Cvičení I

Úloha 1 (oblíbené chyby ve zkouškových písemkách)**.** Opravte následující výroky:

(a) 143 je prvočíslo.
(b) 187 je prvočíslo.
(c) 91 je prvočíslo.
(d) 343 je prvočíslo.
(e) Ideál v komutativním okruhu je podmnožina uzavřená na $+$, $-$ a násobení libovolnými prvky okruhu.
(f) Ireducibilním rozkladem x rozumíme zápis $x = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, kde p_i jsou ireducibilní po dvou neasociované a $e_i \in \mathbb{N}$.
(g) Podobor euklidovského oboru je vždy euklidovský.
(h) Podobor oboru hlavních ideálů je vždy obor hlavních ideálů.
(i) Podobor Gaussova oboru je vždy Gaussův.

Řešení. $143 = 11 \cdot 13$, $187 = 11 \cdot 17$, $91 = 7 \cdot 13$, $343 = 7^3$. Ideál musí být neprázdný, v ireducbilním rozkladu v této podobě požadujeme jen asociovanost (tj. $x \parallel p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$). Každý obor je podoborem svého podílového tělesa, které je euklidovské i OHI i Gaussovo, ovšem existují obory, které nejsou euklidovské / OHI / Gaussovy. □

Vsuvka (kterak počítat NSD ve „složitějších“ oborech aneb Věta 56 (1) z Algebry I)**.** R, Q jako výše, $f, g \in R[x]$. Pak $\mathrm{NSD}_{R[x]}(f, g)$ existuje a $\mathrm{NSD}_{R[x]}(f, g) = c \cdot d$, kde $c = \mathrm{NSD}_R(\mathrm{c}(f), \mathrm{c}(g))$, $d = \mathrm{NSD}_{Q[x]}(f, g)$, $d \in R[x]$ primitivní.

☼ **Úloha 2.** Nalezněte $\mathrm{NSD}_R(f, g)$, je li

(a) $f = 6x^2 - 12x - 18$, $g = 8x^3 + 16x^2 - 8x - 16$, $R = \mathbb{Z}[x]$,
(b) $f = x^2 - y^2$, $g = x^2 + 2xy + y^2$, $R = \mathbb{C}[x, y]$,
(c) $f = x^3 + x^2 + x + x^2y + xy + y^2 + 1$, $g = x^3 + x + x^2y^2 + xy + y^3 + y^2$, $R = \mathbb{Z}_2[x, y]$.[1]

Řešení. (a) Postupujme podle Vsuvky – rozdělení rolí: $R = \mathbb{Z}$, $Q = \mathbb{Q}$. Je $\mathrm{c}(f) = 6$, $\mathrm{c}(g) = 8$, takže c ze Vsuvky je $\mathrm{NSD}_{\mathbb{Z}}(6, 8) = 2$. Nyní potřebujeme spočítat $\mathrm{NSD}_{\mathbb{Q}[x]}(f, g)$, což se udělá libovolnou metodou – rozkladem na ireducibilní faktory, Euklidovým algoritmem atd. Protože prvky $\mathbb{Q}$ jsou v $\mathbb{Q}[x]$ invertibilní, můžeme stejně dobře počítat jen $\mathrm{NSD}_{\mathbb{Q}[x]}(\frac{1}{6}f, \frac{1}{8}g)$, čímž zpřehledníme výpočet. Je

$$x^3 + 2x^2 - x - 2 = (x + 4)(x^2 - 2x - 3) + (10x + 10),$$

dle Euklida tedy

$$\mathrm{NSD}_{\mathbb{Q}[x]}(x^2 - 2x - 3, x^3 + 2x^2 - x - 2) = \mathrm{NSD}_{\mathbb{Q}[x]}(x^2 - 2x - 3, 10x + 10)$$

a $x^2 - 2x - 3$ už je dělitelné $10x + 10$ v $\mathbb{Q}[x]$, tedy $d' = 10x + 10$ je největší společný dělitel v $\mathbb{Q}[x]$. Hledané d ze vsuvky má být prvkem $\mathbb{Z}[x]$ a ještě k tomu primitivní, což splňuje jen a pouze $d = \frac{1}{10}d' = x + 1$. Hledané $\mathrm{NSD}_{\mathbb{Z}[x]}(f, g)$ tedy je $c \cdot d = 2(x + 1)$.

