Algebra — cvičení 6, řešení

1. (a) Najděte všechny racionální kořeny polynomu $2x^3 - x^2 + 3$. Dosazením prvků $\pm 1, \pm 1/2, \pm 3, \pm 3/2$ zjistíme, že jediným racionálním kořenem je -1. Přičemž je možná i rychlejší po nalezení -1 podělit: dostaneme $2x^3 - x^2 + 3 = (x+1)(2x^2 - 3x + 3)$ a polynom $2x^2 - 3x + 3$ jistě nemá reálné kořeny, jelikož má záporný diskriminant.

3. Rozmyslete si, proč jsou následující polynomy v příslušných oborech ireducibilní:

(b) $x^4 + x^3 - x + 1$ v $\mathbb{Z}[x]$. Dosazením zjistíme, že není 1 ani -1 kořenem. Polynom tedy nemá racionální kořen. Mohl by se ale rozkládat jako součin dvou polynomů stupně 2. Nejlepší je všimnout si, že kdyby se polynom netriviálně rozkládal nad $\mathbb{Z}$, pak by se musel také netriviálně rozkládat nad $\mathbb{Z}_3$, kde ale také nemá žádné kořeny. Jelikož ireducibilní polynomy stupně 2 jsou (až na asociovanost) nad $\mathbb{Z}_3$ právě $x^2 + x + 2, x^2 + 2x + 2, x^2 + 1$, přičemž není těžké ověřit, že ani jeden z nich nedělí v $\mathbb{Z}_3[x]$ zadaný polynom.

Jinou možností je napsat si hypotetický rozklad v $\mathbb{Z}[x]$, bez újmy na obecnosti, jako $x^4 + x^3 - x + 1 = (x^2 + ax + b)(x^2 + cx + d)$, kde $a, b, c, d \in \mathbb{Z}$. Porovnáním koeficientů dostaneme: $bd = 1, ad+bc = -1, b+d+ac = 0, a+c = 1$. Z první rovnice plyne $b = d = \pm 1$, z druhé a čtvrté potom $b = d = -1$. Ze třetí nakonec $ac = 2$, což vzhledem ke čtvrté rovnici znamená, že $\{a, c\} = \{1, 2\}$, což ale implikuje $a + c = 3$, spor.

(c) $4x^3 - 15x^2 + 60x + 180$. Vzhledem k tomu, že se jedná o primitivní polynom, můžeme použít Eisensteinovo kritérium pro 5 (nikoliv ovšem pro 3, jelikož $9 \mid 180$).

(d) $x^5 - 36x^4 + 6x^3 + 30x^2 + 24$ v $\mathbb{Q}[x]$. Z Eisensteinova kritéria pro 3 dostaneme ireducibilitu v $\mathbb{Z}[x]$. Aplikace věty 8.3 ze skript (tj. Gaussova lemmatu) pak dává ireducibilitu nad $\mathbb{Q}$; zadaný polynom je monický, je tedy jistě primitivní v $\mathbb{Z}[x]$.

4. Spočtěte v oboru $\mathbb{Z}[x, y]$ NSD pro polynomy $f = 6x^2y$ a $g = 15xy^2 + 21x^3y$. (Zaměřte se na zdůvodnění dle věty 8.3 ze skript.) Ještě než se zaměříme, můžeme si všimnout, že

$$f = 2 \cdot 3 \cdot x \cdot x \cdot y, \quad g = 3xy(y + 7x^2).$$

Budeme-li vědět, že jsme právě napsali ireducibilní rozklady zadaných prvků v Gaussově oboru $\mathbb{Z}[x, y]$, dostáváme dle tvrzení z přednášky NSD rovno $3xy$. Položíme-li $R = \mathbb{Z}[x]$, pak $\mathbb{Z}[x, y] = R[y]$; užijeme větu 8.3 (2) pro toto R a s y namísto x ve formulaci věty. Nejzajímavější zdůvodnění ireducibility je potom u polynomu $f = y + 7x^2$, který je ireducibilní, jelikož je primitivní a stupně 1. To, že je stupně 1, znamená mimo jiné, že je ireducibilní v $Q[y]$, kde Q je podílové těleso oboru R.

