1. Dělitelnost

Připomeňme, že komutativní okruh $(R, +, -, 0, \cdot, 1)$ nazveme oborem integrity, platí-li pro každou dvojici nenulových prvků $a, b \in R$, že $a \cdot b \neq 0$. O oboru integrity hlavních ideálů mluvíme v případě, že jsou všechny jeho ideály hlavní, tj. tvaru $iR = \{i \cdot r | \ r \in R\}$. Dobře známými příklady oborů integrity jsou okruhy celých čísel $(\mathbf{Z}, +, -, 0, \cdot, 1)$ či reálných (resp. racionálních) polynomů $(\mathbf{R}[x], +, -, 0, \cdot, 1)$ (resp. $(\mathbf{Q}[x], +, -, 0, \cdot, 1)$). O oboru $(\mathbf{Z}, +, -, 0, \cdot, 1)$ víme, že jde o oboru integrity hlavních ideálů a o polynomech nad tělesy to bude brzo dokázáno.

Buď $(R, +, -, 0, \cdot, 1)$ obor integrity a $a, b \in R$. V souladu s pojmem dělitelnosti na celých číslech nebo reálných polynomech řekneme, že *a dělí b* (píšeme a/b), existuje-li takové $c \in R$, že $b = a \cdot c$. Dále řekneme, že je *a asociováno s b* (píšeme $a \| b$), jestliže a/b a b/a.

Všimněme si, že v oboru integrity 0 dělí pouze opět 0 (a tedy s 0 je asociována jen 0), obvykle ji proto z našich úvah budeme vypouštět. V následujícívh úvahách si nejprve uvědomíme, jak vyjádřit otázky dělitelnosti pomocí ideálů.

1.1. Nechť $(R, +, -, 0, \cdot, 1)$ je obor integrity a $a, b \in R \setminus \{0\}$.

(1) Dokažte, že a/b, právě když $bR \subseteq aR$.
(2) Dokažte, že $a \| b$, právě když $aR = bR$.
(3) Dokažte, že $a \| b$, právě když existuje invertibilní $u \in R$, pro které $b = a \cdot u$.

(1) $(\Rightarrow)$ Existuje-li $c \in R$, pro které $b = a \cdot c$, pak $b \in aR$, a proto i $b \cdot s \in aR$ pro každé $s \in R$.

$(\Leftarrow)$ Máme-li $bR \subseteq aR$, potom $b = b \cdot 1 \in bR \subseteq aR$, tedy existuje takové $c \in R$, že $b = a \cdot c$

(2) Stačí dvakrát použít (1).

(3) $(\Rightarrow)$ Protože a/b, existuje $u \in R$, pro nějž $b = a \cdot u$, a protože také b/a existuje takové $v \in R$, že $a = b \cdot v$, Dosadíme-li do první rovnosti, dostaneme

$$b = a \cdot u = (b \cdot v) \cdot u = b \cdot (v \cdot u),$$

a proto $b \cdot (1 - v \cdot u) = 0$. Z definice oboru integrity je $1 - v \cdot u = 0$, tedy $v \cdot u = 1$ a u je invertibilní prvek.

$(\Leftarrow)$ Okamžitě z předpokladu $b = a \cdot u$ máme a/b. Protože $a = b \cdot u^{-1}$, vidíme, že b/a. $\square$

1.2. Je-li $(R, +, -, 0, \cdot, 1)$ okruh a $a, b \in R$, dokažte, že $aR + bR = \{ar + bs | \ r, s \in R\}$ je nejmenší pravý ideál obsahující hlavní ideály aR a bR.

Nejprve ukážeme, že množina $aR + bR$ tvoří pravý ideál. Předně $0 = a \cdot 0 + b \cdot 0 \in aR + bR$. Zvolme $x_i \in aR + bR$ pro $i = 1, 2$ a $u \in R$ libovolně. Potom existuje $r_i, s_i \in R$, pro něž $x_i = ar_i + bs_i$, a proto $-x_1 = a \cdot (-r_1) + b \cdot (-s_1) \in aR + bR$, dále $x_1 + x_2 = a \cdot (r_1 + r_2) + b \cdot (s_1 + s_2) \in aR + bR$ a $x_1 \cdot u = a \cdot (r_1 \cdot u) + b \cdot (s_1 \cdot u) \in aR + bR$.

Protože $a \cdot r = a \cdot r + b \cdot 0 \in aR + bR$ a $b \cdot r = a \cdot 0 + b \cdot r \in aR + bR$, pro každé $r \in R$. Navíc přímo podle definice pravého ideálu musí každý pravý ideál obsahující aR a bR obsahovat i $aR + bR$. $\square$

Ze známých příkladů oborů integrity $(\mathbf{Z}, +, -, 0, \cdot, 1)$ a $(\mathbf{R}[x], +, -, 0, \cdot, 1)$ zobecníme pojem největšího společného dělitele. Je-li $(R, +, -, 0, \cdot, 1)$ obor integrity a

$A \subseteq R$, řekneme, že je $c \in R$ *největší společný dělitel* prvků A (píšeme c je $\mathrm{NSD}(A)$), jestliže c/a pro všechna $a \in A$, a pokud pro nějaké $d \in R$ platí, že d/a pro všechna $a \in A$, potom d/c

1.3. Je-li $(R, +, -, 0, \cdot, 1)$ obor integrity hlavních ideálů a $a, b \in R \setminus \{0\}$, dokažte, že $aR + bR = cR$ právě tehdy, když c je $\mathrm{NSD}(a, b)$.

($\Rightarrow$) Předpokládejme, že $aR + bR = cR$. Potom podle 1.2 máme $aR, bR \subseteq cR$, a proto podle 1.1 je c/a a c/b. Vezmeme-li $d \in R$, pro něž d/a a d/b, tedy díky 1.1 $aR, bR \subseteq dR$. Z minimality $aR + bR = cR$, potom dostáváme, že $cR = aR + bR \subseteq dR$, tedy d/c.

($\Leftarrow$) Je-li c je $\mathrm{NSD}(a, b)$ a vezmeme-li takové $d \in R$, že $aR + bR = dR$ (to musí existovat, protože každý ideál $(R, +, -, 0, \cdot, 1)$ je hlavní), pak i d je $\mathrm{NSD}(a, b)$, proto jsou podle definice NSD prvky c a d asociovány a 1.1 říká, že $aR + bR = dR = cR$. $\square$

Připomeňme ve formě, která nám snadno umožní zobecnění, jakým způsobem se sčítají a násobí reálné polynomy $p = \sum_{n \in \mathbf{N}_0} p_n x^n, q = \sum_{n \in \mathbf{N}_0} q_n x^n \mathbf{R}[x]$ (zdůrazněme, že jen konečně mnoho koeficientů p_n a q_n je nenulových):

$$p + q = \sum_{n \in \mathbf{N}_0} (p_n + q_n) x^n, \qquad p \cdot q = \sum_{n \in \mathbf{N}_0} \Big(\sum_{i+j=n} p_i \cdot q_j \Big) x^n,$$

Zaměníme-li v definici monoid $(\mathbf{N}_0, +, 0)$, přesněji řečeno jemu izomorfní momoid $(\{x^i |\ i \in \mathbf{N}_0), x^0)$, obecným monoidem $(M, \cdot, 1)$ a těleso reálných čísel obecným okruhem, dostáváme právě definici sčítání a násobení na monoidovém okruhu.

4.3.

1.4. Označme monoid $\mathcal{G} = (G, \cdot, 1)$ izomorfní monoidu $(\mathbf{Z}_2, +, 0)$, tj. $G = \{1, g\}$ a $g \cdot g = 1 \cdot 1 = 1$, $g \cdot 1 = 1 \cdot g = g$. Je-li $\mathcal{Q}$ okruh racionálních čísel, uvažujme monoidový okruh $\mathcal{Q}\mathcal{G}$.

(a) Popište operace okruhu $\mathcal{Q}\mathcal{G} = (\mathbf{Q}G, +, -, \mathbf{0}, \cdot, \mathbf{1})$,
(b) rozhodněte, zda je $\mathcal{Q}\mathcal{G}$ obor integrity,
(c) popište nilpotentní prvky okruhu $\mathcal{Q}\mathcal{G}$ (tj. prvky p, pro něž existuje takové kladné n, že $p^n = 0$),
(d) najděte ideál I okruhu polynomů $\mathbf{Q}[x]$, aby $\mathbf{Q}[x]/I \cong \mathbf{Q}G$.

(a) Obecný prvek je tvaru $ag+b = ag+b1$, kde $a, b \in \mathbf{Q}$. Pro prvky $ag+b, cg+d \in \mathbf{Q}G$ popišme sčítání a násobení:

$$(ag + b) + (cg + d) = (a + c)g + (b + d)$$

$$(ag + b) \cdot (cg + d) = (ad + bc)g + (ac + bd)$$

Připomeňmě také, že $\mathbf{0} = 0g + 0$, $\mathbf{1} = 0g + 1$ a $-(ag + b) = (-a)g + (-b)$. Všimněme se, že sčitat a násobit prvky monoidového okruhu lze zcela „formálně", tj. s využitím u okruhu očekávané distributivity. Navíc připomeňme, že členy s nulovým koeficientem v zápisu můžeme vynechat, tj. například píšeme ag místo $ag + 0$.

(b) Uvědomíme-li, že $1g \cdot 1g = \mathbf{1}$, pak vidíme, že $(1g + 1) \cdot (1g - 1) = 0$, tedy součin dvou nenulových prvků okruhu je nulový a okruh $\mathcal{Q}\mathcal{G}$ není oborem integrity.

(c) Nejprve poznamenejme, že nula je vždy nilpotentní prvek, a uvědomme si, že existuje-li v okruhu nenulový nilpotentní prvek p, potom existuje nenulový prvek q, pro který $q^2 = 0$. Abychom to ověřili, stačí vzít nenulový nilpotentní prvek p a nejmenší kladné n, pro nějž $p^n = 0$. To znamená, že $n > 1$, $q = p^{n-1} \neq 0$ a $q^2 = p^{2n-2} = 0$.

Zeptáme se tedy nejprve na existenci prvků $ag + b \in \mathbf{Q}G$, pro které $(ag + b)^2 = (2ab)g + (a^2 + b^2) = 0$. Vidíme, že $a^2 + b^2 = 0$ a $2ab = 0$, proto nutně $a = b = 0$. Zjsitili jsme, že okruh $\mathcal{QG}$ obsahuje pouze nulový nilpotentní prvek.

