5 Gauss je náš!

Řešení
Cvičení 20. a 21. března, verze ze dne 21. března 2024

Cíle cvičení: Tentokrát oceníme Gaussovu větu a zhluboka si zapřemýšlíme nad ireducibilními rozklady polynomů nad Gaussovými obory. Vyzkoušíme si rovněž Eisensteinovo kritérium ireducibility a elementární postup pro hledání racionálních kořenů, což se nám pro nalezení rozkladů může hodit.

Budeme bez důkazu předpokládat, že kromě oborů $\mathbb{Z}$ a $\mathbb{Z}[i]$, o nichž to bylo dokázáno na přednášce, jsou eukleidovské s obvyklou normou také obory $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{-2}]$ a $\mathbb{Z}[\sqrt{3}]$.

Úlohy, které bychom určitě měli umět řešit:

Úloha 5.1. Najděte ireducibilní rozklady v oborech $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Z}[x]$ a $(\mathbb{Z}[i])[x]$ polynomů

(a) $6x - 6$,

(b) $2x^2 + 2$,

(c) $7x^3 - 14$.

Řešení. (a) Protože je 6 v tělesech $\mathbb{C}$ i $\mathbb{R}$ invertibilní, tedy asociované s jednotkou 1, je lineární polynom $6x-6$ ireducibilní v $\mathbb{C}[x]$, $\mathbb{R}[x]$, všimněme si, že je tento polynom asociovaný s polynomem $x-1$. Nad obory $\mathbb{Z}$ i $\mathbb{Z}[i]$ snadno zjistíme, že obsah polynomu $6x-6$ je 6, tedy $6x-6 = 6\cdot(x-1)$, kde $x-1$ je jeho primitivní část. Lineární polynom je samozřejmě ireducibilní v $\mathbb{Q}[x]$, tedy je jeho primitivní část ireducibilní i v $\mathbb{Z}[x]$, zbývá provést ireducibilní rozklad obsahu. Ten je $6 = 2\cdot 3$ v $\mathbb{Z}$ a $6 = (1+i)\cdot(1-i)\cdot 3$ v $\mathbb{Z}[i]$ (viz úloha 4.3(a)), tedy díky větě 8.5(2) z přednášky dostáváme ireducibilní rozklady:

$$6x-6 = 2\cdot 3\cdot(x-1) \in \mathbb{Z}[x], \quad 6x-6 = (1+i)\cdot(1-i)\cdot 3\cdot(x-1) \in (\mathbb{Z}[i])[x]$$

(b) Zatímco v $\mathbb{R}[x]$ všichni vidí, že je polynom $2x^2+2$ asociovaný se slavným polynomem x^2+1 jistě ireducibilní, nad komplexními čísly snadno spočteme jeho ireducibilní rozklad

$$2x^2 + 2 = (2x+2i)(x-i) \in \mathbb{C}[x]$$

sestávající ze součinu dvou lineárních polynomů. Obsah polynomu v oborech $\mathbb{Z}$ i $\mathbb{Z}[i]$ je tentokrát 2. Protože je primitivní část x^2+1 ireducibilní v $\mathbb{Q}[x]$ a rozkládá se na ireducibilní faktory $(x+i)\cdot(x-i)$ v $(\mathbb{Z}[i])[x]$, získáme stejnou úvahou jako v (a) ireducibilní rozklady

$$2x^2+2 = 2\cdot(x^2+1) \in \mathbb{Z}[x], \quad 2x^2+2 = (1+i)\cdot(1-i)\cdot(x+i)\cdot(x-i) \in \mathbb{Z}[i][x]$$

(c) Vidíme, že $7x^3-14 = 7(x^3-2)$, proto můžeme využít výsledky rozkladu asociovaného polynomu x^3-2 v úloze 3.4. Tak dostáváme ireducibilní rozklady

$$7(x^3-2) = (7x - 7\sqrt[3]{2})\cdot\left(x + \frac{1}{\sqrt[3]{4}} + \frac{\sqrt{3}}{\sqrt[3]{4}}i\right)\cdot\left(x + \frac{1}{\sqrt[3]{4}} - \frac{\sqrt{3}}{\sqrt[3]{4}}i\right) \in \mathbb{C}[x]$$

$$7(x^3-2) = (7x - 7\sqrt[3]{2})\cdot(x^2 + \sqrt[3]{2}x + \sqrt[3]{4}) \in \mathbb{R}[x]$$

