5 Gauss – ideální matematik

Řešení
Verze ze dne 18. března 2025

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. Cvičení zakončíme výhledem do světa ideálů.

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 $\mathbb{Z}$, kterého 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

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

v oboru $\mathbb{Q}[x]$, přičemž tento polynom 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 kořeny daných polynomů ze $\mathbb{Z}[x]$ v zadaném tělese:

(a) $3x^3 - x^2 - 5x - 2$ v $\mathbb{Q}$,

(b) $x^5 + 2x^2 - 4x - 4$ v $\mathbb{Q}$ a $\mathbb{Q}(\sqrt{2})$ (kteréžto těleso se shoduje s podílovým tělesem Gaussova oboru $\mathbb{Z}[\sqrt{2}]$).

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 $3x^3 - x^2 - 5x - 2$ je 3 a absolutním členem je -2, kandidáti na racionální kořeny jsou

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

I bez počítání díky paritě koeficientů vidíme, že ± 1 kořenem není, pro ± 2 zase člen $3x^3$ v abs. hodnotě „převáží“ ostatní členy. Hodnoty $\pm\frac{1}{3}$ se snadno vyloučí dosazením a ze zbylých $\pm\frac{2}{3}$ vyhovuje pouze ta se záporným znaménkem, tedy je $-\frac{2}{3}$ jediný kořen uvedeného polynomu v $\mathbb{Q}$.

(b) V tomto případě jde o monický polynom s absolutním členem -4, takže kandidáti na kořeny v $\mathbb{Q}$ jsou ± 1, ± 2, ± 4. Hodnoty ± 1 zřejmě kořeny nejsou díky paritě, dále ± 2 a ± 4 nejsou kořeny díky snadnému náhledu, že všechny členy stupně alespoň 1 by v tomto případě byly dělitelné 8, což ale neplatí pro abs. člen.

V tělese $\mathbb{Q}(\sqrt{2})$ máme navíc kandidáty na kořeny $\pm\sqrt{2}$ a $\pm 2\sqrt{2}$, ovšem $\pm 2\sqrt{2}$ můžeme vyloučit podobnou úvahou jako pro ± 2 (nebo je prostě vyzkoušíme). Oproti tomu $\pm\sqrt{2}$ jsou oba kořeny. (Úvahou podobnou jako pro komplexně sdružené polynomy reálných polynomů můžeme nahlédnout, že analogickou vlastnost musí mít i „sdružené“ kořeny z $\mathbb{Q}(\sqrt{2})$ pro polynomy s koeficienty v $\mathbb{Q}$).

Úloha 5.4. Zdůvodněte, 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 $\mathbb{Q}[x]$,

(d) $\frac{10}{17}x^8 + 5x^6 + \frac{9}{2}x^5 - 12x^4 + \frac{4}{3}x - 6$ v $\mathbb{Q}[x]$,

(e) $x^3y + 2x^2y^2 + 2xy - x + y^4$ v $\mathbb{C}[x, y]$. (Nápověda: Nahlížejte jako na polynom v proměnné y.)

Řešení. (a) Jedná se o polynom stupně tři, proto kdyby byl reducibilní, 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. Tímto jsme zdůvodnili ireducibilitu v $\mathbb{Q}[x]$; díky primitivnosti a větě 8.5(2) dostáváme také ireducibilitu v $\mathbb{Z}[x]$.

(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 $\mathbb{Q}[x]$.

(d) Polynom nejprve převedeme na asociovaný primitivní celočíselný polynom přenásobením nejmenším společným násobkem jmenovatelů $2 \cdot 3 \cdot 17$

$$60x^8 + 17 \cdot 30x^6 + 17 \cdot 27x^5 - 17 \cdot 72x^4 + 17 \cdot 8x - 17 \cdot 36,$$

u nějž vidíme, že je díky Eisensteinově kritériu použitém pro prvočíslo 17 ireducibilní v $\mathbb{Z}[x]$. Nyní nám stejně jako v (c) dá ireducibilitu tohoto i každého s ním asociovaného polynomu v $\mathbb{Q}[x]$ věta 8.5(2).

(e) Nahlédneme-li na zadaný polynom p jako na prvek $(\mathbb{C}[x])[y]$, máme

$$y^4 + 2x^2y^2 + (x^3 + x)y - x,$$

kde vidíme, že abs. člen je dělitelný x (což je prvočinitel v oboru $\mathbb{C}[x]$), ovšem ne x^2, a zbývající členy vyjma toho s nejvyšší mocninou jsou také dělitelné x. Výsledek plyne z Eisensteinova kritéria.