(d) Z přednášky víme, že monoidový homomorfismus $\mathbf{N}_0 \to G$ daný $n \to g^{(n)\text{mod}2}$ lze rozšířit na okruhový homomorfismus $\varphi : \mathbf{Q}[x] \to \mathbf{Q}G$ vztahem $\varphi(\sum_i a_i x^i) = (\sum_i a_{2i+1})g + (\sum_i a_{2i})$. Protože $\varphi(ax^1 + bx^0) = ag + b$, jde o homomorfismus na $\mathbf{Q}G$, využijeme-li 1. větu o izomorfismu pro okruhy, dostaneme $\mathbf{Q}[x]/\text{Ker}\varphi \cong \mathbf{Q}G$. Zbývá nám popsat ideál $I = \text{Ker}\varphi$. Z přednášky víme, že je ideál I hlavní, navíc jeho generátorem je právě nenulový polynom nejmenšího možného stupně, který v I leží. Přímočaře nahlédneme, že $\varphi(x^2 - 1) = 0$, tedy $x^2 - 1 \in I$ a $\varphi(ax + b) = ag + b \neq 0$ pro žádný nenulový polynom $ax + b$, proto $I = (x^2 - 1)\mathbf{Q}[x]$. □

1.5. Dokažte, že ideál $I = x\mathbf{Z}[x] + 2\mathbf{Z}[x]$ (tj. množina všech celočíselných polynomů se sudým absolutním členem) okruhu $\mathbf{Z}[x]$ není hlavní.

Předpokládejme, že ideál I hlavní je, tedy že existuje jeho generátor a, což znamená, že $I = a\mathbf{Z}[x]$. Protože $2\mathbf{Z}[x] \subseteq a\mathbf{Z}[x]$, vidíme, že $a/2$, tj. $a \in \{1, -1, 2, -2\}$. Podobně $x\mathbf{Z}[x] \subseteq a\mathbf{Z}[x]$, a proto a/x a $a \in \{1, -1, x, -x\}$. Tedy a je nutně invertibilní prvek, tudíž $I = a\mathbf{Z}[x] = \mathbf{Z}[x]$. Protože zřejmě $1 \notin I$, dostáváme spor, tedy ideál I nemůže být hlavní. □

11.3.

1.6. Najděte v okruhu $(\mathbf{Z}[x], +, -, 0, \cdot, 1)$ největší společný dělitel prvků 2 a x.

V 1.5 jsme zjistili, že společní dělitelé prvků 2 a x jsou jen 1 a -1 oba prvky jsou tedy podle definice největší společní dělitelé 2 a x. □

1.7. Je-li $p \in \mathbf{Z}[x] \setminus \{0\}$ a $q \in \mathbf{Q}[x] \setminus \{0\}$, dokažte, že

(a) existuje $c \in \mathbf{Z}$ a $s = \sum_i s_i x^i \in \mathbf{Z}[x]$, pro která 1 je $\text{NSD}(s_0, \dots, s_{\deg(s)})$ a $p = c \cdot s$,
(b) existuje $c \in \mathbf{Z} \setminus \{0\}$ a $r \in \mathbf{Z}[x]$, pro která $q = \frac{1}{c} \cdot r$,
(c) existuje $d \in \mathbf{Q}$ a $s = \sum_i s_i x^i \in \mathbf{Z}[x]$, pro která 1 je $\text{NSD}(s_0, \dots, s_{\deg(s)})$ a $q = d \cdot s$.

(a) Je-li $p = \sum_i p_i x^i$, stačí z p vytknout $\text{NSD}(p_0, \dots, p_{\deg(p)})$.

(b) Je-li $q = \sum_i \frac{a_i}{b_i} x^i \in \mathbf{Q}[x]$, kde $a_i, b_i \in \mathbf{Z}$ a $b_i \neq 0$, stačí, abychom položili $c = \text{NSD}(b_0, \dots, b_{\deg(q)})$ a pak $r = c \cdot q \in \mathbf{Z}[x]$.

(c) Zkombinujeme (a) a (b). □

1.8. Rozhodněte, zda jsou v okruhu $(\mathbf{Z}[x], +, -, 0, \cdot, 1)$ hlavní ideály:

(a) fundamentální ideál $\{\sum_i p_i x^i \in \mathbf{Z}[x] | \sum_i p_i = 0\}$,
(b) $\{p \in \mathbf{Z}[x] | p(\frac{1}{2}) = 0\}$,

(c) $(x^2-1)\mathbf{Z}[x]+(x^2+3x+2)\mathbf{Z}[x]$,

(a) Všimněme si, že $x-1 \in J_a = \{\sum_i p_i x^i \in \mathbf{Z}[x] |\ \sum_i p_i = 0\}$, tedy máme inkluzi $(x-1)\mathbf{Z}[x] \subseteq J_a$. Zvolíme-li $p \in \mathbf{J}_a$, můžeme p podle věty z přednášky vydělit se zbytkem polynomem $x-1$, tj. existují polynomy $q, z \in \mathbf{Z}[x]$, pro které $p = q \cdot (x-1) + z$ a $\deg(z) < \deg(x-1) = 1$. Vidíme, že $z = p - q \cdot (x-1) \in J_a$, protože z má nejvýše jeden nenulový koeficient (u x^0) ten musí být podle definice J_a nulový, dostáváme, že $p \in (x-1)\mathbf{Z}[x]$

(b) Rovněž tentokrát snadno najdeme polynom nejnižšího možného nezáporného stupně, který leží v množině $J_b = \{p \in \mathbf{Z}[x] |\ p(\frac{1}{2}) = 0\}$, konkrétně $2x-1 \in J_b$. Poznamenejme, že důkaz faktu, že je J_b ideál je zcela přímočarý. Vidíme tedy, že $(2x-1)\mathbf{Z}[x] \subseteq J_b$ a ukážeme obrácenou inkluzi. Zvolme proto $p \in \mathbf{J}_a$. Tentokrát ovšem nemůžeme vydělit se zbytkem přimo v okruhu $(\mathbf{Z}[x], +, -, 0, \cdot, 1)$, protože vedoucí koeficient polynomu $2x-1$ není v $\mathbf{Z}$ invertibilní, ovšem můžeme vydělit se zbytkem v okruhu $(\mathbf{Q}[x], +, -, 0, \cdot, 1)$. To znamená, že existují polynomy $q, z \in \mathbf{Q}[x]$ $q, z \in \mathbf{Z}[x]$, pro které $p = q \cdot (2x-1) + z$ a $\deg(z) < \deg(x-1) = 1$. Dosadíme-li $x = \frac{1}{2}$, vidíme, že $z = 0$, a proto $p = q \cdot (2x-1)$. Nyní uvážíme, že $q = \sum_i q_i x^i \in \mathbf{Z}[x]$, tj. že $q_i \in \mathbf{Z}$ pro všechna i. Dokažme to indukcí. Nejprve označme $p = \sum_i p_i x^i$ a všimněme si, že $q_0 = p_0$ a $p_i = q_i - 2q_{i-1}$ pro každé $i > 0$. To jednak znamená, že $q_0 \in \mathbf{Z}$ a předpokládáme-li, že $q_{i-1} \in \mathbf{Z}$, pak $q_i = p_i + 2q_{i-1} \in \mathbf{Z}$. Tím jsme ověřili, že $J_b = (2x-1)\mathbf{Z}[x]$ je hlavní ideál.

(c) Ptáme se, zda existuje polynom $p \in J_c = (x^2-1)\mathbf{Z}[x] + (x^2+3x+2)\mathbf{Z}[x]$, který generuje J_c, tedy, zda existují polynomy $a, b \in \mathbf{Z}[x]$, že $p = (x^2-1) \cdot a + (x^2+3x+2) \cdot b$ a $J_c = p\mathbf{Z}[x]$. Předpokládajme, že je tato podmínka splněna. Protože $p = (x+1)[(x-1) \cdot a + (x+2) \cdot b]$, vidíme, že $J_c = p\mathbf{Z}[x]$, právě když $[(x-1) \cdot a + (x+2) \cdot b]\mathbf{Z}[x] = (x-1)\mathbf{Z}[x] + (x+2)\mathbf{Z}[x]$. Dále můžeme argumentovat stejně jako v 1.6: $q = (x-1) \cdot a + (x+2) \cdot b$ musí být společným dělitelem polynomů $x-1$ a $x+2$, a 1 a -1 jsou jedinými společnými dělitely. Protože ovšem $q(1) = 3 \cdot b(1)$ je číslo dělitelné trojkou, $\mathbf{Z}[x] \neq (x-1)\mathbf{Z}[x] + (x+2)\mathbf{Z}[x]$, hledané q, a tudíž ani p neexistuje, proto ideál J_c není hlavní. □

18.3.

1.9. Rozhodněte, zda v okruhu $(\mathbf{Z}[x], +, -, 0, \cdot, 1)$ existují největší společní dělitelé libovolné dvojice nenulových polynomů.

Nejprve definujeme zobrazení $\phi : \mathbf{Z}[x] \setminus \{0\} \to \mathbf{N}$ podmínkou $\phi(\sum_i p_i x^i)$ je rovnou kladnému $\mathrm{NSD}(p_0, \dots, p_{\deg(p)})$. Dokážeme, že je ϕ homomorfismus monoidů $(\mathbf{Z}[x], \cdot, 1)$ a $(\mathbf{N}, \cdot, 1)$. Zvolme libovolně $p, q \in \mathbf{Z}[x] \setminus \{0\}$. Zřejmě $\phi(p) \cdot \phi(q) / \phi(p \cdot q)$, $\frac{p}{\phi(p)}, \frac{q}{\phi(q)} \in \mathbf{Z}[x]$ a $\phi(\frac{p}{\phi(p)}) = \phi(\frac{q}{\phi(q)}) = 1$, proto stačí dokázat, že $\phi(\frac{p}{\phi(p)} \cdot \frac{q}{\phi(q)}) = 1$. Bez újmy na obecnosti můžeme předpokládat, že $\phi(p) = \phi(q) = 1$. Dokazujme sporem. Mějme $p = \sum_i p_i x^i$ a $q = \sum_i q_i x^i$ a předpokládejme, že α je provočíslo, které dělí $\phi(p \cdot q)$. Označme n a m nejmenší hodnoty, pro něž α nedělí p_n a q_m. Nyní spočítáme koeficient monomu x^{n+m}, který α musí dělit

$$\sum_{i=0}^{n-1} p_i \cdot q_{n+m-i} + p_n \cdot q_m + \sum_{i=0}^{m-1} p_{n+m-i} \cdot q_i.$$

Protože α nedělí $p_n \cdot q_m$, ačkoli ostatní sčítance díky minimalitě volby n a m dělí, dostáváme spor.