Alternativní přístup je, že f a g přímo v $\mathbb{Z}[x]$ rozložíme na ireducibilní prvky; tyto rozklady jsou

$$f = 2 \cdot 3 \cdot (x + 1) \cdot (x - 3), \quad g = 2^3 \cdot (x + 1) \cdot (x - 1) \cdot (x + 2).$$

Snadno se nahlédne, že prvočísla a primitivní lineární dvojčleny jsou ireducibilní v $\mathbb{Z}[x]$, a jelikož jediné invertibilní prvky v $\mathbb{Z}[x]$ jsou ± 1, žádné činitele nejsou asociované a jde tedy vskutku o ireducibilní rozklady. Dle standardního SŠ postupu pro výpočet NSD tedy je $\mathrm{NSD}_{\mathbb{Z}[x]}(f, g) = 2 \cdot (x + 1)$.

(b) Postup dle Vsuvky: na $\mathbb{C}[x, y]$ můžeme nahlížet jako na $\mathbb{C}[x][y]$, nebo jako na $\mathbb{C}[y][x]$; zvolme si třeba druhou variantu. Potom je $R = \mathbb{C}[y]$ (komplexní polynomy v y) a $Q = \mathbb{C}(y)$ (komplexní racionální funkce v y, tj. podílové těleso $\mathbb{C}[y]$). Potom je $\mathrm{c}(f) = \mathrm{NSD}_{\mathbb{C}[y]}(1, -y^2) = 1$ a $\mathrm{c}(g) = \mathrm{NSD}_{\mathbb{C}[y]}(1, 2y, y^2) = 1$, takže $c = 1$. Zbývá najít $\mathrm{NSD}_{\mathbb{C}(y)[x]}(f, g)$, což lze opět udělat rozličně; z pedagogických důvodů zkusme opět Euklida. Je

$$x^2 + 2xy + y^2 = 1 \cdot (x^2 - y^2) + 2xy + 2y^2,$$

takže

$$\mathrm{NSD}_{\mathbb{C}(y)[x]}(x^2 - y^2, x^2 + 2xy + y^2) = \mathrm{NSD}_{\mathbb{C}(y)[x]}(x^2 - y^2, 2xy + 2y^2)$$

[1] V zadání vytištěném na cvičení chyběl člen y^2 v g.

a protože $2xy + 2y^2$ dělí $x^2 - y^2$ v $\mathbb{C}(y)[x]$,[2] je $d' = \mathrm{NSD}_{\mathbb{C}(y)[x]}(f,g) = 2xy + 2y^2$. Z tohoto potřebujeme vyrobit primitivní polynom náležící do $\mathbb{C}[y][x]$, kterým je přesně $d = \frac{1}{2y}d' = x + y$. Závěrem tedy $\mathrm{NSD}_{\mathbb{C}[x,y]}(f,g) = \mathrm{NSD}_{\mathbb{C}[y][x]}(f,g) = x + y$.

V tomto případě je jinak určitě rychlejší přímo f a g rozložit.

$$f = (x+y)\cdot(x-y), \quad g = (x+y)^2,$$

dle Úlohy 3 jsou všechny faktory ireducibilní v $\mathbb{C}[x,y]$ a $\mathrm{NSD}_{\mathbb{C}[x,y]}(f,g) = x + y$.

