteq d\mathbb{Z}$.

   Duálně, jestliže $g := \mathrm{NSN}(a, b)$ a $h\mathbb{Z} \subseteq a\mathbb{Z} \cap b\mathbb{Z}$, pak $a, b/g$, a protože je h nejmenší společný násobek, dostáváme, že g/h a $h\mathbb{Z} \subseteq g\mathbb{Z}$.

   Úvaha projde v jakémkoli Eukleidovském oboru (dokonce i v OIHI).