Vezměme nyní libovolné polynomy $p, q \in \mathbf{Z}[x] \setminus \{0\}$ a najděme jejich největší společný dělitel u v okruhu $\mathbf{Q}[x]$. Můžeme přitom díky 1.7 předpokládat, že $u \in \mathbf{Z}[x] \setminus \{0\}$ a $\phi(u)$ je $\mathrm{NSD}(\phi(p), \phi(q))$. To znamená, že existují nesoudělná celá čísla α, β a polynom $a \in \mathbf{Z}[x]$, pro něž $\phi(a) = 1$ a $p = \frac{\alpha}{\beta} \cdot a \cdot u$, tedy $\beta \cdot p = \alpha \cdot a \cdot u$. Použijeme-li funkci ϕ, dostaneme

$$\beta \cdot \phi(p) = \phi(\beta \cdot p) = \phi(\alpha \cdot a \cdot u) = \phi(\alpha) \cdot \phi(a) \cdot \phi(u) = \alpha \cdot \phi(u).$$

Protože $\phi(u)/\phi(p)$, dostáváme, že β/α, a protože α a β jsou nesoudělná, musí být $\beta = 1$. Stejným argumentem zjistíme, že $\frac{q}{u} \in \mathbf{Z}[x]$, tedy u je společný dělitel p a q. Vezmeme-li společný dělitel w polynomů p a q v $\mathbf{Z}[x]$, pak víme, že w/u v $\mathbf{Q}[x]$, proto opět existují taková nesoudělná celá čísla α, β a polynom $\phi(b) = 1$ a $b \in \mathbf{Z}[x]$, že $\beta \cdot u = \alpha \cdot b \cdot w$, proto $\beta \cdot \phi(u) = \alpha \cdot \phi(w)$. Protože $\phi(w)/\phi(p)$ a $\phi(w)/\phi(q)$, tak $\phi(w)/\phi(u)$, a proto ze stejného důvodu jako výše je $\beta = 1$, a tudíž w/u v $\mathbf{Z}[x]$. □

25.3.

1.10. Uvažujme komutativní okruh $(R, +, -, 0, \cdot, 1)$ a označme $\mathbb{F}(R)$ množinu všech zobrazení R do R. Na $\mathbb{F}(R)$ definujme operace $+$, $-$, $\cdot$ předpisem $[f+g](r) = f(r)+g(r)$, $[-f](r) = -f(r)$ a $[f \cdot g](r) = f(r) \cdot g(r)$, konstatnty v $\mathbb{F}(R)$ označujeme příslušnými prvky R. Poznamenejme, že $\mathcal{F}(R) = (\mathbb{F}(R), +, -, 0, \cdot, 1)$ je komutativní okruh.

(a) Je-li $A \subseteq \mathbf{Z}$, označme $\chi_A \in \mathcal{F}(\mathbf{Z})$ charakteristickou funkci množiny A, tj. $\chi_A(z) = 1$, jestliže $z \in A$, $\chi_A(z) = 0$ pro $z \notin A$. Dokažte, že $\chi_A\mathbf{Z} + \chi_B\mathbf{Z} = \chi_{A\cup B}\mathbf{Z}$ pro každé $A, B \subseteq \mathbf{Z}$.
(b) Ukažte pro $R = \mathbf{Z}$, že okruh $\mathcal{F}(\mathbf{Z})$ není noetherovský.
(c) Najděte pro okruh $R = \mathbf{Z}$ celých čísel ideál $\mathcal{F}(\mathbf{Z})$, který není hlavní.
(d) Dokažte, že zobrazení $\nu : R \to \mathbb{F}(R)$ dané $\nu(r) = r$ je prostý okruhový homomorfismus.
(e) Dokažte, že zobrazení $\mu : R[x] \to \mathbb{F}(R)$ dané $\mu(\sum_i a_i x^i) = \sum_i a_i x^i$, kde x^i chápeme jako zobrazení $a \to a^i$ na okruhu R pro $a \in R$, je okruhový homomorfismus.
(f) Je-li $R = \mathbf{R}$, ověřte, že je zobrazení μ prosté.
(g) Je-li R konečný okruh, dokažte, že zobrazení μ není prosté.
(h) Je-li R těleso $\mathbf{Z}_7$, najděte nenulový polynom $p \in \mathbf{Z}_7[x]$, který leží v jádru $\mathrm{Ker}\mu$.
(i) Je-li $R = \mathbf{R}$ těleso reálných čísel, dokažte, že spojité funkce na $\mathbf{R}$ tvoří podokruh $\mathcal{F}(\mathbf{R})$.

(a) Nejprve si uvědomme, že $\chi_{A\cup B} \cdot \chi_A = \chi_A$ a $\chi_{A\cup B} \cdot \chi_B = \chi_B$, a proto $\chi_A\mathbf{Z} + \chi_B\mathbf{Z} \subseteq \chi_{A\cup B}\mathbf{Z}$. Naopak $\chi_{A\cup B} = \chi_A + \chi_B - \chi_A \cdot \chi_B$, čímž jsme ověřili i druhou inkluzi $\chi_{A\cup B}\mathbf{Z} \subseteq \chi_A\mathbf{Z} + \chi_B\mathbf{Z}$.

(b) Označme $\mathrm{supp}(f) = \{n \in \mathbf{Z} | \ f(n) \neq 0\}$ a $A_n = \{z \in \mathbf{Z} | \ |z| \leq n\}$. V části (a) jsme dokázali, že $\chi_{A_n}\mathbf{Z} \subseteq \chi_{A_{n+1}}\mathbf{Z}$, navíc $\chi_{A_{n+1}} \notin \chi_{A_n}\mathbf{Z}$, čímž jsme našli nekonečnou ostře rostoucí posloupnost ideálů $\chi_{A_1}\mathbf{Z} \subset \chi_{A_2}\mathbf{Z} \cdots \subset \chi_{A_n}\mathbf{Z} \subset \dots$ v okruhu $\mathcal{F}(\mathbf{Z})$, čímž jsme podle definice ověřili, že $\mathcal{F}(\mathbf{Z})$ není noetherovský okruh.

(c) Vezmeme-li množinu $I = \{f \in \mathcal{F}(\mathbf{Z}) | \ |\mathrm{supp}(f)| < \omega\}$, snadno ověříme, že $I = \bigcup_{n\in\mathbf{N}} \chi_{A_n}\mathbf{Z}$. Argument důkazu tvrzení, které říká, že okruh není noetherovksý, právě když obsahuje nekonečně generovaný ideál, ukazuje, že I je ideál, který nemůže být konečně generovaný. Zopakujme tento argument v naší konkrétní situaci. Vezmeme-li libovolnou konečnou podmnožinu $F \subset I$, pak existuje n, pro něž $F \subset \chi_{A_n}\mathbf{Z}$, a proto $\sum_{f\in F} f\mathbf{Z} \subseteq \chi_{A_n}\mathbf{Z} \neq I$. Tedy F negeneruje I. Prože ideál I není konečně generovaný, není ani hlavní (tj. jednogenerovaný).

(d) Okamžitě vidíme, že $\nu(a+b) = \nu(a) + \nu(b)$, $\nu(a \cdot b) = \nu(a) \cdot \nu(b)$ a $\nu(1) = 1$, což stačilo ověřit, navíc ν je zjevně prosté zobrazení.

(e) Opět potřebujme dokázat rovnosti $\mu(p+q) = \mu(p)+\mu(q)$, $\mu(p\cdot q) = \mu(p)\cdot\mu(q)$ pro každý poynom $p, q \in R[x]$ a $\mu(1) = 1$. Poslední rovnost je triviální, položme tedy $p = \sum_{n\geq 0} p_n x^n$ a $q = \sum_{n\geq 0} q_n x^n$. Potom

$$\mu(p+q) = \sum_{n\geq 0}(p_n + q_n)x^n = \sum_{n\geq 0} p_n x^n + \sum_{n\geq 0} q_n x^n = \mu(p) + \mu(q),$$

$$\mu(p\cdot q) = \sum_{n\geq 0}(\sum_{i+j=n} p_i \cdot q_j)x^n = \sum_{n\geq 0}(\sum_{i=0}^{n} p_i \cdot q_{n-i})x^n = \mu(p)\cdot\mu(q).$$

(f) Stačí ověřit, že $\mathrm{Ker}\mu = \{0\}$. Vezměme proto polynom $p \in \mathrm{Ker}\mu$, tj. $\mu(p) = 0$. Kdyby byl $\deg p \geq 0$, pak by existoval polynom $q \in R[x]$, pro který $p = q \cdot x \cdot (x - 1) \cdot \dots \cdot (x - \deg p)$, proto $q = 0$ a tedy i $p = 0$, což je spor.

(g) Protože je $R[x]$ nekonečné, zatímco množina $\mathbb{F}(R)$ je konečná, nemůže žádné prosté zobrazení $R[x]$ do $\mathbb{F}(R)$ existovat.

(h) Uvážíme-li, že $(\mathbf{Z}_7 \setminus \{0\}, \cdot, ^{-1}, 1)$ je grupa řádu 6, pak pro každé $a \in \mathbf{Z}_7 \setminus \{0\}$ je $a^6 = 1$, a proto $a^7 = a$ pro každé $a \in \mathbf{Z}_7$, vidíme, že $\mu(x^7 - x) = 0$.

(i) Stačí si uvědomit, že konstanty jsou spojité a součet, rozdíl i součin spojitých funkcí na $\mathbf{R}$ je spojitá funkce. $\square$

1.4.

1.11. Nechť $R = \{\sum_i p_i x^i \in \mathbf{Q}[x] |\ p_0 \in \mathbf{Z}\} \subseteq \mathbf{Q}[x]$.

(a) Dokažte, že je R podkruh okruhu $(\mathbf{Q}[x], +, -, 0, \cdot, 1)$,
(b) ověřte, že je R obor integrity,
(c) rozhodněte, zda R splňuje podmínku (K),
(d) rozhodněte, zda je R noetherovský,
(e) rozhodněte, zda R splňuje podmínku (E).

(a) Protože součet, rozdíl i součin polynomů s celočíselným absolutním členem má tutéž vlastnost a $0, 1 \in R$, je R podkruh okruhu $(\mathbf{Q}[x], +, -, 0, \cdot, 1)$.

(b) Plyne okamžitě z faktu, že $\mathbf{Q}[x]$ je obor integrity a R jeho podkruh.

(c) Uvědomme si, že $2^{-n}x \in R$, $2^{-n}xR \subseteq 2^{-(n+1)}xR$, protože $2^{-n}x = 2 \cdot 2^{-(n+1)}x$, a $2^{-n}xR \neq 2^{-(n+1)}xR$, protože $2^{-(n+1)}x \notin 2^{-n}xR$, čímž jsme našli nekonečnou posloupnost vlastních dělitelů $x/2^{-1}x/\dots/2^{-n}x/2^{-(n+1)}x\dots$, tedy R nesplňuje podmínku (K).

(d) V (c) jsme našli rostoucí posloupnost ideálů, tedy R není noetherovský. Všimněme si navíc, že ideál $I = \bigcup_{n\in\mathbf{N}} 2^{-n}xR$ není konečně generovaný.

(e) Kdyby existoval ireducibilní rozklad $x = p_1 \cdot \dots \cdot p_n$, pak by právě jeden z polynomů $p_i = \frac{1}{c}x$ a součin ostatních by byl roven c, kde $c \in \mathbf{Z}$. Ovšem polynom $\frac{1}{c}x$ umíme napsat jako součin $\frac{1}{c}x = 2 \cdot \frac{1}{2c}x$, kde $2, \frac{1}{2c}x \in R$ nejsou invertibilní, tedy $\frac{1}{c}x$ není inreducibilní a podmínka (E) splněna není. $\square$

1.12. Uvažujme eukleidovský okruh $(\mathbf{Z}[i], +, -, 0, \cdot, 1)$, kde $\mathbf{Z}[i] = \{a+bi \in \mathbf{C} |\ a, b \in \mathbf{Z}\}$ je podokruh tělesa komplexních čísel a označme $\nu(a+bi) = a^2 + b^2$ jeho eukleidovskou normu.