(c) Postup podle Vsuvky, varianta $\mathbb{Z}_2[x,y] = \mathbb{Z}_2[y][x]$: $R = \mathbb{Z}_2[y]$, $Q = \mathbb{Z}_2(y)$. Jak f, tak g jsou monické jakožto prvky $\mathbb{Z}_2[y][x]$, tedy stejně jako v (b) máme $c = 1$. Pro přehlednost si napišme f a g jako „polynomy v x“:

$$f = x^3 + (y+1)x^2 + (y+1)x + (y^2+1), \quad g = x^3 + y^2x^2 + (1+y)x + (y^3+y^2).$$

Dále použijeme Euklidův algoritmus; jelikož jsou oba polynomy monické stejného stupně, v prvním kroku přičteme g k f.

$$\begin{aligned}\mathrm{NSD}_{\mathbb{Z}_2(y)[x]}(f,g) &= \mathrm{NSD}_{\mathbb{Z}_2(y)[x]}(f, f+g) = \\ &= \mathrm{NSD}_{\mathbb{Z}_2(y)[x]}\big(x^3 + (y+1)x^2 + (y+1)x + (y^2+1), (y^2+y+1)x^2 + (y^3+1)\big).\end{aligned}$$

Nyní využijeme toho, že $y^2 + y + 1$ je jakožto prvek $\mathbb{Z}_2(y)[x]$ invertibilní (patří do tělesa $\mathbb{Z}_2(y)$), zároveň nám hraje do karet $y^3 + 1 = (y+1)(y^2+y+1)$, můžeme tedy $f + g$ podělit $y^2 + y + 1$ a je tedy

$$\mathrm{NSD}_{\mathbb{Z}_2(y)[x]}(f,g) = \mathrm{NSD}_{\mathbb{Z}_2(y)[x]}\big(x^3 + (y+1)x^2 + (y+1)x + (y^2+1), \underbrace{x^2 + (y+1)}_{h}\big).$$

Když nyní budeme f dělit h, vyjde to beze zbytku:

$$x^3 + (y+1)x^2 + (y+1)x + (y^2+1) = \big(x^2 + (y+1)\big)\big(x + (y+1)\big).$$

Vidíme tedy, že $d' = \mathrm{NSD}_{\mathbb{Z}_2(y)[x]}(f,g) = x^2 + y + 1$, což už je i prvek $\mathbb{Z}_2[y][x]$ a je tam i primitivní (protože je monický), takže $d = d'$ a $\mathrm{NSD}_{\mathbb{Z}_2[x,y]}(f,g) = \mathrm{NSD}_{\mathbb{Z}_2[y][x]}(f,g) = x^2 + y + 1$.

Postup podle Vsuvky, varianta $\mathbb{Z}_2[x,y] = \mathbb{Z}_2[x][y]$: $R = \mathbb{Z}_2[x]$, $Q = \mathbb{Z}_2(x)$. I zde platí $c = 1$. Přepíšeme

$$f = y^2 + (x^2+x)y + (x^3+x^2+x+1), \quad g = y^3 + (x^2+1)y^2 + xy + (x^3+x).$$

Vidíme, že volba $\mathbb{Z}_2[x,y] = \mathbb{Z}_2[x][y]$ je *heuristicky lepší* než ta v předchozím odstavci, protože f je jakožto polynom v y stupně jen 2, proto je jasné, že Euklidův algoritmus dá odpověď po nejvýše dvou krocích.[3] Vydělíme tedy v $\mathbb{Z}_2(x)[y]$ se zbytkem polynom g polynomem f:

$$\begin{array}{rl}
y^3 + (x^2+1)y^2 + xy + (x^3+x) & : y^2 + (x^2+x)y + (x^3+x^2+x+1) = y + (x+1). \\
+\big(y^3 + (x^2+x)y^2 + (x^3{+}x^2{+}x{+}1)y\big) & \\
\hline
= (x+1)y^2 + (x^3+x^2+1)y + (x^3+x) & \\
+\big((x+1)y^2 + (x^3+x)y + (x^4+1)\big) & \\
\hline
= (x^2+x+1)y + (x^4{+}x^3{+}x{+}1) &
\end{array}$$

