

### 3 Dobře rozložený polynom – hnojivo algebry

Řešení

Verze ze dne 4. března 2025

**Cíle cvičení:** Tentokrát se podíváme na otázku dělitelnosti, algoritmus dělení a proces rozkládání v okruzích polynomů. Všimneme si, že dělení se zbytkem celých čísel a reálných polynomů funguje obdobně také v obecných okruzích polynomů, a nad některými tělesy se polynomy naučíme rozkládat na součin dále nerozložitelných polynomů. Rovněž nám již známý výpočet největšího společného dělitele úspěšně aplikujeme na polynomy.

**Úlohy, které bychom určitě měli umět řešit:**

**Úloha 3.1.** Dělte se zbytkem polynomy

- (a)  $x^4 + 3x^3 + 4x^2 + x + 3$  a  $x^2 + 2$  v  $\mathbb{Z}[x]$ ,
- (b)  $x^4 + 3x^3 + 4x^2 + x + 3$  a  $x^2 + 2$  v  $\mathbb{Z}_5[x]$ ,
- (c)  $x^{10} + x^9 + x^7 + x^5 + x^3 + x^2 + x$  a  $x + 1$  v  $\mathbb{Z}_2[x]$ ,
- (d)  $x^n - 1$  a  $x^m - 1$  v oboru  $\mathbb{Z}[x]$ ,
- (e)  $xy^2 + y$  a  $x + y$  v oborech  $(\mathbb{Z}[x])[y]$  a  $(\mathbb{Z}[y])[x]$ .

**Řešení.** (a) Postupujeme standardně algoritmem dělení se zbytkem:

$$\begin{array}{r} x^4 + 3x^3 + 4x^2 + x + 3 : x^2 + 2 = x^2 + 3x + 2 \\ -x^4 \phantom{+ 3x^3} - 2x^2 \phantom{+ x} \phantom{+ 3} \\ \hline = 3x^3 + 2x^2 + x + 3 \\ -3x^3 \phantom{+ 2x^2} - 6x \phantom{+ 3} \\ \hline = 2x^2 - 5x + 3 \\ -2x^2 \phantom{- 5x} - 4 \\ \hline = -5x - 1 \end{array}$$

Spočítali jsme, že  $x^4 + 3x^3 + 4x^2 + x + 3 = (x^2 + 3x + 2)(x^2 + 2) - (5x + 1)$  v  $\mathbb{Z}[x]$ ,

(b) V oboru v  $\mathbb{Z}_5[x]$  stačí předchozí výsledek upravit modulo 5, proto dostaneme

$$x^4 + 3x^3 + 4x^2 + x + 3 = (x^2 + 3x + 2)(x^2 + 2) + 4.$$

(c) Stejným postupem jako v (a) ovšem s počítáním modulo 2 snadno spočteme, že

$$x^{10} + x^9 + x^7 + x^5 + x^3 + x^2 + x = (x^9 + x^6 + x^5 + x^2 + 1)(x + 1) + 1.$$

(d) Nejprve vydělíme se zbytkem  $n = qm + r$  v  $\mathbb{N}$ , kde  $0 \leq r < m$ , a poté nahlédneme (třeba pomocí dělení se zbytkem polynomů), že

$$x^{qm} - 1 = (x^m - 1) \sum_{i=0}^{q-1} x^{im},$$

tedy

$$x^n - x^r = x^r (x^m - 1) \sum_{i=0}^{q-1} x^{im},$$

a proto

$$x^n - 1 = x^r(x^m - 1) \sum_{i=0}^{q-1} x^{im} + x^r - 1.$$

Tedy dostáváme podíl  $x^r \sum_{i=0}^{q-1} x^{im} = \sum_{i=0}^{q-1} x^{im+r}$  a zbytek  $x^r - 1$ .