Úloha 5.5. Najděte $a \in \mathbb{N}$ tak, aby byl hlavní ideál $a\mathbb{Z}$ oboru celých čísel roven ideálu

(a) $2\mathbb{Z} \cap 3\mathbb{Z}$, (b) $2\mathbb{Z} + 3\mathbb{Z}$, (c) $28\mathbb{Z} + 63\mathbb{Z}$, (d) $15\mathbb{Z} + 18\mathbb{Z} + 40\mathbb{Z}$, (e) $(-28)\mathbb{Z} \cap (-63)\mathbb{Z}$.

Řešení. (a) Stačí si všimnout, že $2\mathbb{Z} \cap 3\mathbb{Z}$ obsahuje právě společné násobky 2 a 3, tedy je generován nejmenším společným násobkem 6.

(b) Protože $1 = 3 - 2 \in 2\mathbb{Z} + 3\mathbb{Z}$, je tento ideál roven všem násobkům jedničky, tedy $2\mathbb{Z} + 3\mathbb{Z} = 1\mathbb{Z}$.

(c) Díky Bezoutovým koeficientům $u, v \in \mathbb{Z}$ víme, že

$$7 = \mathrm{NSD}(28, 63) = 28u + 63v \in 28\mathbb{Z} + 63\mathbb{Z},$$

proto $7\mathbb{Z} \subseteq 28\mathbb{Z} + 63\mathbb{Z}$. Naopak, protože $28 = 7 \cdot 4 \in 7\mathbb{Z}$ a $63 = 7 \cdot 9 \in 7\mathbb{Z}$, dostáváme z definice ideálu, že $28\mathbb{Z} + 63\mathbb{Z} \subseteq 7\mathbb{Z}$. Ověřili jsme, že $7\mathbb{Z} = 28\mathbb{Z} + 63\mathbb{Z}$.

(d) Dvojím aplikováním Bezoutovy rovnosti dostaneme rovnost

$$1 = \mathrm{NSD}(15, 18, 40) = \mathrm{NSD}(\mathrm{NSD}(15, 18), 40) = \mathrm{NSD}(3, 40) = 40 - 13 \cdot 3 = 40 - 13 \cdot 18 + 13 \cdot 15,$$

kde $3 = \mathrm{NSD}(15, 18) = 18 - 15$. Z rovnosti potom plyne, že $1 \in 15\mathbb{Z} + 18\mathbb{Z} + 40\mathbb{Z}$ a odtud stejně jako v (b) vidíme $1\mathbb{Z} = 15\mathbb{Z} + 18\mathbb{Z} + 40\mathbb{Z}$.

(e) Stejně jako v (a) si uvědomíme, že hledaný generátor je nejmenší společný násobek čísel -28 a -63, tedy $(-28)\mathbb{Z} \cap (-63)\mathbb{Z} = 252\mathbb{Z}$.

Úloha 5.6. Ať R je obor hlavních ideálů. Dokažte, že pro zadaná nenulová $a, b \in R$ je $aR \cap bR = cR$ a $aR + bR = dR$, kde $c = \mathrm{nsn}(a, b)$ a $d = \mathrm{NSD}(a, b)$.

Řešení. Platnosti obou tvrzení jsme si všimli v případě oboru celých čísel. Proveďme tedy formální důkaz.

Nejprve připomeňme. že $u \mid v$, právě když $vR \subseteq uR$ pro každou dvojici prvků $u, v \in R$. Protože $a, b \mid c$ a $d \mid a, b$, dostáváme inkluze $cR \subseteq aR \cap bR$ a $aR, bR \subseteq dR$. Protože je dR uzavřený na sčítání, platí i $aR + bR \subseteq dR$.

Protože jsou podle definice ideály $aR \cap bR$ i $aR + bR$ hlavní, existují prvky $e, f \in R$ takové, že $aR \cap bR = eR$, $aR + bR = fR$, tedy $fR \subseteq dR$ a $cR \subseteq eR$. Protože $f \mid a, b$, tedy jde o společný dělitel a, b a d je největší společný dělitel, dostáváme z definice, že $f \mid d$, tedy $dR \subseteq fR$, a proto $aR + bR = fR = dR$. Podobně $a, b \mid e$, tedy jde o společný násobek a, b a c je nejmenší společný násobek, dostáváme opět z definice, že $c \mid e$, tudíž $eR \subseteq cR$. To znamená, že $aR \cap bR = eR = cR$.