Dále si všimneme, že obsah 7 je ireducibilní v obou oborech $\mathbb{Z}[i]$ i $\mathbb{Z}$ podle 4.8 a zbylé ireducibilní rozklady jsou tudíž $7x^3-14 = 7\cdot(x^3-2)$ v obou oborech $(\mathbb{Z}[i])[x]$ i $\mathbb{Z}[x]$.

Úloha 5.2. Spočtěte $\mathrm{NSD}(f, g)$

(a) $f = 6x^3 - 6$, $g = 8x^2 - 8$ v oboru $\mathbb{Z}[x]$,

(b) $f = 6x^2 + 3x - 3$, $g = 6x^2 + 6x$ v oboru $\mathbb{Z}[x]$

(c) $f = 6x^2y$, $g = 15xy^2 + 21x^3y$ v oboru $\mathbb{Z}[x, y]$

Řešení. (a) Snadno zjistíme obsahy $c(f) = 6$ a $c(g) = 8$, proto jejich $\mathrm{NSD}_{\mathbb{Z}}(c(f), c(g)) = 2$. Nyní zbývá spočítat v eukleidovském oboru $\mathbb{Q}[x]$ největší společný dělitel primitivních částí x^3-1 a x^2-1 a vzít jeho reprezentanta primitivního nad $\mathbb{Z}$, který snadno najdeme i bez Eukleidova algoritmu $\mathrm{NSD}_{\mathbb{Q}[x]}(x^3 - 1, x^2 - 1) = x - 1$.

Podle věty 8.5 z přednášky je $\mathrm{NSD}_{\mathbb{Z}[x]}(f, g) = 2(x - 1)$.

(b) Postupujeme jako v (a). Spočítáme

$$\mathrm{NSD}_{\mathbb{Z}}(c(f), c(g)) = 3 \quad \text{a} \quad \mathrm{NSD}_{\mathbb{Q}[x]}(2x^2 + x - 1, x^2 + 1) = (x + 1)$$

v oboru $\mathbb{Q}[x]$, který je primitivní v $\mathbb{Z}[x]$. Tudíž $\mathrm{NSD}_{\mathbb{Z}[x]}(f, g) = 3(x + 1)$

(c) Tentokrát se nejprve na oba prvky podíváme jako na polynomy v neurčité y s koeficienty v oboru $\mathbb{Z}[x]$ a spočítáme obsahy, $c(f) = 6x^2$, $c(g) = \mathrm{NSD}_{\mathbb{Z}[x]}(15x, 21x^3) = 3x$ a jejich největší společný dělitel $\mathrm{NSD}_{\mathbb{Z}[x]}(6x^2, 3x) = 3x$. Dále určíme největší společný dělitel primitivních částí $pp(f) = y$ a $pp(g) = 5y^2+7x^2y$, který je primitivní jako polynom s koeficienty v oboru $\mathbb{Z}[x]$, dostáváme polynom $\mathrm{NSD}_{\mathbb{Q}(x)[y]}(y, 5y^2 + 7x^2y) = y$. Nakonec opět pomocí věty 8.5(1) z přednášky snadno určíme

$$\mathrm{NSD}_{\mathbb{Z}[x,y]}(f, g) = \mathrm{NSD}_{\mathbb{Z}[x]}(c(f), c(g)) \cdot pp_{(\mathbb{Z}[x])[y]}(\mathrm{NSD}_{\mathbb{Q}(x)[y]}(pp(f), pp(g)) = 3xy.$$

Úloha 5.3. Najděte všechny racionální kořeny daných polynomů z $\mathbb{Z}[x]$:

(a) $3x^5 - 2x^2 + x + 1$, (b) $x^3 - 7x^2 + 11x + 3$ (c) $2x^3 - x^2 + 3$.