(a) Najděte všechny invertibilní prvky okruhu $\mathbf{Z}[i]$,
(b) spočítejte v $\mathbf{Z}[i]$ ireducibilní rozklad prvků 2, 3, 13,
(c) spočítejte v $\mathbf{Z}[i]$ ireducibilní rozklad prvků $2-2i$, $3-i$, $17-6i$,
(d) najděte největší společný dělitel dvojic prvků $3-i$ a $17-6i$, $6-7i$ a $7+i$, $11-2i$ a $5+10i$,
(e) najděte $\alpha, \beta, \gamma, \delta \in \mathbf{Z}[i]$, aby $\alpha \cdot (6-7i) + \beta \cdot (7+i)$ byl největší společný dělitel dvojice $6-7i$ a $7+i$ a $\beta \cdot (11-2i) + \gamma \cdot (5+10i)$ byl největší společný dělitel dvojice, $11-2i$ a $5+10i$,
(f) rozhodněte, zda jsou prvky 2, 3, $2-3i$, $1-3i$ prvočinitelé,
(g) rozhodněte, které dvojice prvků množiny $\{2\epsilon + 3\delta |\ \epsilon, \delta \in \{\pm 1, \pm i\}\}$ jsou asociovány,

Nejprve připomeňme $|c_1 \cdot c_2| = |c_1| \cdot |c_2|$, pro každdou dvojici komplexních čísel c_1 a c_2, proto $\nu(\alpha \cdot \beta) = |\alpha \cdot \beta|^2 = |\alpha|^2 \cdot |\beta|^2 = \nu(\alpha) \cdot \nu(\beta)$ pro všechna $\alpha, \beta \in \mathbf{Z}[i]$.

(a) Protože prvek $\alpha \in \mathbf{Z}[i]$ je invertibilní existuje-li $\beta \in \mathbf{Z}[i]$, pro nkteré $\alpha \cdot \beta = 1$, proto $\nu(\alpha \cdot \beta) = 1$, tedy $\nu(\alpha) = 1$. Vidíme, že $\alpha \in \{1, -1, i, -i\}$.

(b) Protože $\nu(2) = 4$ musí mít netriviální a neinvertibilní dělitel prvku 2 normu rovnou 2, snadno přitom nahlédneme, že $2 = (1+i)(1-i)$. Protože $\nu(1+i) = \nu(1-i) = 2$ je prvočíslo, oba tyto prvky už jsou nutně ireducibilní, tedy $2 = (1+i)(1-i)$ už je ireducibilní rozklad.

Stejným argumentem pro $\nu(3) = 9$ jako při hledání rozkladu prvku 2 dostáváme, že případný netriviální a neinvertibilní dělitel prvku 3 by musel mít normu rovnou 3. Projdeme-li všechny takové kandidáty, tj. Gaussova celá čísla velikostei(nejvýše) rovné $\sqrt{3}$, žádný takový prvek nenajdeme, proto je 3 ireducibilní.

Konečně, protože $13 = 2^2 + 3^2$, spočítáme $13 = (2+3i)(2-3i)$, kde ze stejného důvodu jako výše jsou prvky $2+3i$ a $2-3i$ v $\mathbf{Z}[i]$ ireducibilní. (Lze dokázat, že prvočíslo p je tvaru $p = a^2 + b^2$ pro přirozená a, b, tedy $p = (a+bi)(a-bi)$, právě když $(p)\mathrm{mod}4 = 1$.)

8.4.

(c) Vidíme, že $2 - 2i = 2 \cdot (1-i) = (1+i) \cdot (1-i) \cdot (1-i) = -i \cdot (1-i)^3$, kde $\nu(1-i) = 2$, tedy prvky $1-i$ jsou ireducibilní.

Spočítáme nejprve $\nu(3-i) = 10$, proto jako prvky ireducibilního rozkladu připadají v úvahu nutně právě prvky s eukleidovskou normou 2 a 5. Vydělíme proto v komplexním oboru $\frac{3-i}{1+i} = \frac{(3-i)(1-i)}{(1+i)(1-i)} = 1 - 2i$, tedy $3 - i = (1+i)(1-2i)$, kde oba členy rozkaldu už mají prvočíselnou eukleidovskou normu, proto musí jít o ireducibilní prvky.

Opět spočítáme $\nu(17-6i) = 289 + 36 = 325 = 13 \cdot 5^2$. Jako ireducibilní činitelé tedy připadají v úvahu prvku s normou, která dělí číslo 325. Uvážíme nejprve prvky s normou 5, tj. $2+i$, $2-i$. Oběma prvky zkusíme vydělit v $\mathbf{C}$:

$$\frac{17-6i}{2+i} = \frac{(17-6i)(2-i)}{5} = \frac{28-29i}{5} \notin \mathbf{Z}[i],$$
$$\frac{17-6i}{2-i} = \frac{(17-6i)(2+i)}{5} = \frac{40+5i}{5} = 8 + i \in \mathbf{Z}[i].$$

Pokračujeme stejnou úvahou dál pro prvek $8+i$, kdy $\nu(8+i) = 13\cdot 5$, je už zbytečné dělit prvkem $2+i$, pokusíme se tedy vydělit prvkem $2-i$: $\frac{8+i}{2-i} = \frac{(8+i)(2+i)}{5} = \frac{15+10i}{5} = 3+2i \in \mathbf{Z}[i]$. Protože eukleidovská norma prvků $2-i$ a $3+2i$ je prvočíselná, dostáváme ireducibilní rozklad $17-6i = (2-i)^2(3+2i)$.

(d) Pro prvky $3-i$ a $17-6i$ využijeme znalost rozkladů na ireducibilní prvky spolu s podmínkou (J), která v našem oboru platí, abychom zjistili, že jsou prvky nesoudělné, protože prvek $1-2i$ není asociován s prvkem $2-i$.

Pro dvojici $a_0 = 6-7i$ a $a_1 = 7+i$ použijem Eukleidův algoritmus. Nejprve spočítáme $\frac{6-7i}{7+i} = \frac{(6-7i)(7-i)}{(7+i)(7-i)} = \frac{35}{50} - \frac{55}{50}i$, tedy

$$q_1 = 1-i \quad \text{a} \quad a_2 = a_0 - q_1 \cdot a_1 = 6-7i-(1-i)(7+i) = -2-i.$$

V dalším kroku počítáme $\frac{7+i}{-2-i} = \frac{(7+i)(-2+i)}{(-2-i)(-2+i)} = -\frac{15}{5} + \frac{5}{5}i = -3+i \in \mathbf{Z}[i]$, tedy vidíme, že $q_2 = -3+i$ a že a_2/a_1. Zjistili jsme, že $-2-i$ je největší společný dělitel prvků $6-7i$ a $7+i$. Nakonec si všimněme, že $\nu(6-7i) = 85$ a $\nu(7+i) = 50$, tedy jiné společné dělitele než ty s normou 1 a 5 nepřipadaly v úvahu.

I pro prvky $a_0 = 11-2i$ a $a_1 = 5+10i$ použijeme Eukleidův algoritmus. Poznamenejme, že $\nu(11-2i) = \nu(5+10i) = 125$. Protože $\frac{11-2i}{5+10i} = \frac{11-2i}{5+10i} \cdot \frac{5-10i}{5-10i} = \frac{35}{125} - \frac{120}{125}i$ položíme

$$q_1 = -i \quad \text{a} \quad a_2 = a_0 - q_1 \cdot a_1 = 11-2i+i(5+10i) = 1+3i.$$

Dále $\frac{5+10i}{1+3i} = \frac{5+10i}{1+3i} \cdot \frac{1-3i}{1-3i} = \frac{35}{10} - \frac{5}{10}i$, a proto

$$q_2 = 3 \quad \text{a} \quad a_3 = a_2 - q_2 \cdot a_1 = 5+10i-3(1+3i) = 2+i.$$

Nyní už snadno ověříme, že $2+i/1+3i$, tedy $2+i$ je největší společný dělitel prvků $11-2i$ a $5+10i$.

(e) Přímo z 1. kroku Eukleidova algoritmu dostáváme vyjádření

$$-2-i = (6-7i) + (-1+i)(7+i),$$

tedy $\alpha = 1$, $\beta = -1+i$.

V (d) jsme zjistili, že $2+i = 5+10i-3(1+3i) = 2+i$ a $1+3i = 11-2i+i(5+10i)$, proto dosazením spočítáme, že

$$2+i = 5+10i-3(1+3i) = 5+10i-3(11-2i+i(5+10i)) = -3(11-2i)+(1-3i)(5+10i),$$

tedy $\gamma = -3$, $\delta = 1-3i$.

(f) V eukleidovském oboru jsou ireducibilní prvky prvočinitelé, proto zjistíme stejně jako v (b) a (c), zda jde ireducibilní prvky. Prvek 2 tedy není prvočinitelem a 3 a $2-3i$ jsou prvočinitelé, konečně $1-3i = (2-i)(1-i)$ není ireducibilní, tedy ani prvočinitel.

(g) Protože dva prvky jsou asociované, právě když se liší o násobek invertibilním prvkem, jsou všechny prvky $3+2i$, $-3-2i$, $i\cdot(3+2i) = -2+3i$ a $-i\cdot(3+2i) = 2-3i$ vzájemně asociované, stejně jako jsou asociované všechny dvojice prvků ze souboru $3-2i$, $-3+2i$, $i\cdot(3-2i) = 2+3i$ a $-i\cdot(3-2i) = -2-3i$. Naopak prvky $3+2i$ a $3-2i$ asociovány nejsou. Kdyby $3+2i$ dělilo $3-2i$, pak by prvek $3+2i$ dělil i $3+2i-(3-2i) = 4i$, což není možné, protože $\nu(3+2i) = 13$ nedělí $\nu(4i) = 16$. □

1.13. Uvažujme okruh $(\mathbf{Z}[\sqrt{2}], +, -, 0, \cdot, 1)$, kde $\mathbf{Z}[\sqrt{2}] = \{a + b\sqrt{2} \in \mathbf{R} | \ a, b \in \mathbf{Z}\}$ je podokruh tělesa reálných čísel a označme $\mu(a + b\sqrt{2}) = |a^2 - 2b^2|$.

(a) Dokažte, že je μ eukleidovská norma,
(b) ukažte, že okruh $\mathbf{Z}[\sqrt{2}]$ obsahuje nekonečně invertibilních prvků,
(c) rozhodněte, zda jsou prvky $11 + 8\sqrt{2}$ a $3 - \sqrt{2}$ asociovány,
(d) spočítejte ireducibilní rozklad prvků 2, $3 + \sqrt{2}$ a $-2 + 5\sqrt{2}$.