(e) Nejprve provedeme dělení v oboru  $(\mathbb{Z}[x])[y]$ , tedy chápeme uvedené polynomy jako s neznámou  $y$  a koeficienty v  $\mathbb{Z}[x]$ . Máme tedy

$$\begin{array}{r} xy^2 \quad +y \quad +0 \\ -xy^2 \quad -x^2y \\ \hline = (1-x^2)y \quad +0 \\ \quad -(1-x^2)y \quad -(x-x^3) \\ \hline = \quad \quad \quad x^3 - x \end{array} : y + x = xy + (1 - x^2).$$

Nyní provedeme dělení v oboru  $(\mathbb{Z}[y])[x]$ :

$$\begin{array}{r} y^2x \quad +y \\ -y^2x \quad -y^3 \\ \hline = y - y^3 \end{array} : y + x = y^2.$$

**Úloha 3.2.** Dokažte pomocí 3.1(d), že  $x^m - 1 \mid x^n - 1$  v  $\mathbb{Z}[x]$  právě tehdy, když  $m \mid n$ .

**Řešení.** Vidíme, že  $x^m - 1 \mid x^n - 1$ , právě když  $x^r - 1 = 0$ , což nastává právě tehdy, když  $r = 0$ , což je ekvivalentní podmínce  $m \mid n$ .

**Úloha 3.3.** Spočítejte v oborech  $\mathbb{C}[x]$ ,  $\mathbb{R}[x]$ ,  $\mathbb{Q}[x]$ ,  $\mathbb{Z}_3[x]$  a  $\mathbb{Z}_5[x]$  ireducibilní rozklady polynomů (a)  $x^3 - 2$ , (b)  $x^4 - x^2 - 2$ .

**Řešení.** V  $\mathbb{C}[x]$  se všechny polynomy rozkládají na kořenové činitele, které v našem případě snadno spočítáme:

$$x^3 - 2 = \prod_{j=0}^2 (x - e^{2\pi i j/3} \sqrt[3]{2}) = (x - \sqrt[3]{2}) \left( x + \frac{1}{\sqrt[3]{4}} + \frac{\sqrt{3}}{\sqrt[3]{4}} i \right) \left( x + \frac{1}{\sqrt[3]{4}} - \frac{\sqrt{3}}{\sqrt[3]{4}} i \right)$$

$$x^4 - x^2 - 2 = (x + i)(x - i)(x + \sqrt{2})(x - \sqrt{2}).$$

V oboru  $\mathbb{R}[x]$  sloučíme ryze komplexní kořeny polynomů do ireducibilního faktoru stupně 2:

$$x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4}), \quad x^4 - x^2 - 2 = (x^2 + 1)(x + \sqrt{2})(x - \sqrt{2}).$$

V oboru  $\mathbb{Q}[x]$  se musíme pomocí součinu zbavit faktorů z  $\mathbb{R}[x]$  obsahující iracionální koeficienty, to znamená, že  $x^3 - 2$  je ireducibilní (také si můžeme ekvivalentně uvědomit, že nemá žádné racionální kořeny a jeho stupeň je  $\leq 3$ ) a  $x^4 - x^2 - 2 = (x^2 + 1)(x^2 - 2)$ .

Nyní se podíváme na rozklady nad konečnými tělesy. Nejprve upravíme polynom  $x^3 - 2$  i rozklad  $x^4 - x^2 - 2 = (x^2 + 1)(x^2 - 2)$  modulo prvočíslo 3 a 5, a protože jsou všechny uvažované faktory stupně nejvýše 3, stačí z nich vytknout kořenové činitele. Tedy

$$x^3 - 2 = x^3 + 1 = (x + 1)^3, \quad x^4 - x^2 - 2 = (x^2 + 1)(x^2 + 1) = (x^2 + 1)^2 \in \mathbb{Z}_3[x],$$

$$x^3 - 2 = x^3 + 3 = (x + 2)(x^2 + 3x + 4), \quad x^4 - x^2 - 2 = (x^2 + 1)(x^2 + 3) = (x + 2)(x + 3)(x^2 + 3) \in \mathbb{Z}_5[x].$$

V oboru  $\mathbb{Z}_3[x]$  je polynom  $x^2 + 1$  nerozložitelný, jelikož je to kvadratický polynom bez kořene v  $\mathbb{Z}_3$ , a analogicky se také zdůvodní ireducibilita  $x^2 + 3 \in \mathbb{Z}_5[x]$ .