Jinou možností je vydělit polynomy se zbytkem v $Q[y]$, kde Q je stále podílové těleso oboru R výše. Dostaneme $15xy^2 + 21x^3y = (6x^2y)(\frac{5y}{2x} + \frac{7x}{2})$, zbytek 0. Pak věta 8.3 (1) říká, že hledané NSD je rovno $c \cdot h$, kde $h = \mathrm{NSD}_{Q[y]}(f, g) = y$ a $c = \mathrm{NSD}_R(6x^2, 3x) = 3x$.

5. Najděte v příslušných oborech ireducibilní rozklady daných polynomů:

	$x^2 - y + 2$	$x^2 - 2y^2$	$x^2 + y^2$	$x^2 + xy + y - 1$
$\mathbb{Q}[x, y]$	$x^2 - y + 2$	$x^2 - 2y^2$	$x^2 + y^2$	$(x+1)(y+x-1)$
$\mathbb{R}[x, y]$	$x^2 - y + 2$	$(x - \sqrt{2}y)(x + \sqrt{2}y)$	$x^2 + y^2$	$(x+1)(y+x-1)$
$\mathbb{C}[x, y]$	$x^2 - y + 2$	$(x - \sqrt{2}y)(x + \sqrt{2}y)$	$(x + iy)(x - iy)$	$(x+1)(y+x-1)$

Ireducibilitu prvků z rozkladu zdůvodníme např. větou 8.3 (2).

6. (a) Vyřešte kongruenci $(x^3+x+1)f(x) \equiv 1 \pmod{x^4+x+1}$. Na cvičení on-line jsme jen dopočítali, že tato zadaná kongruence je ekvivalentní $f(x) \equiv x^2+1 \pmod{x^4+x+1}$. Odpovědí je pak každý polynom tvaru $x^2+1+q(x)(x^4+x+1)$, kde $q(x) \in \mathbb{Z}_2[x]$.

6. (b) Vyřešte kongruenci $(2x+1)f(x) \equiv x^3 \pmod{x^2+1}$ v $\mathbb{Z}_3[x]$. Polynom x^2+1 je ireducibilní nad $\mathbb{Z}_3$, stačí tedy najít inverzní prvek k $2x+1$ modulo polynom x^2+1. To lze udělat například spuštěním rozšířeného Eukleidova algoritmu na dvojici x^2+1, $2x+1$. Na druhou stranu lze inverzní prvek také snadno uhodnout, ježto $(2x+1)(2x-1) = 4x^2-1 = x^2+2$, což je modulo x^2+1 kongruentní 1.

Dostáváme, že zadaná kongruence je ekvivalentní kongruenci

$$f(x) \equiv x^3(2x-1) \pmod{x^2+1}, \text{ což je po úpravě } f(x) \equiv x+2 \pmod{x^2+1}.$$

Řešením je proto každý polynom tvaru $x+2+q(x)(x^2+1)$, kde $q(x) \in \mathbb{Z}_3[x]$.

7. Najděte všechny polynomy $f \in \mathbb{Q}[x]$ stupně menšího než 3 splňující $f(0)=1$, $f(1)=0$, $f(2)=2$. Podíváme-li se na vzorec pro konkrétní Lagrangeův interpolační polynom, dostáváme $f = \frac{1}{2}(1-x)(2-x) + x(x-1) = \frac{1}{2}(3x^2-5x+2)$.

Přes čínskou zbytkovou větu řešíme v $\mathbb{Q}[x]$ soustavu kongruencí: $f \equiv 1 \pmod{x}$, $f \equiv 0 \pmod{x-1}$, $f \equiv 2 \pmod{x-2}$. Tu lze řešit buď postupným dosazováním, nebo jako soustavu lineárních rovnic. Nejprve ukážeme první metodu.