Je tedy

$$\mathrm{NSD}_{\mathbb{Z}_2(x)[y]}(f,g) = \mathrm{NSD}_{\mathbb{Z}_2(x)[y]}\big((x^2+x+1)y + (x^4+x^3+x+1), y^2 + (x^2+x)y + (x^3+x^2+x+1)\big)$$

a můžeme dále využít toho, že v $\mathbb{Z}_2(x)$ je $(x^2+1)(x^2+x+1) = x^4+x^3+x+1$, proto je první z polynomů v $\mathbb{Z}_2(x)[y]$ asociován s $d' = y + (x^2+1)$. Snadno se ukáže (můžeme dále dělit), že d' už dělí g v $\mathbb{Z}_2(x)[y]$, je to tedy $\mathrm{NSD}_{\mathbb{Z}_2(x)[y]}(f,g)$ a protože jde o prvek $\mathrm{NSD}_{\mathbb{Z}_2[x][y]}(f,g)$, který je primitivní, je to i hledané d a tedy i $\mathrm{NSD}_{\mathbb{Z}_2[x,y]}(f,g)$.

Zkusme nyní opět postupovat přímo rozkladem na ireducibilní prvky; půjde trochu o metodu „pokus-omyl“. Polynom f má sedm členů, takže pokud se nějak rozkládá, nejspíš se při tom něco „posčítá“; to g má šest členů, takže můžeme „doufat“, že ho lze rozložit na dvě závorky, jednu s dvěma členy a jednu se třemi. Protože se v $g = a \cdot b$ vyskytuje samostatné x, musí jedna závorka (a) obsahovat x a druhá (b) 1; a

[2] To protože $x^2 - y^2 = \frac{1}{2y}(x-y)\cdot(2xy + 2y^2)$.

[3] Při volbě $\mathbb{Z}_2[x,y] = \mathbb{Z}_2[y][x]$ to potenciálně mohlo trvat až tři kroky.

naopak *nemůže* obsahovat 1 (protože g neobsahuje 1), tedy nemůže obsahovat ani y (g neobsahuje y a po roznásobení $a \cdot b$ by se $y \cdot 1$ nemělo s čím pokrátit). Na druhou stranu, když g obsahuje y^3 (samostatně) a také y^2, nejspíš budou a a b v nějakém pořadí obsahovat členy y a y^2, přičemž už víme, že y není v a. Tedy asi je $a = x + y^2 +$ možná něco dalšího, ovšem snadno zjistíme, že $a = x + y^2$ opravdu funguje a $b = x^2 + y + 1$. Dle Úlohy 3 jsou oba tyto polynomy ireducibilní a také zjevně neasociované. Je jasné, že a nemůže dělit f (protože f má nenulový absolutní člen), a když už máme celkem naději, že b bude dělit f, tak se to i celkem snadno ověří; $f = (x^2 + y + 1)(x + y + 1)$. Je tedy $\mathrm{NSD}_{\mathbb{Z}_2[x,y]}(f, g) = x^2 + y + 1$.[4]

Nakonec zkusme ještě „hybridní“ postup, potenciálně uplatnitelný v libovolném Gaussově oboru. Jelikož $\mathbb{Z}_2[x, y]$ není euklidovský obor, „naivní“ Euklidův algoritmus nám typicky brzy přestane fungovat, protože nebudeme moct dělit jednou z proměnných.[5] Stále ale platí, že největší společný dělitel dvou (či více) polynomů musí dělit i libovolnou $\mathbb{Z}_2[x, y]$-lineární kombinaci těchto polynomů. Můžeme tedy provádět nějaké „kroky à la Euklidův algoritmus“ s tím, že *snad* dospějeme k něčemu, co se bude snáz rozkládat a my tak odhalíme kandidáty na NSD. Konkrétně, snadno nalezneme ireducibilní rozklad

$$f + g = (y^2 + y + 1)x^2 + (y^3 + 1) = (y^2 + y + 1) \cdot (x^2 + y + 1)$$

a snadno také ověříme, že zatímco $y^2 + y + 1$ nedělí ani jeden z polynomů f, g, tak $x^2 + y + 1$ je dělí oba, a je to tedy hledaný NSD v $\mathbb{Z}_2[x, y]$. □