**Úloha 3.4.** Dokažte, že všechny ireducibilní polynomy v  $\mathbb{R}[x]$  mají stupeň  $\leq 2$ .

**Řešení.** Nechť  $f \in \mathbb{R}[x]$  je stupně aspoň 1. Pokud je  $f$  lichého stupně, víme, že má reálný kořen  $\alpha$ , proto  $(x - \alpha) \mid f$  v oboru  $\mathbb{R}[x]$  a  $f$  je v  $\mathbb{R}[x]$  ireducibilní, právě když  $\deg(f) = 1$ . Je-li  $f$  sudého stupně, pak sice reálný kořen mít nemusí, ale pokud má komplexní kořen  $\alpha \in \mathbb{C} \setminus \mathbb{R}$ , pak má za kořen i  $\bar{\alpha}$ . Označme  $s = (x - \alpha)(x - \bar{\alpha}) \mid f$ ; pak z  $(x - \alpha) \mid f$  a  $(x - \bar{\alpha}) \mid f$  máme  $s \mid f$  v  $\mathbb{C}[x]$ , zároveň ovšem  $s = x^2 + 2\operatorname{Re}(\alpha)x + |\alpha|^2 \in \mathbb{R}[x]$ , takže také  $f/s \in \mathbb{R}[x]$ . Je-li tedy  $f$  ireducibilní, musí v tomto případě mít stupeň 2.

**Úloha 3.5.** Najděte všechny ireducibilní polynomy nad  $\mathbb{Z}_2$  stupně nejvýše 3.

**Řešení.** Nulové ani konstantní polynomy nad tělesem z definice nejsou ireducibilní. Protože je polynom kladného stupně nad tělesem ireducibilní, právě když ho nelze napsat jako součin dvou polynomů kladného stupně, a protože víme, že  $\deg(ab) = \deg(a) + \deg(b)$  pro všechny nenulové polynomy  $a, b$ , jsou oba polynomy stupně 1, tedy  $x, x + 1$  jistě ireducibilní. Dále si uvědomíme, že polynomy stupně 2 a 3 jsou ireducibilní, právě když nemají faktor stupně 1, což nastává právě tehdy, když nemají kořen. Protože polynom má kořen 0, právě když má nulový absolutní člen a nad  $\mathbb{Z}_2$  má kořen 1, právě když obsahuje sudý počet nenulových monomů  $x^j$ , hledáme právě polynomy s absolutním členem 1 a lichým počtem nenulových monomů, jimž jsou právě polynomy  $x^2 + x + 1, x^3 + x + 1, x^3 + x^2 + 1$ . Existuje tedy právě 5 ireducibilních polynomů nad  $\mathbb{Z}_2$  stupně nejvýše 3:

$$x, \quad x + 1, \quad x^2 + x + 1, \quad x^3 + x + 1, \quad x^3 + x^2 + 1.$$

**Úloha 3.6.** Pro následující dvojice polynomů spočítejte NSD( $f, g$ ) a určete také Bézoutovy koeficienty.

(a)  $f = x^3 + 2, g = x^2 - 2x + 2$  v  $\mathbb{R}[x]$ ,

(b)  $f = x^4 + 3x^2 + 2, g = x^3 + x^2 + x + 1$  v  $\mathbb{Z}_5[x]$ .

**Řešení.** (a) Postupujeme rozšířeným Eukleidovým algoritmem:

$a_i$	$u_i$	$v_i$
$x^3 + 2$	1	0
$x^2 - 2x + 2$	0	1
$2x - 2$	1	$-x - 2$
1	$\frac{1}{2}(1 - x)$	$\frac{1}{2}(x^2 + x)$
0		

kde jsme v průběhu spočetli, že

$$\begin{aligned} x^3 + 2 : x^2 - 2x + 2 &= x + 2 \quad \text{zb. } 2x - 2, \\ x^2 - 2x + 2 : 2x - 2 &= \frac{1}{2}x - \frac{1}{2} \quad \text{zb. } 1. \end{aligned}$$

(b) zcela obdobně máme

$a_i$	$u_i$	$v_i$
$x^4 + 3x^2 + 2$	1	0
$x^3 + x^2 + x + 1$	0	1
$3x^2 + 3$	1	$4x + 1$
0		

Jelikož je NSD polynomů nad tělesem určen jednoznačně až na přenásobení nenulovou konstantou, můžeme si namísto  $3x^2 + 3$  vzít  $x^2 + 1$ , což dá Bézoutovu rovnost  $x^2 + 1 = 2f + (3x + 2)g$ .