(a) Postupujeme podobně jako u okruhu Gaussových celých čísel $\mathbf{Z}[i]$. Nejprve označme $\mathbf{Q}[\sqrt{2}] = \{a + b\sqrt{2} \in \mathbf{R} | \ a, b \in \mathbf{Q}\}$ q všimněme si, že rozšíříme-li funkci μ na $\mathbf{Q}[\sqrt{2}] \to \mathbf{Q}$ stejným předpisem, tedy $\mu(a + b\sqrt{2}) = |a^2 - 2b^2|$ pro každé $a, b \in \mathbf{Q}$, pak platí, že $\mu(\alpha \cdot \beta) = \mu(\alpha) \cdot \mu(\beta)$. Označíme-li $\widetilde{a + b\sqrt{2}} = a - b\sqrt{2}$, stačí si všimnout, že $\widetilde{\alpha \cdot \beta} = \widetilde{\alpha} \cdot \widetilde{\beta}$ a že $\mu(\alpha) = |\widetilde{\alpha} \cdot \alpha|$, tedy

$$\mu(\alpha \cdot \beta) = |\widetilde{\alpha \cdot \beta} \cdot \alpha \cdot \beta| = |\widetilde{\alpha} \cdot \widetilde{\beta} \cdot \alpha \cdot \beta| = |\widetilde{\alpha} \cdot \alpha| \cdot |\widetilde{\beta} \cdot \beta| = \mu(\alpha) \cdot \mu(\beta).$$

Odtud přímo dostáváme, že $\mu(\alpha) \leq \mu(\beta)$, jakmile α/β a $\beta \neq 0$.

Zvolme nyní $\alpha, \beta \in \mathbf{Z}[\sqrt{2}]$, kde $\beta \neq 0$. Pak existují $e, f \in \mathbf{Q}$, pro která $e + f\sqrt{2} = \frac{\alpha}{\beta}$. Vezměme nyní $e', f' \in \mathbf{Z}$, aby $|e - e'| \leq \frac{1}{2}$ a $|f - f'| \leq \frac{1}{2}$, položme $\gamma = e' + f'\sqrt{2}$ a $\delta = \alpha - \beta \cdot \gamma$. Zbývá nám ověřit, že $\mu(\delta) < \mu(\beta)$, což je ekvivalentní tomu, že $\mu(\frac{\delta}{\beta}) = \frac{\mu(\delta)}{\mu(\beta)} < 1$. Přitom

$$\mu(\frac{\delta}{\beta}) = \mu(\frac{\alpha}{\beta} - \gamma) = \mu(e - e' + (f - f')\sqrt{2}) = |(e - e')^2 - 2(f - f')^2| \leq \frac{1}{2} < 1.$$

Tím jsme ověřili i druhý axiom eukleidovské normy, proto $(\mathbf{Z}[\sqrt{2}], +, -, 0, \cdot, 1)$ je eukleidovský obor.

(b) Všimneme si, že invertibilní je právě prvek $a + b\sqrt{2} \in \mathbf{Z}[\sqrt{2}]$, pro který $\mu(a + b\sqrt{2}) = 1$. Jakmile $a^2 - 2b^2 = -1$, potom $(a + b\sqrt{2}) \cdot (-a + b\sqrt{2}) = 2b^2 - a^2 = 1$, a v případě, kdy $a^2 - 2b^2 = 1$, pak $(a + b\sqrt{2}) \cdot (a - b\sqrt{2}) = a^2 - 2b^2 = 1$. Protože $\mu(1 + \sqrt{2}) = 1$, je i $\mu((1 + \sqrt{2})^n) = 1^n = 1$ pro každé n, tedy prvky $(1 + \sqrt{2})^n$ jsou invertibilní. Přitm $1 + \sqrt{2} > 1$, proto $(1 + \sqrt{2})^n < (1 + \sqrt{2})^{n+1}$, tedy jsme našli nekonečnou množinu $\{(1 + \sqrt{2})^n | \ n \in \mathbf{N}\}$ invertibilních prvků oboru $(\mathbf{Z}[\sqrt{2}], +, -, 0, \cdot, 1)$.

(c) Stačí abychom v $\mathbf{R}$ spočítali podíly

$$\frac{11 + 8\sqrt{2}}{3 - \sqrt{2}} = \frac{(11 + 8\sqrt{2})(3 + \sqrt{2})}{7} = \frac{49 + 35\sqrt{2}}{7} = 7 + 5\sqrt{2},$$

$$\frac{3 - \sqrt{2}}{11 + 8\sqrt{2}} = \frac{(3 - \sqrt{2})(11 - 8\sqrt{2})}{-7} = -\frac{49 - 35\sqrt{2}}{7} = -7 + 5\sqrt{2},$$

tedy prvky se vzějemně dělí, tedy jsou asociované. Dodejme, že stačilo určit jen například první podíl a u něj ověřit, že $\mu(7 + 5\sqrt{2}) = 1$.

(d) Uvažujeme podobně jako v 1.12(b), (c). Nejprve spočítáme normy $\mu(2) = 4$, $\mu(3 + \sqrt{2}) = 7$, $\mu(-2 + 5\sqrt{2}) = 46$. Vidíme, že $3 + \sqrt{2}$ už je nutně ireducibilní, protože norma μ je kompatabilní s násobením a 7 je prvočíslo. Jsou-li zbylé hodnoty 2, $-2 + 5\sqrt{2}$ rozložitelné, musí je obě dělit prvek s normou 2. Přímočaře spočítáme, že takovým prvkem je $\sqrt{2}$ a že skutečně oba orvky dělí, konkrétně $2 = \sqrt{2} \cdot \sqrt{2}$, $-2 + 5\sqrt{2} = \sqrt{2} \cdot (5 - 1\sqrt{2})$, protože jsou hodnoty $\mu(\sqrt{2})$ a $\mu(5 - 1\sqrt{2})$ prvočíselné, našli jsme opravdu ireducibilní rozklady. $\square$

2. Symetrické polynomy

2.1. Uvažujme polynomy $p, q, r \in \mathbf{Q}[x_1, x_2, x_3]$, kde $p = 3x_1x_2x_3 - x_1x_2^3 - x_1x_3^3 - x_2x_1^3 - x_2x_3^3 - x_3x_1^3 - x_3x_2^3 + 2x_1x_2^2x_3^2 + 2x_2x_1^2x_3^2 + 2x_3x_2^2x_1^2$, $q = x_1x_2^2x_3^3$ a $r = 5(x_1 + x_2 + x_3) + 3$.

(a) Rozhodněte, které z polynomů p, q, r, $p + q$, $p \cdot r$ jsou symetrické,
(b) spočítejte stupeň polynomů p, q, r, $p \cdot r$,
(c) určete výšku a vedoucí koeficient polynomů p, q, r, $p \cdot r$.

(a) Postupujeme nejprve podle definice. Přímočaře zjistíme, že $\pi(p) = p$ a $\pi(r) = r$ pro všechny permutace proměnných π, zatímco $\pi(q) = x_2x_1^2x_3^3 \neq q$ například pro permutaci $\pi = (12)$. Protože množina všech synmetrických polynomů tvoří podokruh okruhu $\mathbf{Q}[x_1, x_2, x_3]$, musí být $p \cdot r$ symetrický a $p + q$ naopak symetrický být nemůže.

(b) Opět počítáme podle definice, tedy zjišťujeme nejvyšší součet mocnin v jednotlivých monočlenech, tedy $\deg(p) = 5$, $\deg(q) = 6$, $\deg(r) = 1$ a $\deg(p \cdot r) = 6$.

(c) Tentokrát podle definice hledáme v lexikografickém uspořádání největší trojici (k_1, k_2, k_3), pro kterou je koeficient u monočlenu $x_1^{k_1}x_2^{k_2}x_3^{k_3}$ nenulový, a dále hledáme hodnotu příslušného koeficientu. Tedy $\mathrm{ht}(p) = (3, 1, 0)$ a $\mathrm{lc}(p) = -1$, $\mathrm{ht}(q) = (3, 2, 1)$ a $\mathrm{lc}(q) = 1$, $\mathrm{ht}(r) = (1, 0, 0)$ a $\mathrm{lc}(r) = 5$, $\mathrm{ht}(p \cdot r) = (4, 1, 0)$ a $\mathrm{lc}(p \cdot r) = -5$. $\square$

Připomeňme, že $\delta_{13} = x_1 + x_2 + x_3$, $\delta_{23} = x_1x_2 + x_1x_3 + x_2x_3$ a $\delta_{33} = x_1x_2x_3$.

2.2. Najděte pro symetrický polynom $p \in S_{\mathbf{Q}}[x_1, x_2, x_3]$ polynom $f \in \mathbf{Q}[x_1, x_2, x_3]$, aby $p = f(\delta_{13}, \delta_{23}, \delta_{33})$, jestliže

(a) $p = x_1^3x_2x_3 + x_1x_2^3x_3 + x_1x_2x_3^3$,
(b) $p = 3x_1^4x_2^2x_3^2 + 2x_1^2x_2^4x_3^2 + x_1^2x_2^2x_3^4$,
(c) $p = 2x_1^3 + 2x_2^3 + 2x_3^3 - 1$.

(a) Využijme důkazu Věty o symetrických polynomech. Položíme $p_0 = p$ a budeme postupně indukčním krokem snižovat výšku polynomu p_i.

Protože $\mathrm{ht}(p_0) = (3, 1, 1) = (k_1, k_2, k_3)$ a $\mathrm{lc}(p_0) = 1$, definujeme polynom $f_0 = \mathrm{lc}(p_0) \cdot x_1^{k_1-k_2}x_2^{k_2-k_3}x_3^{k_3} = x_1^2x_3$. Potom má polynom $p_1 = p_0 - f_0(\delta_{13}, \delta_{23}, \delta_{33}) = x_1^3x_2x_3 + x_1x_2^3x_3 + x_1x_2x_3^3 - (x_1 + x_2 + x_3)^2x_1x_2x_3 = -2(x_1x_2 + x_1x_3 + x_2x_3)$ nižší výšku než symetrický polynom p_0. Konkrétně $\mathrm{ht}(p_1) = (1, 1, 0)$ a $\mathrm{lc}(p_1) = -2$, tedy $f_1 = -2 \cdot x_2$ a $p_1 - f_1(\delta_{13}, \delta_{23}, \delta_{33}) = 0$.

Zjistili jsme, že hledaným polynomem f je polynom $f = f_0 + f_1 = x_1^2x_3 - 2x_2$.

(b) Všimneme-li si, že

$$p = 3x_1x_2x_3 \cdot (x_1^3x_2x_3 + x_1x_2^3x_3 + x_1x_2x_3^3) = 3\delta_{33} \cdot g(\delta_{13}, \delta_{23}, \delta_{33}),$$

kde $g = x_1^2x_3 - 2x_2$ jsme spočítali v bodu (a), pak $f = 3x_3 \cdot g = 3x_1^2x_3^2 - 6x_2x_3$.

(c) Postupujeme stejně jako v bodu (a). Nejprve položíme $p_0 = p$, spočítáme $\mathrm{ht}(p_0) = (3, 0, 0)$ a $\mathrm{lc}(p_0) = 2$ a definujeme polynom $f_0 = 2x_1^3$.