Řešení. Pomocí tvrzení 8.1 z přednášky určíme možné kandidáty na racionální kořeny $\frac{r}{s}$ polynomu, pro něž musí platit, že čitatel r dělí absolutní člen a jmenovatel s dělí vedoucí koeficient.

(a) Protože vedoucí koeficient polynomu $3x^5-2x^2+x+1$ má přirozené dělitele $1, 3$ a jeho absolutní člen je 1, máme právě čtyři kandidáty $\pm\frac{1}{1}, \pm\frac{1}{3}$ na kořeny. I bez počítání díky paritě koeficientů vidíme, že ± 1 kořenem není a podobně snadno vidíme, že $\pm\frac{3}{3^5} = \frac{1}{3^4} \neq \frac{2}{3^2} \pm \frac{1}{3} - 1$, tudíž polynom $3x^5 - 2x^2 + x + 1$ nemá žádný racionální kořen.

(b) Tentokrát je polynom $x^3 - 7x^2 + 11x + 3$ monický s absolutním členem dělitelným hodnotami $1, 3$, tedy stačí otestovat racionální hodnoty kořeny jsou $\pm\frac{1}{1}, \pm\frac{3}{1}$. Snadno spočítáme, že kořenem je pouze hodnota 3, což je tedy jediný racionální kořen našeho polynomu.

(c) Protože vedoucí koeficient polynomu $2x^3 - x^2 + 3$ má přirozené dělitele $1, 2$ a jeho absolutní člen má dělitele $1, 3$, proto představuje posloupnost

$$\pm\frac{1}{1}, \pm\frac{1}{2}, \pm\frac{3}{1}, \pm\frac{3}{2},$$

všechny možné kandidáty na kořeny. Vyzkoušením zjistíme, že -1 je jediným racionálním kořenem.

Úloha 5.4. Rozmyslete si, proč jsou následující polynomy v příslušných oborech ireducibilní:

(a) $x^3 + x^2 + x + 3$ v $\mathbb{Z}[x]$,

(b) $4x^3 - 15x^2 + 60x + 180$ v $\mathbb{Z}[x]$,

(c) $x^5 - 36x^4 + 6x^3 + 30x^2 + 24$ v $\mathbb{Q}[x]$.

Řešení. (a) Jedná se o polynom stupně tři, proto kdyby byl ireducibilní musel by mít racionální kořen. Úvahou z 5.3, zjistíme že pouze čísla ± 1 a ± 3 jsou kandidáty na kořeny a snadno spočteme, že žádný z nich kořenem není.

(b) Využijeme Eisensteinovo kritérium pro prvočíslo 5: polynom $4x^3-15x^2+60x+180$ je primitivní, 5 dělí všechny koeficienty kromě vedoucího a 25 nedělí absolutní člen, proto je polynom ireducibilní.

(c) Nejprve použijeme Eisensteinovo kritérium pro prvočíslo 3 a primitivní polynom $x^5 - 36x^4 + 6x^3 + 30x^2 + 24$ v oboru $\mathbb{Z}[x]$, díky němuž je ireducibilní v oboru $\mathbb{Z}[x]$. To ovšem podle věty 8.5(2) nutně znamená, že je ireducibilní i v oboru $\mathbb{Q}[x]$.

A teď něco navíc, abychom se při těšení na další cvičení nenudili:

Úloha 5.5. Rozložte polynom $2x^2 + 2x - 1$ nad eukleidovským oborem $\mathbb{Z}[\sqrt{3}]$ na součin ireducibilních prvků.

Řešení. Standardním postupem najdeme reálné kořeny polynomu, které nám dají ireducibilní rozklad nad $\mathbb{R}$, zároveň ireducibilně rozložíme v $\mathbb{Z}[\sqrt{3}]$ prvek $2 = (\sqrt{3} - 1)(\sqrt{3} + 1)$ a nakonec součin přeskupíme

$$2x^2 + 2x - 1 = (\sqrt{3} - 1)(\sqrt{3} + 1)(x + \frac{1}{2} + \frac{\sqrt{3}}{2})(x + \frac{1}{2} - \frac{\sqrt{3}}{2}) =$$

$$= (\sqrt{3} - 1)(x + \frac{1}{2} + \frac{\sqrt{3}}{2}) \cdot (\sqrt{3} + 1)(x + \frac{1}{2} - \frac{\sqrt{3}}{2}) = ((\sqrt{3} - 1)x + 1)((\sqrt{3} + 1)x - 1)$$

Vidíme, že polynomy $(\sqrt{3} - 1)x + 1), ((\sqrt{3} + 1)x - 1) \in \mathbb{Z}[\sqrt{3}][x]$ jsou v oboru $\mathbb{Z}[\sqrt{3}][x]$ primitivní a lineární, tedy jsme získali ireducibilní rozklad.