**Úloha 3.7.** Máme-li obor  $R$ , polynom  $f \in R[x]$  a prvek  $a \in R$ , co je (zcela obecně) zbytkem po dělení  $f$  dvočlenem  $x - a$ ?

**Řešení.** Jelikož zbytek musí mít stupeň menší než dělitel, musí jít o konstantní polynom. Je-li  $q \in R[x]$  (neúplný) podíl a  $r \in R$  zbytek, tj.  $f = (x - a) \cdot q + r$ , pak dosazením  $a$  za  $x$  v této rovnosti dostáváme

$$f(a) = (a - a) \cdot q(a) + r = r,$$

tedy  $r = f(a)$ .

## A teď něco pro zlepšení nálady:

**Úloha 3.8.** Najděte všechny ireducibilní polynomy nad  $\mathbb{Z}_2$  stupně 4.

**Řešení.** Využijeme zjištění 3.5, kde jsme nahlédli, že nerozložitelný polynom nutně obsahuje absolutní člen 1 a lichý počet nenulových monomů a navíc si všimneme, že nesmí být součinem dvou ireducibilních polynomů stupně 2. Protože  $x^2 + x + 1$  je jediný ireducibilní polynom stupně 2, jediný rozložitelný polynom stupně 4 splňující předchozí dvě podmínky je polynom  $x^4 + x^2 + 1 = (x^2 + x + 1)^2$ . Tedy polynomy  $x^4 + x + 1$ ,  $x^4 + x^3 + 1$ ,  $x^4 + x^3 + x^2 + x + 1$  jsou právě všechny ireducibilní polynomy stupně 4 nad  $\mathbb{Z}_2$ .

**Úloha 3.9.** Dokažte, že pro každé  $t \in \mathbb{Q}$  a  $f(x) \in \mathbb{Q}[x]$  platí, že je  $f(x)$  ireducibilní v  $\mathbb{Q}[x]$ , právě když je  $f(x + t)$  ireducibilní v  $\mathbb{Q}[x]$ .

**Řešení.** Nejprve si všimneme, že pro libovolnou trojici polynomů  $a, b, s \in \mathbb{Q}[x]$  platí pro substituci  $s$  za neznámou  $x$  do polynomů  $a, b$ , že  $(a \cdot b)(s) = a(s) \cdot b(s)$ . Navíc jsou-li polynomy  $a, s$  nenulové, pak  $\deg(a(s)) = \deg(a) \cdot \deg(s)$ .

Je-li tedy polynom  $f$  rozložitelný, existují polynomy  $a, b \in \mathbb{Q}[x]$  kladného stupně, pro něž  $f = a \cdot b$ , proto

$$f(x - t) = a(x - t) \cdot b(x - t), \quad \text{kde } \deg(a(x - t)) = \deg(a) > 0, \quad \deg(b(x - t)) = \deg(b) > 0,$$

tedy polynom  $f(x - t)$  je rozložitelný. Naopak, je-li  $f(x - t)$  rozložitelný, existují  $c, d \in \mathbb{Q}[x]$  kladného stupně pro něž  $f(x - t) = c \cdot d$ , a tudíž

$$f = f((x + t) - t) = c(x + t) \cdot d(x + t) \quad \text{pro } \deg(c(x + t)) = \deg(c) > 0, \quad \deg(d(x + t)) = \deg(d) > 0.$$

Dokázali jsme obměnu požadované ekvivalence.

**Úloha 3.10.** Najděte polynom  $f \in \mathbb{Z}[x]$  co nejmenšího stupně takový, že čísla 1 a  $i$  jsou jeho kořeny a  $f(3) = f(4)$ .

**Řešení.** Protože  $f(i) = 0$ , plyne z úvahy řešení 3.4, že  $x^2 + 1 = (x + i)(x - i)$  je ireducibilní faktor hledaného polynomu  $f$  v  $\mathbb{R}[x]$ , a protože je vedoucí koeficient  $x^2 + 1$  invertibilní v  $\mathbb{Z}$ , jedná se o faktor  $f$  v oboru  $\mathbb{Z}[x]$ . Podobně  $(x - 1)$  dělí polynom  $f$ , neboť 1 je jeho kořenem. Proto  $g = (x - 1)(x^2 + 1)$  dělí polynom  $f$  a zkusíme najít takový celočíselný lineární polynom  $ax + b$ , aby  $f = (ax + b)g$  a platilo poslední podmínka  $f(3) = f(4)$ :

$$60a + 20b = 20(3a + b) = (3a + b)g(3) = f(3) = (4a + b)g(4) = 51(4a + b) = 204a + 51b.$$