V dalším kroku spočítáme symetrický polynom $p_1 = p_0 - f_0(\delta_{13}, \delta_{23}, \delta_{33}) = p_0 - 2(x_1 + x_2 + x_3)^3 = -6(x_1x_2^2 + x_1x_3^2 + x_2x_1^2 + x_2x_3^2 + x_3x_1^2 + x_3x_2^2 + x_1x_2x_3) - 1$. Opět určíme $\mathrm{ht}(p_1) = (2, 1, 0)$ a $\mathrm{lc}(p_1) = -6$, tedy $f_1 = -6x_1x_2$.

Nyní dostáváme $p_2 = p_1 - f_1(\delta_{13}, \delta_{23}, \delta_{33}) = p_1 + 6(x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3) = 18(x_1x_2x_3) - 1$, proto $\mathrm{ht}(p_2) = (1, 1, 1)$, $\mathrm{lc}(p_2) = 18$ a $f_2 = 18x_3$.

Konečně $p_3 = p_2 - f_1(\delta_{13}, \delta_{23}, \delta_{33}) = p_2 - 18(x_1x_2x_3) = -1$, tudíž $\mathrm{ht}(p_3) = (0,0,0)$, $\mathrm{lc}(p_3) = -1$ a $f_3 = -1$

Zjistili jsme, že $f = \sum_i f_i = 2x_1^3 - 6x_1x_2 + 18x_3 - 1$. $\square$

22.4.

3. Kořeny polynomů

3.1. Uvažujme polynom $p = x^5 + x^4 + x^3 + x + 2 \in \mathbf{Z}_5[x]$.

(a) Najděte nad tělesem $\mathbf{Z}_5$ všechny kořeny polynomu p,
(b) určete násobnost všech kořenů polynomu p nad $\mathbf{Z}_5$,
(c) spočítejte ireducibilní rozklad p v $\mathbf{Z}_5[x]$.

(a) V souladu s definicí nám stačí postupně dosazovat do p jednotlivé prvky $\mathbf{Z}_5$:
$\mathrm{id}_0(p) = 2 \neq 0$, $\mathrm{id}_1(p) = 1^5 + 1^4 + 1^3 + 1 + 2 = 1 \neq 0$,
$\mathrm{id}_2(p) = 2^5 + 2^4 + 2^3 + 2 + 2 = 2 + 1 + 3 + 2 + 2 = 0$,
$\mathrm{id}_3(p) = 3^5 + 3^4 + 3^3 + 3 + 2 = 3 + 1 + 2 + 3 + 2 = 1 \neq 0$,
$\mathrm{id}_4(p) = 4^5 + 4^4 + 4^3 + 4 + 2 = 4 + 1 + 4 + 4 + 2 = 0$,
Zjistili jsme, že kořeny jsou právě čísla 2 a 4.

(b) Protože je charakteristika tělesa rovna stupni polynomu, nemůžeme přímočaře použít větu, která určí násobnost kořenu pomocí derivace. Proto nejprve vydělíme se zbytkem polynom p kořenovým činitelem $x - 4 = x + 1$:

$$\begin{array}{rcccl}
x^5 + x^4 + x^3 + x + 2 & : & x+1 & = & x^4 + x^2 + 4x + 2 \\
-(x^5 + x^4) \\
= x^3 + x + 2 \\
-(x^3 + x^2) \\
= 4x^2 + x + 2 \\
-(4x^2 + 4x) \\
= 2x + 2 \\
-(2x + 2) \\
= 0
\end{array}$$

Spočítali jsme, že $p = (x+1)(x^4 + x^2 + 4x + 2)$. Označme si $q = x^4 + x^2 + 4x + 2$ a poznamenejme, že q má kořen 2 stejné násobnosti jako je násobnost kořenu 2 v p, a je-li k násobnost kořenu 4 v p, pak bude 4 kořen násobnosti $k - 1$ v q. Žádné jiné kořeny přitom q mít v $\mathbf{Z}_5$ nemůže.

Nejprve zjistíme, že $\mathrm{id}_4(q) = 1 + 1 + 1 + 20$, tedy 4 je kořenem q. Nyní spočítáme formální derivaci q, tedy $D(q) = 4x^3 + 2x + 4$. Protože $\mathrm{id}_4(D(q)) = 3 \neq 0$, má kořen 4 v q násobnost 1 a v p násobnost 2. Dále $\mathrm{id}_2(D(q)) = 2 + 4 + 4 = 0$. Spočítáme-li druhou derivaci $D^2(q) = 2x^2 + 2$, vidíme, že $\mathrm{id}_2(D^2(q)) = 3 + 2 = 0$ a protože $D^3(q) = 4x$, je $\mathrm{id}_2(D^3(q)) = 3 \neq 0$, ukázali jsme, že kořen 2 má v q i p násobnost 3.

(c) Protože jsme zjistili, že $(x-4)^2/p$ a $(x-2)^3/p$, dostáváme dokonce rozklad na kořenové činitele $p = \mathrm{lc}(p)(x-4)^2(x-2)^3 = (x+1)^2(x+3)^3$. $\square$

3.2. Mějme dvacetipětiprvkové nadtěleso U tělesa Z_5 a uvažujme polynom $p = x^5 + x^4 + x^3 + x + 2 \in \mathbf{U}[x]$.

(a) Najděte nad tělesem U všechny kořeny polynomu p,

(b) určete nad U násobnost všech kořenů polynomu p,
(c) spočítejte ireducibilní rozklad p v $\mathbf{U}[x]$.

Protože jsme v 3.1 zjistili, že se polynom p rozkládá na kořenové činitele už nad tělesem $\mathbf{Z}_5$, máme i nad větším tělesem rozklad $p = (x-4)^2(x-2)^3$. Přitom jsou kořenové činitele, tedy polynomy stupně 1, ireducibilní nad jakýmkoli tělesem, tedy $p = (x-4)^2(x-2)^3$ je ireducibilní rozklad i v oboru $\mathbf{U}[x]$.

Odtud okamžitě vidíme, že p má v U právě kořeny $2, 4 \in \mathbf{Z}_5 \subseteq U$, první násobnosti 3 a druhý 2. $\square$

3.3. Buď U těleso, T jeho podtěleso a $p, q \in T[x]$, $p \neq 0$. Předpokládejme, že existuje $r \in U[x]$, pro které $p = q \cdot r$ (tedy q/p v oboru $U[x]$). Dokažte, že $r \in T[x]$ (tedy q/p v oboru $T[x]$).

Stačí vydělit se zbytkem polynom p polynomem q v oboru $T[x]$. Potom existují $a, b \in T[x]$, pro která $p = aq + b$ a $\deg(b) < \deg(q)$. Uvědomíme-li si, že hodnoty pro dělení se zbytkem musí být stejné i při dělení v oboru $U[x]$ a že jsou jednoznačně určeny, dostáváme $a = r$ a $b = 0$, proto $r \in T[x]$. $\square$

3.4. Dokažte, že polynom $x^2 + 2$ dělí polynom $x^5 + x^2 - 4x + 2$ v oboru $\mathbf{Q}[x]$.

Využijeme-li pozorování 3.3 a zjistíme-li, že kořeny $x^2 + 2$ nad tělesem $\mathbf{C}$ jsou $\pm\sqrt{2}i$, stačí ověřit, že $\pm\sqrt{2}i$ jsou kořeny polynomu x^5+x^2-4x+2, tedy, že x^2+2 dělí polynom x^5+x^2-4x+2 v oboru $\mathbf{C}[x]$. Tedy počítáme: $(\sqrt{2}i)^5+(\sqrt{2}i)^2-4(\sqrt{2}i)+2 = 4\sqrt{2}i-2-4\sqrt{2}i+2 = 0$ a $(-\sqrt{2}i)^5+(-\sqrt{2}i)^2-4(-\sqrt{2}i)+2 = -4\sqrt{2}i-2+4\sqrt{2}i+2 = 0$. $\square$

29.4.

3.5. Uvažujme tělesa reálných čísel $\mathbf{R}$ a jeho podtěleso racionálních čísel $\mathbf{Q}$.
(a) Dokažte , že je prvek $\sqrt{3}$ algebraický nad $\mathbf{Q}$,
(b) spočítejte stupeň rozšíření $[\mathbf{Q}(\sqrt{3}) : \mathbf{Q}]$,
(c) najděte nad $\mathbf{Q}$ minimální polynom prvku $\sqrt{3}$,
(d) ověřte, že je prvek $2 + 5\sqrt{3}$ algebraický nad $\mathbf{Q}$ a najděte jeho minimální polynom nad $\mathbf{Q}$,
(e) ověřte, že $\frac{2-\sqrt{3}}{3+\sqrt{3}}$ je algebraický prvek nad $\mathbf{Q}$ a najděte jeho minimální polynom nad $\mathbf{Q}$,
(f) dokažte , že je prvek $\sqrt[3]{2}$ algebraický nad $\mathbf{Q}$,
(g) najděte nad $\mathbf{Q}$ minimální polynom prvku $\sqrt[3]{2}$ a spočítejte stupeň rozšíření $[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}]$,
(h) ověřte, že $[\mathbf{Q}(\sqrt[3]{2}, \sqrt[5]{5}) : \mathbf{Q}] \leq 15$,
(i) najděte nějakou generující množinu vektorového prostoru $\mathbf{Q}(\sqrt[3]{2}, \sqrt[5]{5})$ nad tělesem $\mathbf{Q}$.

(a) Prvek α je podle definice algebraický nad $\mathbf{Q}$, právě když existuje polynom $p \in \mathbf{Q}[x]$, jehož je α kořenem. V našem případě okamžitě vidíme, že $\sqrt{3}^2 = 3$, a proto je $\sqrt{3}$ kořenem polynom $x^2 - 3 \in \mathbf{Q}[x]$.

(b) Nahlédneme, že je těleso $\mathbf{Q}(\sqrt{3})$, tedy nejmenší podtěleso tělesa $\mathbf{R}$ obsahující množinu $\mathbf{Q} \cup \{\alpha\}$, rovno množině $A = \{a + b\sqrt{3} \in \mathbf{R} |\ a, b \in \mathbf{Q}\}$. Protože pro každé $a, b \in \mathbf{Q}$, máme z uzavřenosti na operace $a, b, b\sqrt{3}, a + b\sqrt{3} \in ,Q(\sqrt{3})$, proto $A \subseteq Q(\sqrt{3})$. Přitom je A zjevně množina uzavřená na sčítání, odčítání a násobení a $0, 1 \in A$, tedy je A podokruh okruhu $\mathbf{R}$. Vezmeme-li nenulové $a + b\sqrt{3} \in A$, potom $(a + b\sqrt{3})^{-1} = \frac{(a-b\sqrt{3})}{(a+b\sqrt{3})(a-b\sqrt{3})} = \frac{a}{a^2-3b^2} - \frac{b}{a^2-3b^2}\sqrt{3} \in A$, protože $\frac{a}{a^2-3b^2} \in \mathbf{Q}$ a $-\frac{b}{a^2-3b^2} \in \mathbf{Q}$. To znamená, že je A podtěleso tělesa $\mathbf{Q}(\sqrt{3})$ obsahující $\mathbf{Q} \cup \{\alpha\}$, proto $A = \mathbf{Q}(\sqrt{3})$.