Úloha 3. Nechť $\Bbbk$ je těleso a $p \in \Bbbk[y]$. Dokažte, že $x + p$ je ireducibilní prvek $\Bbbk[x, y]$.

Vsuvka (kterak nalézti vyjádření pomocí elementárních symetrických polynomů)**.** Nechť R je obor integrity. Máme-li symetrický polynom $f_0 \in R[x_1, \ldots, x_n]$, jehož nejvyšším termem (v lexikografickém uspořádání) je $x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$ (nezbytně $k_1 \geq k_2 \geq \cdots \geq k_n$) a koeficient u onoho členu je c, pak přejdeme k polynomu

$$f_1 = f_0 - c s_1^{k_1 - k_2} s_2^{k_2 - k_3} \cdots s_{n-1}^{k_{n-1} - k_n} s_n^{k_n},$$

kde s_i je i-tý elementární symetrický polynom v $x_1, \ldots, x_n$. Dále totéž provedeme s polynomem f_1 atd., dokud ještě je co odčítat. Hledané vyjádření je součtem toho, co jsme postupně poodčítali.

☼ **Úloha 4.** Nalezněte vyjádření pomocí elementárních symetrických polynomů v $\mathbb{C}[x, y, z]$:

(a) $x^2yz + xy^2z + xyz^2$,

(b) $x^3(y + z) + y^3(x + z) + z^3(x + y)$.

Řešení. (a) Lexikograficky nejvyšší člen je x^2yz, odečítáme tedy $s_1^{2-1} s_2^{1-1} s_3^1 = s_1 s_3$ a je okamžitě vidět, že onen zadaný polynom už je ono $s_1 s_3$.

(b) Roznásobíme závorky; lexikograficky nejvyšší člen je x^3y, odečítáme tedy

$$s_1^{3-1} s_2^{1-0} s_3^0 = s_1^2 s_2 = x^3y + x^3z + 2x^2y^2 + 5x^2yz + 2x^2z^2 + xy^3 + 5xy^2z + 5xyz^2 + xz^3 + y^3z + 2y^2z^2 + yz^3,$$

takže nyní máme

$$f_1 = -2(x^2y^2 + y^2z^2 + z^2x^2) - 5(x^2yz + y^2zx + z^2xy).$$

lexikograficky nejvyšší člen je x^2y^2, odečítáme tedy

$$-2s_1^{2-2} s_2^{2-0} s_3^0 = -2s_2^2 = -2(x^2y^2 + y^2z^2 + z^2x^2) - 4(x^2yz + y^2zx + z^2xy),$$

takže

$$f_2 = -(x^2yz + y^2zx + z^2xy).$$

Jako v části (a) nahlédneme, že toto je $-s_1 s_3$, takže hledané vyjádření je $s_1^2 s_2 - 2s_2^2 - s_1 s_3$. □

Úloha 5. Je reálný polynom $(x_1 + x_2 - x_3 - x_4)(x_1 - x_2 + x_3 - x_4)(x_1 - x_2 - x_3 + x_4)$ symetrický?[6]

Řešení. Není těžké si rozmyslet, že na to, aby byl polynom symetrický, stačí, aby se neměnim při *transpozicích* proměnných (jelikož každá permutace je složením transpozic).[7] Znaménka v závorkách můžeme chápat jako (všechny tři) možnosti, jak rozdělit čtyři prvky na dvě skupiny po dvou; proto kdykoliv prohodíme dvě proměnné, tak ve výsledku prohodíme ty dvě závorky, ve kterých mají ony proměnné různá znaménka, a ta, ve které mají znaménko stejné, se nezmění. □