Z první kongruence máme $f = 1+kx$, kde $k \in \mathbb{Q}[x]$. Dosazením do druhé potom $1+kx \equiv 0 \pmod{x-1}$, což je ekvivalentní $k \equiv -1 \pmod{x-1}$, a tedy $k = -1+l(x-1)$, pročež $f = 1+(-1+l(x-1))x = 1-x+l(x^2-x)$, kde $l \in \mathbb{Q}[x]$. Nakonec dosazením do 3. kongruence dostaneme $1-x+l(x^2-x) \equiv 2 \pmod{x-2}$, což je ekvivalentní $2l \equiv 3 \pmod{x-2}$, a proto $l = \frac{3}{2} + m(x-2)$, kde $m \in \mathbb{Q}[x]$, což po dosazení dává $f = 1-x+(\frac{3}{2}+m(x-2))(x^2-x) = \frac{3}{2}x^2 - \frac{5}{2}x + 1 + m(x^3-3x^2+2x)$. Jelikož hledáme polynom stupně menšího než 3, stačí položit $m=0$.

Nyní metodou se soustavou lineárních rovnic. Hledáme polynom ve tvaru ax^2+bx+c, kde $a,b,c \in \mathbb{Q}$. Z podmínek ze zadání dostáváme po řadě, že $c=1$, $a+b+c=0$ a $4a+2b+c=2$. Je proto $a+b=-1$ a $4a+2b=1$, z čehož $a=\frac{3}{2}$ a dále pak $b=\frac{-5}{2}$.

8. Najděte polynom $f \in \mathbb{Z}_5[x]$ co nejmenšího stupně, který splňuje

$$\begin{cases} f \equiv x+1 \pmod{x^2+1}, \\ f \equiv x \pmod{x^3+1}. \end{cases}$$

Z ČZV dostáváme, že existuje právě jeden polynom tvaru $f = ax^4+bx^3+cx^2+dx+e \in \mathbb{Z}_5[x]$, kde $a,b,c,d,e \in \mathbb{Z}_5$, který řeší danou soustavu. Proč? Stačí ověřit, že polynomy x^2+1 a x^3+1 jsou nad $\mathbb{Z}_5$ nesoudělné: to ovšem plyne ihned z ireducibilních rozkladů $x^2+1 = (x-2)(x-3)$, $x^3+1 = (x+1)(x^2-x+1)$.

Z první kongruence máme $f = x+1+k(x^2+1)$. Dosazením do druhé kongruence dostaneme $k(x^2+1) \equiv 4 \pmod{x^3+1}$. Nyní již zbývá jen nalézt inverzní prvek k x^2+1 modulo x^3+1.

Jest $x^3+1 = x(x^2+1)+(-x+1)$ a dále $x^2+1 = (-x-1)(-x+1)+2$. Dohromady potom $1 = 3(x^2+1)+(3x+3)(-x+1) = 3(x^2+1)+(3x+3)(x^3+1-x(x^2+1))$, a tedy $(x^2+1)^{-1} = 2x^2+2x+3$. Z toho již dostáváme kýžené $f = x+1+(3x^2+3x+2)(x^2+1) = 3x^4+3x^3+4x+3$.

9. Buď p prvočíslo. Stačí si uvědomit, že zobrazení $\psi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$, které polynomu $\sum_{i=0}^n a_i x^i$ přiřadí polynom $\sum_{i=0}^n (a_i \mod p)x^i$, je (surjektivní) okruhový homomorfismus.

Obecně pro každý okruhový homomorfismus $g : R \to S$ je zobrazení $g_x : R[x] \to S[x]$ definované vztahem $g_x(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} g(a_i)x^i$ opět okruhovým homomorfismem (to je snadné cvičení). Navíc je g_x prosté/surjektivní/bijektivní právě tehdy, když je g takové.