Úloha 5.6. Najděte ireducibilní rozklady v oborech $\mathbb{Q}[x, y]$, $\mathbb{R}[x, y]$ a $\mathbb{C}[x, y]$ polynomů

(a) $x^2 - y + 2$,

(b) $x^2 - 2y^2$,

(c) $x^2 + y^2$,

(d) $x^2 + xy + y - 1$,

(e)* $2y^3 + y^2x + yx^2 + x^2 + 7y^2 + 7y - x + 2$.

Řešení. (a) Polynom $x^2 - y + 2$ je ireducibilní ve všech oborech, protože je primitivní a lineární v proměnné y.

(b) Snadno najdeme rozklad nad $\mathbb{R}$, proto $x^2 - 2y^2 = (x - \sqrt{2}y)(x + \sqrt{2}y)$ je ireducibilní rozklad v $\mathbb{R}[x, y]$ a $\mathbb{C}[x, y]$. Protože je jeden z koeficientů faktorů racionální a druhý iracionální, je $x^2 - 2y^2$ ireducibilní v $\mathbb{Q}[x, y]$.

(c) Vidíme, že $x^2 + y^2 = (x + iy)(x - iy)$ je ireducibilní rozklad v $\mathbb{C}[x, y]$. Protože tentokrát je jeden z koeficientů faktorů imaginární a druhý reálný, je $x^2 + y^2$ ireducibilní v oborech $\mathbb{R}[x, y]$ i $\mathbb{Q}[x, y]$.

(d) Pokud si všimneme, že dosazením hodnoty -1 za x dostaneme $(-1)^2 - y + y - 1 = 0$, můžeme (například pomocí algoritmu dělení se zbytkem) vydělit

$$\frac{x^2 + xy + y - 1}{(x + 1)} = (x + y - 1).$$

Oba polynomy $x + 1$ i $x + y - 1$ jsou primitivní lineární polynomy v okruhu polynomů jedné neurčité (x i y), odkud použitím věty z přednášky dostáváme, že jsou oba ireducibilní. Proto je rozklad $x^2 + xy + y - 1 = (x + 1)(x + y - 1)$ ireducibilní ve všech třech oborech.

(e) I tentokrát si můžeme všimnout, že dosazení $y = -1$ nám vynuluje celý polynom, což znamená, že můžeme vytknout ireducibilní činitel $(y + 1)$. Dostaneme

$$2y^3 + y^2x + yx^2 + x^2 + 7y^2 + 7y - x + 2 = (y + 1)(x^2 + x(y - 1) + (2y^2 + 5y + 2)),$$

což už je ireducibilní rozklad ve všech třech oborech, neboť je primitivní v obou proměnných a nelze najít kořen v proměnné x vyjádřený jako polynom v neznámé y (k důkazu posledního můžeme využít například starý známý vzoreček pro hledání kořenů kvadratické funkce).

Úloha 5.7. Spočítejte v $\mathbb{Z}[x, y]$ největší společný dělitel následujících dvou (dechberoucím způsobem přenádherných) polynomů:

$$f = 2xy + 2x^2y + 8xy^2 + 15x^2y^2 + 7x^3y^2 + 8x^2y^3 + 13x^3y^3 + 5x^4y^3$$
$$g = 6y + 6xy + 24y^2 + 39xy^2 + 15x^2y^2.$$

Řešení. Oba polynomy budeme chápat jako polynomy v neznámé y s koeficienty v oboru $\mathbb{Z}[x]$

$$f = y[(2x + 2x^2) + (8x + 15x^2 + 7x^3)y + (8x^2 + 13x^3 + 5x^4)y^2]$$
$$g = y[(6 + 6x) + (24 + 39x + 15x^2)y].$$