Odtud dostáváme lineární rovnici  $144a + 31b = 0$ , která má celočíselné řešení například  $a = -31$ ,  $b = 144$ . Nyní zbývá dopočítat:

$$f = (-31x + 144)(x - 1)(x^2 + 1) = (-31x^2 + 175x - 144)(x^2 + 1) = -31x^4 + 175x^3 - 175x^2 + 175x - 144.$$

**Úloha 3.11.** Je-li  $p$  prvočíslo a  $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ , dokažte, že v oboru  $\mathbb{Z}_p[x]$  platí

(a)  $x - j$  dělí  $x^{p-1} - 1$  pro každé  $j \in \mathbb{Z}_p^*$ ,

(b)  $x^{p-1} - 1 = \prod_{j \in \mathbb{Z}_p^*} (x - j)$ .

**Řešení.** (a) Nechť  $j \in \mathbb{Z}_p^*$ . Z malé Fermatovy věty víme, že  $j^{p-1} \equiv 1 \pmod{p}$ , proto je  $j$  kořenem polynomu  $x^{p-1} - 1$ , což podle tvrzení 3.3 z přednášky znamená, že  $(x - j) \mid x^{p-1} - 1$ .

(b) Využijeme toho, že jsme si v (a) uvědomili, že všechna  $j \in \mathbb{Z}_p^*$  jsou kořeny polynomu  $x^{p-1} - 1$  a okamžitě vidíme, že všechna  $j \in \mathbb{Z}_p^*$  jsou i kořenem polynomu  $\prod_{j \in \mathbb{Z}_p^*} (x - j)$ . Oba polynomy jsou stupně  $p - 1$  a mají stejný vedoucí koeficient 1, proto je jejich rozdíl polynom stupně menšího než  $p - 1$ , který má  $p - 1$  různých kořenů. Podle věty 3.4 se nutně jedná o nulový polynom, a tudíž  $x^{p-1} - 1 = \prod_{j \in \mathbb{Z}_p^*} (x - j)$ .

★ **Úloha 3.12.** Necht' jsou  $p, q$  dvě různá lichá prvočísla.

(a) Dokažte, že má polynom  $x^3 + 3x^2 + 2x$  v okruhu  $\mathbb{Z}_{pq}$  právě 9 kořenů.

(b) Rozhodněte, zda existují  $a, b \in \mathbb{Z}_{pq}$ , aby měl polynom  $x^2 + ax + b$  v okruhu  $\mathbb{Z}_{pq}$  právě 3 kořeny.

**Řešení.** (a) Nejprve si všimneme, že  $f = x^3 + 3x^2 + 2x = x(x+1)(x+2)$ , tedy pro polynom platí, že má v  $\mathbb{Z}_p$  i  $\mathbb{Z}_q$  právě kořeny  $0, -1, -2$ . Protože  $p, q > 2$  jedná se v obou případech o tři různé kořeny a pomocí kongruencí můžeme pozorování zapsat ve tvaru

$$f(\xi) \equiv 0 \pmod{p} \ \& \ f(\xi) \equiv 0 \pmod{q} \Leftrightarrow \exists a, b \in \{0, -1, -2\} : \begin{cases} \xi \equiv a \pmod{p} \\ \xi \equiv b \pmod{q} \end{cases} .$$

Nyní nám Čínská věta o zbytcích zaručuje pro každou volbu  $a, b \in \{0, -1, -2\}$  existenci právě jednoho  $\xi \in \mathbb{Z}_{pq}$  splňujícího kongruence vpravo, z nichž každé je právě jedním z kořenů polynomu  $f$  v  $\mathbb{Z}_{pq}$ . Protože dvojic  $a, b$  máme  $3^2 = 9$ , ověřili jsme, že polynom  $f$  má právě 9 různých kořenů.