V důsledku výše uvedeného pak pro polynom $f \in \mathbb{Z}[x]$ a jeho netriviální rozklad $f = gh$ platí $\psi(f) = \psi(g)\psi(h)$. Je-li navíc f primitivní, mají g, h ostře menší stupně než f (ovšem stále $\deg g, \deg h > 0$). A pokud p nedělil vedoucí koeficient, pak totéž platí i po aplikaci homomorfismu ψ, tj. $\psi(g)$ a $\psi(h)$ mají ostře menší stupně než $\psi(f)$ (ovšem stále $\deg \psi(g), \deg \psi(h) > 0$).

10. Rozhodněte o ireducibilitě polynomu $f = x^5 + 4x^4 + 2x^3 + 3x^2 - x + 5$ v $\mathbb{Z}[x]$. (Využijte předchozí tvrzení.) Chceme volit postupně co možná nejmenší prvočísla p. Pro $p = 2$ dostáváme po vymodulení koeficientů polynom $x^5 + x^2 + x + 1$, který má v $\mathbb{Z}_2$ kořen; tvrzení výše nám tedy a priori nic neřekne.

Pro $p = 3$ obdržíme po vymodulení $x^5 + x^4 + 2x^3 + 2x + 2$, který — jak se snadno zjistí dosazením — nemá v $\mathbb{Z}_3$ kořen. Navíc není v $\mathbb{Z}_3[x]$ dělitelný ani (až na asociovanost) jedinými ireducibilními polynomy nad $\mathbb{Z}_3$ stupně 2, konkrétně $x^2 + x + 2$, $x^2 + 2x + 2$, $x^2 + 1$. Tento polynom je tedy nad $\mathbb{Z}_3$ ireducibilní, a proto je zadaný polynom ireducibilní nad $\mathbb{Z}$ v důsledku předchozího cvičení.

11. Podobně jako v 9. úloze použijeme homomorfismus. Tentokrát uvážíme, že $\mathbf{R}$ je přirozeným způsobem podokruhem v oboru $\mathbf{R}[x]$ (ztotožňujeme konstantní polynomy s prvky oboru $\mathbf{R}$). Proto můžeme pro libovolný $h \in \mathbf{R}[x]$ uvážit dosazovací homomorfismus $d_h : \mathbf{R}[x] \to \mathbf{R}[x]$ definovaný vztahem $d_h(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} a_i h^i$. Ten samozřejmě nemusí být ani prostý, ani surjektivní. Konkrétně například pro volbu $h = x^2$ nebude surjektivní. Pak nás nemůže překvapit, že x je ireducibilní nad $\mathbf{R}$, zatímco $d_h(x) = x^2$ již není ireducibilní.

Pro volbu $h = ax + b$, kde $a, b \in R$ a a je invertibilní, je ovšem d_h izomorfismem (tj. automorfismem okruhu $\mathbf{R}[x]$). Proč? Stačí totiž uvážit $h^* = a^{-1}x - ba^{-1}$. Je snadné si uvědomit, že $d_h \circ d_{h^*} = d_{h^*} \circ d_h = \mathrm{id}_{\mathbf{R}[x]}$, a proto musí být d_h i d_{h^*} automorfismy.

Jelikož je tedy v našem případě d_h automorfismus, platí pro každé $f \in \mathbf{R}[x]$, že f je ireducibilní nad $\mathbf{R}$ právě tehdy, když $d_h(f)$ je ireducibilní nad $\mathbf{R}$. To plyne z toho, že definice ireducibility je vyjádřena pomocí vztahu dělitelnosti, to jest pomocí operace násobení, kterou každý izomorfismus (i jeho inverz) zachovává.