Úloha 5.7. Nechť $R = \mathbb{Z}[i]$. Najděte $a, b \in R$ taková, že

$$aR = (3+i)R + (4+2i)R \quad \text{a} \quad bR = (3+i)R \cap (4+2i)R.$$

Řešení. Využijeme-li výsledek úlohy 4.2(a), máme $\mathrm{NSD}(3+i, 4+2i) = 1+i$, a proto $\mathrm{nsn}(3+i, 4+2i) = \frac{(3+i)(4+2i)}{1+i} = 2(2+i)(2-i) = 10$. Aplikací tvrzení z úlohy 5.6 dostáváme, že

$$(1+i)R = (3+i)R + (4+2i)R, \quad 10R = (3+i)R \cap (4+2i)R.$$

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

Úloha 5.8. 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

$$\begin{aligned} 2x^2 + 2x - 1 &= (\sqrt{3}-1)(\sqrt{3}+1)\left(x + \frac{1}{2} + \frac{\sqrt{3}}{2}\right)\left(x + \frac{1}{2} - \frac{\sqrt{3}}{2}\right) = \\ &= (\sqrt{3}-1)\left(x + \frac{1}{2} + \frac{\sqrt{3}}{2}\right) \cdot (\sqrt{3}+1)\left(x + \frac{1}{2} - \frac{\sqrt{3}}{2}\right) = \big((\sqrt{3}-1)x + 1\big)\big((\sqrt{3}+1)x - 1\big) \end{aligned}$$

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 5.9. 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 5.10. 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 5.11. 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 o ireducibilní polynom. To znamená (podle cvičení 3.9), že i všechny polynomy $x^{2^k}+1$ jsou v $\mathbb{Z}[x]$ ireducibilní, tedy výše nalezený rozklad je ireducibilní.

Úloha 5.12. 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 5.13. 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 5.14. S využitím substituce $x \to x-a$ a tvrzení úlohy 3.9 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

$$\begin{aligned}(x+1)^4 + (x+1)^3 + (x+1)^2 + (x+1) + 1 = \\ = x^4 + 4x^3 + 6x^2 + 4x + 1 + x^3 + 3x^2 + 3x + 1 + x^2 + 2x + 1 + x + 1 = \\ = x^4 + 5x^3 + 10x^2 + 10x + 1 + 5\end{aligned}$$

Tento polynom je ireducibilní podle Eisensteinova kritéria pro prvočíslo 5 a tudíž je podle cvičení 3.9 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 kritéria 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 použitého pro p a cvičení 3.9 je upravený i původní polynom ireducibilní.

Úloha 5.15. 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 $a, b \in \mathbb{Z}[x]$ podmínku $\overline{a \cdot b} = \overline{a} \cdot \overline{b}$. 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 5.16. 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 5.15 znamená, že je polynom $x^5 + 4x^4 + 2x^3 + 3x^2 - x + 5$ ireducibilní v oboru $\mathbb{Z}[x]$.

Úloha 5.17. Nechť $S = \mathbb{Z}[x]$ a uvažujme ideály $I = 2S + xS$ a $J = 3S + xS$. Ukažte, že:

(a) I, J nejsou hlavní ideály,

(b) množina $\{ab \mid a \in I, b \in J\}$ netvoří ideál v okruhu S.

Řešení. (a) Kdyby ideály I a J byly hlavní, musely by být generovány dělitelem 2, resp. 3, který, protože jde o vlastní ideály, není invertibilní, tedy jde o ± 2 (resp. ± 3), čímž ale nenagenerujeme polynom x.

(b) Polynom x nelze napsat jako součin ab ze zadání; na druhou stranu, pokud by šlo o ideál, tak by v něm prvek x ležel, protože $2x$, $3x$ jsou daného tvaru součinu a ideál musí být uzavřený na sčítání (odčítání).

Úloha 5.18. Najděte v okruhu polynomů $R = \mathbb{Z}_5[x, y]$ ideál, který není hlavní.

Řešení. Obdobnou úvahou jako v předchozí úloze nahlédneme, že $xR + yR$, což je množina všech polynomů s nulovým absolutním členem, je netriviální ideál, který není hlavní, protože jeho generátor by musel dělit polynom x i y, což splňují pouze invertibilní prvky.