Vidíme, že z obou polynomů lze vytknout společný dělitel y a snadno určíme největší společný dělitel $x + 1$ jejich obsahů, neboť koeficient u termu y polynomu g je tvaru $6 + 6x$ a vidíme, že koeficienty obsahů nad x jednotlivých koeficientů jsou nesoudělné a všechny koeficienty mají kořen $x = -1$. Zároveň můžeme oba polynomy vydělením obsahem upravit na primitivní a zbývá najít největší společný dělitel polynomů nad podílovým tělesem racionálních funkcí $\mathbb{Q}(x)$ společný dělitel

$$\tilde{f} = \frac{f}{yx(x + 1)} = 2 + (8 + 7x)y + (8x + 5x^2)y^2$$
$$\tilde{g} = \frac{g}{3y(x + 1)} = 2 + (8 + 5x)y.$$

Stačí nám jedno dělení se zbytkem, abychom zjistili, že $\mathrm{NSD}_{\mathbb{Q}(x)[y]}(\tilde{f}, \tilde{g}) = \tilde{g} = 2 + (5x + 8)y$ je primitivní nad $(\mathbb{Z}[x])[y]$, a proto $\mathrm{NSD}_{\mathbb{Z}[x,y]}(f, g) = y(x + 1)(2 + (5x + 8)y)$.

Úloha 5.8. Rozložte v $\mathbb{Z}[x]$ polynom $x^{16} - 1$ na součin ireducibilních polynomů.

Řešení. Nejprve uvážíme, že

$$x^{16} - 1 = (x^8 + 1)(x^8 - 1) = (x^8 + 1)(x^4 + 1)(x^2 + 1)(x + 1)(x - 1).$$

Dále si rozmyslíme, že

$$(x + 1)^{2^k} \equiv (x^2 + 1)^{2^{k-1}} \equiv (x^4 + 1)^{2^{k-2}} \equiv \cdots \equiv x^{2^k} + 1 \pmod 2,$$

což znamená, že všechny koeficienty kromě vedoucího koeficientu primitivního polynomu $(x+1)^{2^k}+1$ jsou dělitelné dvěma. Protože je navíc absolutní člen roven 2, není dělitelný číslem 2^2, proto se jedná podle Eisensteinova kritéria ireducibilní polynom. To znamená (podle cvičení 3.8), že i všechny polynomy $x^{2^k} + 1$ jsou v $\mathbb{Z}[x]$ ireducibilní, tedy výše nalezený rozklad je ireducibilní.

Úloha 5.9. Najděte všechny racionální kořeny polynomu

$$4x^7 - 16x^6 + x^5 + 55x^4 - 35x^3 - 38x^2 + 12x + 8 \in \mathbb{Z}[x].$$

Řešení. Postupujeme stejně jako v 5.3. Vedoucí koeficient našeho polynomu má přirozené dělitele 2^i pro $= 0, 1, 2$ a jeho absolutní člen má dělitele 2^i pro $= 0, 1, 2, 3$, proto představuje posloupnost

$$\pm\frac{1}{4},\ \pm\frac{1}{2},\ \pm1,\ \pm2,\ \pm4,\ \pm8.$$

Po lítém dosazovacím boji zjistíme, že má náš polynom právě dva racionální kořeny $-\frac{1}{2}, 2$.

Úloha 5.10. Rozmyslete si, proč je polynom $3x^3+2x^2+(4-2i)x+(1+i)$ v $(\mathbb{Z}[i])[x]$ ireducibilní.

Řešení. Použijeme Eisensteinovo kritérium pro prvočinitel $1+i$ v oboru $\mathbb{Z}[i]$, který zjevně dělí všechny koeficienty kromě vedoucího, zatímco $(1+i)^2$ nedělí absolutní člen.