[4] Obecně je problém rozkládání polynomů více proměnných celkem obtížný a nad konečnými tělesy na něj asi ani neexistují rozumné algoritmy, jelikož nejmenovaný software praví `Factoring multivariate polynomials with respect to a modulus is not yet implemented`. Ale nezkoumal jsem podrobnosti.

[5] proto se taky ve Vsuvce přechází k polynomům nad podílovým tělesem!

[6] V zadání vytištěném na cvičení obsahovala první závorka $+x_3$ namísto $-x_3$.

[7] Dokonce tedy stačí testování omezit na takovou množinu permutací, jejichž kombinací lze získat libovolnou permutaci (taková množina je *množina generátorů symetrické grupy*.)

Úloha 6. Nahlédněte, že druhá mocnina determinantu Vandermondovy matice

$$V(x_1, \ldots, x_n) = \left(x_i^{j-1}\right)_{i,j=1}^{n}$$

je symetrický polynom vzhledem k proměnným $x_1, \ldots, x_n$.

Řešení. Permutace proměnných znamená permutaci řádků Vandermondovy matice, což může nanejvýš změnit znaménko determinantu, ale protože nás zajímá druhá mocnina deteminantu, výsledné znaménko se nezmění. □

⋆ **Úloha 7.** Pro všechna $x, y, z \in \mathbb{R}$ dokažte

$$x^4 + y^4 + z^4 + 3x^2y^2 + 3x^2z^2 + 3y^2z^2 \geq 2x^3y + 2x^3z + 2xy^3 + 2xz^3 + 2y^3z + 2yz^3$$

a rozhodněte, kdy nastává rovnost.

Řešení. Všechny členy přehodíme na pravou stranu, čímž dostaneme nerovnost tvaru $f \geq 0$, kde $f \in \mathbb{R}[x, y, z]$. Nyní rozložíme f na elementární symetrické polynomy a zjistíme

$$f = s_1^4 - 6s_1^2s_2 + 9s_2^2 = (s_1^2 - 3s_2)^2.$$

Vidíme, že vskutku $f \geq 0$ pro všechna $x, y, z \in \mathbb{R}$, přičemž rovnost může nastává právě za situace $s_1^2 = 3s_2$. Po rozepsání tato podmínka dostane tvar

$$x^2 + y^2 + z^2 = xy + yz + zx,$$

což lze upravit na

$$(x - y)^2 + (y - z)^2 + (z - x)^2 = 0.$$

Vidíme tedy, že rovnost nastane právě když $x = y = z$. □

⋆ **Úloha 8.** Nechť α, β jsou kořeny reálného polynomu $x^2 + 2x - 2$. Aniž byste určili hodnoty α a β, spočtěte hodnotu $\alpha^6 + \beta^6$.

⋆ **Úloha 9.** Symetrické polynomy lze chápat jako speciální případ polynomů, které jsou *invariantní* vůči některým lineárním zobrazením – v tomto konkrétním případě vůči zobrazením daným permutačními maticemi. Co jsou polynomy v $\mathbb{C}[x, y]$, které jsou invariantní vůči lineárnímu zobrazení

(a) $(x, y) \mapsto (x, 0)$?
(b) $(x, y) \mapsto (-x, y)$?
(c) $(x, y) \mapsto (-y, x)$?
(d) Rozmyslete si, že množina zobrazení, vůči kterým je polynom invariantní, je uzavřená na skládání, a pokud řešíme jen regulární zobrazení (což se typicky děje), pak i na inverzní zobrazení (a samozřejmě tato množina obsahuje identické zobrazení) (tj. jde o *grupu*).