12. S využitím předchozího tvrzení rozhodněte o ireducibilitě následujících polynomů v $\mathbb{Z}[x]$:

(1) $x^3 + 3x^2 + 5x + 5$,
(2) $\frac{x^p-1}{x-1} = \sum_{i=0}^{p-1} x^i$ pro prvočíslo p.

V prvním případě bychom mohli využít pouze kritérium racionálního kořene. Ale budiž! Použijeme tedy předchozí cvičení pro $h = x - 1$. Dostaneme $d_h(x^3 + 3x^2 + 5x + 5) = (x-1)^3 + 3(x-1)^2 + 5x = x^3 + 2x + 2$, který je ireducibilní dle Eisensteinova kritéria pro 2.

Druhý případ je ilustrativní a celkem důležitý. Zde použijeme $h = x + 1$. Dostaneme $d_h(\frac{x^p-1}{x-1}) = \frac{(x+1)^p-1}{x}$, což je polynom, jehož absolutní člen je p a všechny ostatní koeficienty kromě vedoucího jsou dělitelné prvočíslem p, jelikož $p \mid \binom{p}{k}$, pokud $0 < k < p$ (zde využíváme, že p je prvočíslo). Následně užijeme Eisensteinovo kritérium pro p.

13. Rozmyslete si, proč je polynom $3x^3 + 2x^2 + (4-2i)x + (1+i)$ v $(\mathbb{Z}[i])[x]$ ireducibilní. Toto je snadné: stačí použít Eisensteinovo kritérium pro prvočinitel $1+i$. Připomeňme, že $2 = (1+i)(1-i)$.

Na cvičení Olina Slávika a Honzy Václavka navíc přidali příklad níže. Můžete ho zkusit řešit jen užitím věty 8.3. Asi to nebude žádný med.

14. Spočítejte NSD následujících dvou polynomů

$$f = 2xy + 2x^2y + 8xy^2 + 15x^2y^2 + 7x^3y^2 + 8x^2y^3 + 13x^3y^3 + 5x^4y^3,$$
$$g = 6y + 6xy + 24y^2 + 39xy^2 + 15x^2y^2 \text{ v } \mathbb{Z}[x,y].$$

Jelikož $3 \nmid f$ budeme místo g dále uvažovat polynom $2y + 2xy + 8y^2 + 13xy^2 + 5x^2y^2$. Současně, vzhledem k tomu, že $x \nmid g$, budeme místo f dále uvažovat polynom $2y + 2xy + 8y^2 + 15xy^2 + 7x^2y^2 + 8xy^3 + 13x^2y^3 + 5x^3y^3$. Jelikož jsou oba polynomy zřejmě dělitelné monomem y, potřebujeme najít NSD polynomů

$$f_1 = 2 + 2x + 8y + 15xy + 7x^2y + 8xy^2 + 13x^2y^2 + 5x^3y^2,$$
$$g_1 = 2 + 2x + 8y + 13xy + 5x^2y.$$

Polynom g_1 je již lineární v y, což je jistě výhodné pro další počítání. Navíc se oba polynomy trochu podobají. Uvědomíme-li si, že $\mathrm{NSD}(f_1, g_1) = \mathrm{NSD}(f_1 - g_1, g_1)$ a že polynom $f_1 - g_1$ je dělitelný prvkem xy, který je ovšem nesoudělný s g_1, můžeme dále počítat NSD polynomů

$$\frac{f_1 - g_1}{xy} = 2 + 2x + (8 + 13x + 5x^2)y,$$
$$g_1 = 2 + 2x + (8 + 13x + 5x^2)y.$$

A vida, obdrželi jsme shodné polynomy! Hledané $\mathrm{NSD}(f,g)$ je proto rovno $yg_1 = (2+2x)y + (8 + 13x + 5x^2)y^2 = y(x+1)(2 + (5x+8)y)$. Součin úplně vpravo je navíc ireducibilním rozkladem tohoto $\mathrm{NSD}(f,g)$ v Gaussově oboru $\mathbb{Z}[x,y]$.