Úloha 5.11. S využitím substituce $x \to x-a$ a tvrzení úlohy 3.8 rozhodněte o (i)reducibilitě následujících polynomů v $\mathbb{Z}[x]$

(a) $x^4+x^3+x^2+x+1$, (b) x^3+3x^2+5x+5, (c) $\frac{x^p-1}{x-1} = \sum_{i=0}^{p-1} x^i$ pro prvočíslo p.

Řešení. (a) Provedeme-li substituci $x \mapsto x+1$ dostaneme polynom

$$(x+1)^4+(x+1)^3+(x+1)^2+(x+1)+1 = x^4+4x^3+6x^2+4x+1+x^3+3x^2+3x+1+x^2+2x+1+x+1 =$$

$$= x^4+5x^3+10x^2+10x+1+5.$$ Tento polynom je ireducibilní podle Eisensteinova kritéria pro prvočíslo 5 a tudíž je podle cvičení 3.8 původní polynom $x^4+x^3+x^2+x+1$ rovněž ireducibilní.

(b) Tentokrát provedeme substituci $x \mapsto x-1$ a dostaneme

$$(x-1)^3+3(x-1)^2+5(x-1)+5 = x^3+2x+2,$$

což je podle Eisensteinova kritéia pro prvočíslo 2 ireducibilní, tudíž je ireducibilní i x^3+3x^2+5x+5.

(c) Provedeme-li substituci $x \mapsto x+1$, dostáváme

$$\frac{(x+1)^p-1}{(x+1)-1} = x^{p-1} + \sum_{i=1}^{p-1} \binom{p}{i} x^{i-1}.$$

Vidíme, že se jedná o primitivní polynom, jehož všechny koeficienty kromě vedoucího jsou dělitelné p a absolutní člen má hodnotu p, tedy není dělitelný čtvercem p^2. Podle Eisensteinova kritéria použité pro p a cvičení 3.8 je upravený i původní polynom ireducibilní.

Úloha 5.12. Ukažte, že je-li primitivní polynom $f \in \mathbb{Z}[x]$ reducibilní a prvočíslo p nedělí vedoucí koeficient f, pak je reducibilní i polynom $\overline{f} \in \mathbb{Z}_p[x]$ získaný vzetím koeficientů f modulo p.

Řešení. Nejprve si uvědomíme, že zobrazení $f \to \overline{f}$ zachovává násobení (dokonce se jedná o okruhový homomorfismus), tj. splňuje pro každou dvojici a, b podmínku $\overline{ab} = \overline{a}\overline{b}$. Protože prvočíslo p nedělí vedoucí koeficient f, nedělí ani vedoucí koeficient žádného jeho dělitele, což znamená, že $f = ab$, pak $\deg(a) = \deg(\overline{a})$ a $\deg(b) = \deg(\overline{b})$, tedy je-li $f = ab$ netriviální rozklad, pak $\overline{f} = \overline{a}\overline{b}$ je netriviální rozklad. Dokázali jsme obměnu našeho tvrzení.

Úloha 5.13. S využitím předchozího tvrzení rozhodněte v oboru $\mathbb{Z}[x]$ o (i)reducibilitě polynomu (a) $3x^4+7x^3+3x^2-x+5$, (b)* $x^5+4x^4+2x^3+3x^2-x+5$.

Řešení. (a) Vidíme, že $(3x^4+7x^3+3x^2-x+5) \mod 2 = x^4+x^3+x^2+x+1 \in \mathbb{Z}_2[x]$, což je ireducibilní polynom podle zjištění úlohy 3.7

(b) Uvážíme-li polynom $(x^5+4x^4+2x^3+3x^2-x+5) \mod 3 = x^5-x^4-x^3+-x-1 \in \mathbb{Z}_3[x]$, pak (poněkud úmornou) diskusí s využitím výsledků úlohy 3.19 (popisující všechny ireducibilní polynomy stupně dva a tři v $\mathbb{Z}_3[x]$) zjistíme, že $x^5-x^4-x^3+-x-1$ nemá žádný kořen v $\mathbb{Z}_3$ a ani není součinem ireducibilních polynomů stupně 2 a 3. To podle 5.12 znamená, že je polynom $x^5+4x^4+2x^3+3x^2-x+5$ ireducibilní v oboru $\mathbb{Z}[x]$.