Tím jsme ukázali, že $\mathbf{Q}(\sqrt{3})$ je jako racionálná vektorový prostor generováno prvky 1 a $\sqrt{3}$. Ověříme, že jde o lineárně nezávislou množinu. Předpokládejme, že je $\sqrt{3}$ racionální, tj. existují nesoudělná přirozená c a j, pro která $\sqrt{3} = \frac{c}{j}$, a proto $c^2 = 3j^2$. Potom $3/c$, tedy $9/c^2$, a proto $3/j$, spor s nesoudělností c a j. Protože je prvek $\sqrt{3}$ iracionální, není racionálním násobkem prvku 1, tudíž je lineárně nezávislý na 1. Našli jsme dvouprvkovou bázi $\mathbf{Q}(\sqrt{3})$ chápaného jako vektorový prostor nad tělesem $\mathbf{Q}(\sqrt{3})$, tedy $[\mathbf{Q}(\sqrt{3}) : \mathbf{Q}] = \dim_{\mathbf{Q}} \mathbf{Q}(\sqrt{3}) = 2$.

(c) Připomeňme, že minimální polynom $m \in \mathbf{Q}[x]$ prvku α je ireducibilní monický polynom, jehož kořenem je α, ekvivalentně je m monický polynom nejmenšího možného stupně, jehož kořenem je α. Navíc bylo na přednášce dokázáno, že $\deg(\sqrt{3}) = [\mathbf{Q}(\sqrt{3}) : \mathbf{Q}]$. Využijeme-li pozorování $[\mathbf{Q}(\sqrt{3}) : \mathbf{Q}] = 2$ a všimneme-li, že jsme v (a) už polynom stupně 2 s kořenem $\sqrt{3}$ našli, tedy nutně musí jít o minimální polynom. Tedy $x^2 - 3$ je minimální polynom prvku $\sqrt{3}$ nad $\mathbf{Q}$.

(d,e) Na přednášce bylo dokázáno, že každé rozšíření konečného stupně je algebraické, tedy díky (b) je každý prvek $\mathbf{Q}(\sqrt{3})$ algebraický nad $\mathbf{Q}$. Protože $2 + 5\sqrt{3}, \frac{2-\sqrt{3}}{3+\sqrt{3}} \in \mathbf{Q}(\sqrt{3})$, jde o prvky algebraické nad $\mathbf{Q}$.

Dále víme, že každé tři prvky vektorového prostoru dimenze 2 musí být lineárně závislé, tedy existuje netriviální racionální lineární kombinavce $q_0 + q_1(2 + 5\sqrt{3}) + q_2(2 + 5\sqrt{3})^2 = q_1 + q_2(2 + 5\sqrt{3}) + q_2(79 + 20\sqrt{3}) = 0$. Vyjádřeno v souřadnicích vzhledem k bázi 1, $\sqrt{3}$ řešíme homogenní soustavu lineárních rovnic $q_0 + 2q_1 + 79q_2 = 0$, $5q_1 + 20q_2 = 0$ s maticí $\begin{pmatrix} 1 & 2 & 79 \\ 0 & 5 & 20 \end{pmatrix}$. Tedy řešením je například vektor $(q_0, q_1, q_2) = (-71, -4, 1)$, což znamená, že je algebraický prvek $2 + 5\sqrt{3}$ kořenem polynomu $m_1 = x^2 - 4x - 71$.

Podobně budeme uvažovat o prvku $\frac{2-\sqrt{3}}{3+\sqrt{3}}$. Nejprve ho ovšem vyjádříme v bázi 1, $\sqrt{3}$, tedy $\frac{2-\sqrt{3}}{3+\sqrt{3}} = \frac{(2-\sqrt{3})(3-\sqrt{3})}{(3+\sqrt{3})(3-\sqrt{3})} = \frac{9-5\sqrt{3}}{6}$ a opět hledáme $q_i \in \mathbf{Q}$, aby $q_0 + q_1\frac{9-5\sqrt{3}}{6} + q_2(\frac{9-5\sqrt{3}}{6})^2 = 0$, tedy $36q_0 + q_1(54 - 30\sqrt{3}) + q_2(156 - 90\sqrt{3}) = 0$. Řešíme protřo soustavu s maticí

$$\begin{pmatrix} 36 & 54 & 156 \\ 0 & -30 & -90 \end{pmatrix} \sim \begin{pmatrix} 6 & 0 & -1 \\ 0 & 1 & 3 \end{pmatrix}.$$

Tedy snadno najdeme řešení $(q_0, q_1, q_2) = (-\frac{1}{6}, -3, 1)$, jemuž odpovídá monický polynom $m_2 = x^2 - 3x - \frac{1}{6}$ s kořenem $\frac{2-\sqrt{3}}{3+\sqrt{3}}$. Protože jsou oba polynomy m_1 a m_2 monické stupně dva a ani jedno z uvažovaných iracionálních čísel není kořenem racionálního polynomu stupně jedna, je m_1 minimální polynom prvku $2 + 5\sqrt{3}$ nad $\mathbf{Q}$ a m_2 minimální polynom prvku $\frac{2-\sqrt{3}}{3+\sqrt{3}}$ nad $\mathbf{Q}$.

(f) Jako v (a) stačí uvážit, že $\sqrt[3]{2}$ je kořenem polynom $x^3 - 2 \in \mathbf{Q}[x]$.

(g) Protože minimální polynom určitě dělí $x^3 - 2$ v oboru $\mathbf{Q}[x]$, máme $[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] \leq \deg(x^3 - 2) = 3$. To znamená, že mocniny prvku $(\sqrt[3]{2})^0 = 1$, $(\sqrt[3]{2})^1 = \sqrt[3]{2}$

a $(\sqrt[3]{2})^2 = \sqrt[3]{4}$ generují vektorový prostor $\mathbf{Q}(\sqrt[3]{2})$ nad tělesem $\mathbf{Q}$. Ukážeme, že se jedná o bázi $\mathbf{Q}(\sqrt[3]{2})$.

6.5.

(h) Uvážíme-li, že podle (b) je $[\mathbf{Q}(\sqrt{3}) : \mathbf{Q}] = 3$ a že prvek $\sqrt[5]{5}$ je kořenem polynomu $x^5 - 5$, který můžeme chápat jako polynom nad tělesem $\mathbf{Q}(\sqrt[3]{2})$, tedy stupeň minimálního polynomu prvku $\sqrt[5]{5}$ nad $\mathbf{Q}(\sqrt[3]{2})$ je nejvýše 5, proto $[\mathbf{Q}(\sqrt[3]{2}, \sqrt[5]{5}) : \mathbf{Q}(\sqrt[3]{2})] \leq 5$. Podle pozorování z přednášky je

$$[\mathbf{Q}(\sqrt[3]{2}, \sqrt[5]{5}) : \mathbf{Q}] = [\mathbf{Q}(\sqrt[3]{2}, \sqrt[5]{5}) : \mathbf{Q}(\sqrt[3]{2})] \cdot [\mathbf{Q}(\sqrt{3}) : \mathbf{Q}] \leq 5 \cdot 3 = 15.$$

(i) Stačí si podrobněji prohlédnout důkazy tvrzení využívaných v (h), abychom zjistili, že množina $\{\sqrt[3]{2}^i \cdot \sqrt[5]{5}^j \mid i = 0,1,2; j = 0,1,2,3,4\}$, protože $1, \sqrt[3]{2}, \sqrt[3]{2}^2$ generuje $\mathbf{Q}(\sqrt[3]{2})$ nad $\mathbf{Q}$ $1, \sqrt[5]{5}, \sqrt[5]{5}^2, \sqrt[5]{5}^3, \sqrt[5]{5}^4$ generuje $\mathbf{Q}(\sqrt[3]{2}, \sqrt[5]{5})$ nad $\mathbf{Q}(\sqrt[3]{2})$. $\square$

3.6. Uvažujme faktorový okruh $\mathbf{Q}[x]/(x^3-2)\mathbf{Q}[x]$ okruhu polynomů $(\mathbf{Q}[x], +, -, 0, \cdot, 1)$.

(a) Dokažte, že je $\mathbf{Q}[x]/(x^3 - 2)\mathbf{Q}[x]$ těleso,
(b) ověřte, že $\mathbf{Q}[x]/(x^3 - 2)\mathbf{Q}[x] \cong Q(\sqrt[3]{2})$,
(c) ověřte, že $(x + 1) + (x^3 - 2)\mathbf{Q}[x] = (x^3 + x - 1) + (x^3 - 2)\mathbf{Q}[x]$,
(d) najděte v $\mathbf{Q}[x]/(x^3 - 2)\mathbf{Q}[x]$ inverzní prvek k prvku $x + 1 + (x^3 - 2)\mathbf{Q}[x]$.

(a) Protože je podle 3.5(c) polynom x^3-2 minimálním polynomem prvku $\sqrt[3]{2}$ nad $\mathbf{Q}$, jedná se o nerozložitelný polynom okruhu $(\mathbf{Q}[x], +, -, 0, \cdot, 1)$, tedy je hlavní ideál $(x^3 - 2)\mathbf{Q}[x]$ maximální. Nyní stačí připomenou, že faktor komutativního okruhu podle maximálního ideálu je těleso.

(b) Vezmemem-li dosazovací homomorfismus $\mathrm{id}_{\sqrt[3]{2}} : \mathbf{Q}[x] \to \mathbf{Q}(\sqrt[3]{2})$, vidíme díky 3.5, že jde o homomorfismus na a jádro $\mathrm{Ker}(\mathrm{id}_{\sqrt[3]{2}}) = (x^3 - 2)\mathbf{Q}[x]$. Díky první větě o izomorfismu dostáváme $\mathbf{Q}[x]/(x^3 - 2)\mathbf{Q}[x] = \mathbf{Q}[x]/\mathrm{Ker}(\mathrm{id}_{\sqrt[3]{2}}) \cong Q(\sqrt[3]{2})$.

(c) Připoeňme, že dvě rozkladové třídy podle ideálu I splývají, jestliže rozdíl jejich reprezentantantů leží v I. Tedy stačí nahédnout, že $(x^3 + x - 1) - (x + 1) = x^3 - 2 \in (x^3 - 2)\mathbf{Q}[x]$.