(b) Taková  $a, b \in \mathbb{Z}_{pq}$  neexistují. Předchozí úvaha nám říká, že by polynom musel mít například v tělese  $\mathbb{Z}_p$  3 kořeny (a v tom druhém  $\mathbb{Z}_q$  pak jeden), což pro kvadratický polynom nad tělesem není možné.

**Úloha 3.13.** Najděte polynom  $f \in \mathbb{Z}_{15}[x]$  stupně 3, který má aspoň 9 různých kořenů v okruhu  $\mathbb{Z}_{15}$ .

**Řešení.** Můžeme využít předchozí úlohu, která říká, že požadované vlastnosti má pro  $p = 3$ , a  $q = 5$  polynom  $x^3 + 3x^2 + 2x$  nebo můžeme zvolit například polynom  $x(x+2)(x+4)$  a obdobnou argumentací ukázat, že má rovněž 9 kořenů.

**Úloha 3.14.** Buď  $T$  těleso,  $f \in T[y]$  a  $h \in T[x, y]$ . Dokažte, že  $(x - f) \mid h$  v  $T[x, y]$  právě tehdy, když  $h(f, y) = 0$ .

**Řešení.** Díky distributivitě násobení víme, že  $(T[x])[y] = T[x, y] = (T[y])[x]$ . Na  $h$  se stačí dívat jako na polynom v proměnné  $x$  nad oborem  $T[y]$  a použít Tvzení 3.3 ze skript.

★ **Úloha 3.15.** Buď  $u \in T$  kořen polynomu  $f = \sum_{i=0}^n f_i x^i \in T[x]$ , jehož absolutní člen je nenulový. Vyjádřete  $u^{-1}$  jako lineární kombinaci mocnin prvku  $u$  (s nezáporným exponentem).

**Řešení.** Protože  $f_0 = -\sum_{i=1}^n f_i u^i$ , stačí rovnost vydělit prvkem  $f_0 u$ , kde  $u \neq 0$ , protože jde o kořen polynomu s nenulovým absolutním členem, čímž dostáváme  $u^{-1} = -f_0^{-1} \sum_{i=1}^n f_i u^{i-1}$ .

**Úloha 3.16.** Dokažte, že různé polynomy určují nad nekonečným tělesem různá polynomiální zobrazení.

**Řešení.** Jsou-li  $f, g$  dva různé polynomy, pak  $f - g \neq 0$ , a proto má  $f - g$  nejvýše  $\deg(f - g)$  kořenů. Uvažované těleso je nekonečné, proto určitě existuje jeho prvek  $a$ , který není kořenem  $f - g$ , tedy  $(f - g)(a) \neq 0$  a  $f(a) \neq g(a)$ .

**Úloha 3.17.** Rozhodněte, zda je polynom  $x^4 + x^2 + 1$  ireducibilní v oboru  $\mathbb{Z}_5[x]$ .

**Řešení.** Snadno ověříme, že polynom v  $\mathbb{Z}_5$  nemá kořen, tedy zbývá prověřit možnost, zda jde rozložit na součin dvou kvadratických polynomů. Po chvíli líteho boje zjistíme  $x^4 + x^2 + 1 = (1 + x + x^2)(1 + 4x + x^2)$ , tedy polynom není ireducibilní.

**Úloha 3.18.** Najděte všechny ireducibilní polynomy stupně nejvýše 3 v  $\mathbb{Z}_3[x]$

**Řešení.** Postupujeme obdobně jako v 3.5, tedy vezmeme všechny lineární polynomy a dále vybíráme polynomy s nenulovým absolutním členem (tedy ty bez kořenu 0), jejichž kořen není 1 ani  $2 = -1$  (snáze se počítají mocniny s dosazením prvku  $-1$ ). Dostaneme až na přenásobení konstantou ze  $\mathbb{Z}_3^*$  právě polynomy:

$$x, x + 1, x + 2, x^2 + 1, x^2 + x + 2, x^2 + 2x + 2, x^3 + 2x + 1, x^3 + 2x + 2, x^3 + x^2 + 2, \\ x^3 + 2x^2 + 1, x^3 + x^2 + x + 2, x^3 + x^2 + 2x + 1, x^3 + 2x^2 + x + 1, x^3 + 2x^2 + 2x + 2.$$

**Úloha 3.19.** Najděte v  $\mathbb{Z}[x]$  ireducibilní polynom, jehož kořenem je číslo  $a = e^{\pi i/3}$ .

**Řešení.** Víme, že platí  $a^3 = -1$ , tedy  $a$  je kořenem polynomu  $x^3 + 1$ , který má ale za kořen i číslo  $-1$ , tedy hledaným polynomem  $x^2 - x + 1 = (x^3 + 1)/(x + 1)$ .

**Úloha 3.20.** Porovnejte pomocí inkluze podobory tělesa komplexních čísel a ukažte, které z inkluzí jsou ostré:

- (a)  $\mathbb{Z}[\sqrt{6}]$ ,  $\mathbb{Z}[\sqrt{24}]$ ,  $\mathbb{Z}[\sqrt{2}, \sqrt{3}]$ ,
- (b)  $\mathbb{Q}[\sqrt{6}]$ ,  $\mathbb{Q}[\sqrt{24}]$ ,  $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ ,
- (c)  $\mathbb{Z}[\sqrt{2}, \sqrt{3}]$ ,  $\mathbb{Z}[\sqrt{2} + \sqrt{3}]$ ,  $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$  a  $\mathbb{Q}[\sqrt{2} + \sqrt{3}]$ ,

**Řešení.** (a) Protože  $\sqrt{24} = 2 \cdot \sqrt{6}$  a  $\sqrt{6} = \sqrt{2} \cdot \sqrt{3}$  dostáváme inkluze  $\mathbb{Z}[\sqrt{24}] \subseteq \mathbb{Z}[\sqrt{6}] \subseteq \mathbb{Z}[\sqrt{2}, \sqrt{3}]$ . Naopak, rovnice  $\sqrt{6} = a + b \cdot 2\sqrt{6}$  má v racionálním oboru pouze řešení  $(0, \frac{1}{2})$ , tudíž zjišťujeme, že  $\sqrt{6} \notin \mathbb{Z}[\sqrt{24}]$ . Protože jsou prvky  $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$  lineárně nezávislé (důkaz není těžký – zkuste sami), platí, že  $\sqrt{2}, \sqrt{3} \notin \mathbb{Z}[\sqrt{6}]$  a máme ostré inkluze

$$\mathbb{Z}[\sqrt{24}] \subsetneq \mathbb{Z}[\sqrt{6}] \subsetneq \mathbb{Z}[\sqrt{2}, \sqrt{3}]$$

(b) Stejná argumentace jako v (a) nám tentokrát dává  $\mathbb{Q}[\sqrt{6}] = \mathbb{Q}[\sqrt{24}] \subseteq \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ , protože  $\sqrt{6} = \frac{1}{2}\sqrt{24}$ . Navíc i nad racionálními čísly platí, že  $\sqrt{2}, \sqrt{3} \notin \mathbb{Q}[\sqrt{6}]$ , tudíž

$$\mathbb{Q}[\sqrt{24}] = \mathbb{Q}[\sqrt{6}] \subsetneq \mathbb{Q}[\sqrt{2}, \sqrt{3}]$$

(c) Nejprve si všimneme, že pokud  $a = \sqrt{2} + \sqrt{3}$ , pak

$$\sqrt{2} = \frac{a^2 - 5}{2} \cdot a - 2a, \quad \sqrt{3} = 3a - \frac{a^2 - 5}{2} \cdot a$$

proto  $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$ . Vidíme, že  $\mathbb{Z}[\sqrt{2} + \sqrt{3}] \subseteq \mathbb{Z}[\sqrt{2}, \sqrt{3}] \subsetneq \mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$  a zbývá si rozmyslet, že  $\sqrt{2} \notin \mathbb{Z}[\sqrt{2} + \sqrt{3}]$ . To platí, protože pro  $\alpha = \sqrt{2} + \sqrt{3}$  máme  $\mathbb{Z}[\alpha] = \{a + b\alpha + c\alpha^2 + d\alpha^3 \mid a, b, c, d \in \mathbb{Z}\}$ , zatímco  $\sqrt{2} = \frac{1}{2}\alpha^3 - \frac{9}{2}\alpha \notin \mathbb{Z}[\alpha]$ . Zjistili jsme, že

$$\mathbb{Z}[\sqrt{2} + \sqrt{3}] \subsetneq \mathbb{Z}[\sqrt{2}, \sqrt{3}] \subsetneq \mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}].$$