(d) Najdeme-li Eukleidovým algoritmem polynomy $q, r \in \mathbf{Q}[x]$, aby $(x + 1)q + (x^3 - 2)r = c$, kde c je invertibilní, vidíme, že $c^{-1}q$ je prvek rozkladové třídy hledaného inverzu. Tedy vydělíme se zbytkem $x^3 - 2 = (x + 1)(x^2 - x + 1) - 3$, a proto $-3 = -(x+1)(x^2 - x + 1) + (x^3 - 2)$ a $1 = (x+1)\frac{1}{3}(x^2 - x + 1) - \frac{1}{3}(x^3 - 2)$. Tudíž $(x + 1 + (x^3 - 2)\mathbf{Q}[x])^{-1} = \frac{1}{3}(x^2 - x + 1) + (x^3 - 2)\mathbf{Q}[x]$. $\square$

3.7. Najděte kořenové nadtěleso polynomu $p \in T[x]$ nad tělesem T, jestliže

(a) $T = \mathbf{Q}$ a $p = x^3 - 1$,
(b) $T = \mathbf{Q}$ a $p = x^3 - 2$,
(c) $T = \mathbf{Z}_2$ a $p = x^2 + 1$,
(d) $T = \mathbf{Z}_2$ a $p = x^2 + x + 1$.

(a) Protože je $1 \in \mathbf{Q}$ kořenem polynomu $x^3 - 1$, je samotné těleso $\mathbf{Q}$ už jeho kořenovým nadtělesem.

(b) V 3.5 jsme zjistili, že v tělese $\mathbf{Q}(\sqrt[3]{2})$ má polynom $p = x^3 - 2$ kořen $\sqrt[3]{2}$, navíc je $\mathbf{Q}(\sqrt[3]{2})$ nejmenší podtěleso $\mathbf{R}$ obsahující $\sqrt[3]{2}$ a $\mathbf{Q}$, proto jde právě o kořenové nadtěleso.

Také jsme mohli sestrojit kořenové nadtěleso stejně jako ve větě, která ukazuje jeho existenci, tj. mohli jsme uvážit, že je $p = x^3 - 2$ ireducibilní v $\mathbf{Q}[x]$ a vzít faktorový okruh $\mathbf{Q}[x]/(x^3 - 2)\mathbf{Q}[x]$.

(c) Podobně jako v (a) je Protože je $1 \in \mathbf{Z}_2$ kořenem polynomu $x^2 + 1$, je $\mathbf{Z}_2$ kořenovým nadtělesem tohoto polynomu.

(d) Tentokrát stejně jako v 2.konstrukci z (b) vezmeme těleso $\mathbf{Z}_2[x]/(x^2 + x + 1)\mathbf{Z}_2[x]$. Označíme-li $[a] = a+(x^2+x+1)\mathbf{Z}_2[x]$, všimněme si, že má těleso $\mathbf{Z}_2[x]/(x^2+x+1)\mathbf{Z}_2[x]$ právě 4 prvky: $[0]$, $[1]$, $[x]$, $[x + 1]$. □

13.5.

3.8. Nechť k a n jsou přirozená čísla. Dokažte, že

(a) $(x^k - 1)/(x^n - 1)$ v oboru $T[x]$ právě tehdy, když pro k/n, libovolné těleso T,

(b) $(p^k - 1)/(p^n - 1)$ v $\mathbf{N}$ právě tehdy, když pro k/n, libovolné prvočíslo p.

(a) ($\Leftarrow$) Jestliže $n = kd$, snadno spočítáme, že $x^n - 1 = (x^k - 1)\sum_{i=0}^{d-1} x^{ik}$.

($\Rightarrow$) Nechť $(x^k - 1)/(x^n - 1)$ a $n = kd + r$, kde $0 \le r < k$. Víme, že $x^{kd} - 1 = (x^k - 1)\sum_{i=0}^{d-1} x^{ik}$, tedy $(x^k - 1)/((x^n - 1) - (x^{kd} - 1))$. Protože $(x^n - 1) - (x^{kd} - 1) = x^{kd}(p^r - 1)$ a polynomy $x^k - 1$ a x^{kd} jsou nesoudělné, máme $(x^k - 1)/(x^r - 1)$. Ovšem $r < k$, proto $r = 0$.

(b) Uvažujeme stejně jako v (a) Jestliže $n = kd$,pak $p^n - 1 = (p^k - 1)\sum_{i=0}^{d-1} p^{ik}$. A v případě, že $(p^k - 1)/(p^n - 1)$ opět vydělíme se zbytkem $n = kd + r$, kde $0 \le r < k$ a dostaneme $(p^k - 1)/((p^n - 1) - (p^{kd} - 1))$. Protože $(p^n - 1) - (p^{kd} - 1) = p^{kd}(p^r - 1)$ a čísla $p^k - 1$ a p^{kd} jsou nesoudělná, máme $(p^k - 1)/(p^r - 1)$ a $r < k$, tedy opět $r = 0$. □

Další úlohy

(1) Dokažte, že je relace $\|$ na oboru integrity ekvivalencí.

(2) Je-li $(R, +, -, 0, \cdot, 1)$ obor integrity hlavních ideálů a $a, b \in R \setminus \{0\}$, dokažte, že $aR \cap bR = cR$ právě tehdy, když c je $\mathrm{nsn}(a, b)$, (tj. $a, b/c$ a pro každé takové d, že $a, b/d$ platí, že c/d).

(3) Popište nilpotentní prvky monoidového okruhu $\mathcal{RG}$, je-li $\mathcal{G}$ monoid z 1.4 a $\mathcal{R}$ obecný obor integrity.

(4) Buď $\mathcal{A} = (A, \cdot, 1)$ konečná komutativní grupa (chápaná jako monoid) a uvažujme monoidový okruh $\mathcal{QA}$ nad okruhem racionálních čísel.
   (a) Popište operace okruhu $\mathcal{QA} = (\mathbf{Q}A, +, -, \mathbf{0}, \cdot, \mathbf{1})$,
   (b) rozhodněte, zda je $\mathcal{QA}$ obor integrity,
   (c) popište nilpotentní prvky okruhu $\mathcal{QA}$,
   (d) najděte nejmenší kladné celé n a ideál I okruhu $\mathbf{Q}[x_1, \ldots, x_n]$, aby $\mathbf{Q}[x_1, \ldots, x_n]/I \cong \mathbf{Q}A$.

(5) Uvažujme okruh $(\mathbf{Z}[x], +, -, 0, \cdot, 1)$ a jeho prvky $p = 2x^3 + 2$, $q = 6x^3 + 12x^2 + 6x + 12$, $r = 3x^2 + 3x - 18$.
   (a) Najděte největší společný dělitel dvojic p, q, dále p, r q, r,
   (b) najděte největší společný dělitel trojice p, q, r,

- (c) rozhodněte, zda jsou ideály $p\mathbf{Z}[x]+q\mathbf{Z}[x]$, $p\mathbf{Z}[x]+r\mathbf{Z}[x]$, $q\mathbf{Z}[x]+r\mathbf{Z}[x]$ a $p\mathbf{Z}[x]+q\mathbf{Z}[x]+r\mathbf{Z}[x]$ hlavní,
- (d) najděte ireducibilní rozklad prvků p, q i r.

(6) Vyřešte otázky předchozí úlohy v okruzích polynomů $(\mathbf{Q}[x],+,-,0,\cdot,1)$ a $(\mathbf{R}[x],+,-,0,\cdot,1)$.

(7) Rozhodněte, zda v okruhu R z 1.11 platí podmínky (D), (P) a (J).

(8) Uvažujme okruh $(\mathbf{Z}[i],+,-,0,\cdot,1)$.
- (a) spočítejte ireducibilní rozklad prvků $8i$, $12+5i$, $12-5i$, $11+7i$, $11-7i$.
- (b) najděte největší společný dělitel dvojice 64 a $(1-i)^9$,
- (c) najděte největší společný dělitel dvojice $15-3i$ a $3-15i$,
- (d) najděte největší společný dělitel dvojice $13-6i$ a $14+3i$,
- (e) dokažte, že jsou prvky $13-21i$ a $17+11i$ nesoudělné a najděte $\alpha,\beta\in\mathbf{Z}[i]$, aby $\alpha\cdot(13-21i)+\beta\cdot(17+11i)=1$

(9) Najděte pro symetrický polynom $p\in S_{\mathbf{Q}}[x_1,x_2,x_3,x_4]$ takový polynom $f\in\mathbf{Q}[x_1,x_2,x_3,x_4]$, aby $p=f(\delta_{14},\delta_{24},\delta_{34},\delta_{44})$, jestliže
- (a) $p=x_1^3+x_2^3+x_3^3+x_4^3+1$,
- (b) $p=x_1^4+x_2^4+x_3^4+x_4^4+1$,
- (c) $p=x_1^5+x_2^5+x_3^5+x_4^5+1$.

(10) Najděte nad všechny kořeny polynomu p a určete jejich násobnost, jstliže
- (a) $p=x^5+x^3+x^2+1\in\mathbf{Z}_2[x]$,
- (b) $p=x^5+x^3+x^2+1\in\mathbf{U}[x]$, kde U je čtyřprvkové těleso,
- (c) $p=x^5+x^3+x^2+1\in\mathbf{U}[x]$, kde U je osmiprvkové těleso,
- (d) $p=x^5+x^3+x^2+1\in\mathbf{Z}_5[x]$,
- (e) $p=x^5+2x^3+x^2+1\in\mathbf{Z}_5[x]$,
- (f) $p=x^5+x^3+x^2+1\in\mathbf{Z}_7[x]$,

(11) Rozhodněte, zda má polynom $x^7-x^3+2x^2+1\in\mathbf{C}[x]$ nějaký vícenásobný komplexní kořen.

(12) Uvažujme tělesa komplexních čísel $\mathbf{C}$ a jeho podtěleso racionálních čísel $\mathbf{Q}$.
- (a) Dokažte , že jsou prvky $\alpha=2+\sqrt[5]{5}+3i$, $\beta=(2+\sqrt[5]{5}+3i)^{-1}$ $\gamma=\frac{3i-\sqrt[3]{3}+i\sqrt[3]{18}}{3-i+\sqrt{6}+[4]\sqrt{6}}$ algebraické nad $\mathbf{Q}$,
- (b) spočítejte stupně rozšíření $[\mathbf{Q}(\alpha):\mathbf{Q}]$, $[\mathbf{Q}(\beta):\mathbf{Q}]$, $[\mathbf{Q}(\gamma):\mathbf{Q}]$, $[\mathbf{Q}(\alpha,\beta):\mathbf{Q}]$, $[\mathbf{Q}(\alpha,\gamma):\mathbf{Q}]$, $[\mathbf{Q}(\alpha,\beta,\gamma):\mathbf{Q}]$ a $[\mathbf{Q}(\alpha,\beta):\mathbf{Q}(\alpha)]$.
- (c) najděte nad $\mathbf{Q}$ a nad $\mathbf{R}$ minimální polynom prvků α, β, γ, $\alpha\beta$, $\alpha+\beta$.

(13) Najděte rozkladové nadtěleso polynomu $p\in T[x]$ nad tělesem T, jestliže
- (a) pro všechny případy z 3.7,
- (b) $T=\mathbf{R}$ a $p=x^2+1$,
- (c) $T=\mathbf{Q}$ a $p=x^2+1$,
- (d) $T=\mathbf{Z}_3$ a $p=x^2+1$.

(14)

(15)