# Algebra — cvičení 2, řešení

**2. (a)** Tohle jsme si řekli on-line, ale byl jsem upozorněn, že v definici homomorfismu okruhů z přednášky nemáte podmínku, že 1 se musí poslat na 1 (jde-li o homomorfismus mezi okruhy s jednotkou). To je z mnoha důvodů nešťastné. Stěží existuje nějaký přirozený kontext, kde by dávalo smysl se bavit o homomorfismech mezi dvěma okruhy s jednotkou, které nemusejí jednotku zachovávat (ale zachovávají násbení a sčítání). Pro definici z přednášky by tedy bylo řešením příkladu i $a = 0$, ale *domluvme se, že na cvičení nadále budeme uvažovat jen okruhy s jednotkou a homomorfismy okruhů, které jednotku zachovávají.*

**4.** a) Ať pro spor existuje okruhový izomorfismus $f : \mathbb{Q}[\sqrt{n}] \to \mathbb{Q}$, kde $n \in \mathbb{Z}$ je takové, že $\sqrt{n}$ je iracionální. Podle toho, co jsme si řekli on-line, musí platit $f(n) = n$. Zároveň ovšem $n = f(n) = f(\sqrt{n} \cdot \sqrt{n}) = f(\sqrt{n})f(\sqrt{n})$, což znamená, že $f(\sqrt{n})$ je racionální číslo, jehož druhou mocninou je $n$, tj. jde o kořen polynomu $x^2 - n \in \mathbb{Q}[x]$. Tyto kořeny jsou ale právě dva $\sqrt{n}$ a $-\sqrt{n}$ a oba jsou iracionální, spor.

b) Ať pro spor existuje okruhový izomorfismus $g : \mathbb{Q}[\sqrt{p}] \to \mathbb{Q}[\sqrt{q}]$, kde $p, q$ jsou různá prvočísla. Opět víme, že $g(p) = p$, a tedy také, že $p = g(p) = g(\sqrt{p} \cdot \sqrt{p}) = g(\sqrt{p})^2$. Jelikož má polynom $x^2 - p$ v $\mathbb{R}$ pouze dva kořeny $\pm\sqrt{p}$, nutně platí, že $g(\sqrt{p}) \in \{\sqrt{p}, -\sqrt{p}\}$. Ať již je znamínko takové či onaké, v důsledku dostáváme $\sqrt{p} \in \mathbb{Q}[\sqrt{q}]$. Existují proto $a, b \in \mathbb{Q}$ takové, že $\sqrt{p} = a + b\sqrt{q}$.

Umocníme na druhou a dostaneme $p = a^2 + 2ab\sqrt{q} + b^2 q$. Jelikož je $\sqrt{q}$ iracionální, musí nutně $ab = 0$. Dostáváme buď $p = a^2$, což je ihned spor, nebo $p = b^2 q$. V tomto druhém případě napíšeme $b = m/n$, kde $m \in \mathbb{Z}$ a $n \in \mathbb{N}$. Vynásobíme obě strany $n^2$ a obdržíme $pn^2 = m^2 q$. To je spor se základní větou aritmetiky; například proto, že na levé straně je v rozkladu na prvočísla lichý počet $p$, zatímco na pravé straně je sudý počet $p$ (což samozřejmě zahrnuje i možný nulový počet).

**5.** Prostým dosazením prvků ze $\mathbb{Z}_6$ zjistíme, že kořeny jsou $0, 2, 3, 5$. To nám dává dva rozklady: $x^2+x = (x-5)x$ a $x^2+x = (x-2)(x-3)$. K tomu, že jich není více, si například stačí uvědomit, že vydělení $x^2 + x$ libovolným kořenovým činitelem je jednoznačné. Stále nám zde totiž platí vztahy mezi kořeny a koeficienty: je-li $x^2 + ax + b = (x - k)(x - l)$, pak $-(k + l) = a$, pročež při fixovaných $a$ a $k$ existuje právě jedno $l$, a sice $-a - k$.

**6.** Stačí uvážit polynom $5x^2 + 5x = 5x(x + 1) = 5x(5x + 1)$. Ten má zřejmě deset kořenů. Zároveň zde můžete vidět, že vydělení polynomu $5x^2 + 5x$ polynomem $5x$ již jednoznačné není. (To souvisí s tím, že v $\mathbb{Z}_{10}$ není jednoznačné dělení pěti. Např. $5 \cdot 1 = 5 \cdot 5 = 5$.)

**7.** Na cvičení jsem říkal, že zde stačí uvažovat podílové těleso oboru $\mathbb{Z}[i]$ jakožto podtěleso tělesa $\mathbb{C}$ sestávající z prvků $\left\{\frac{a+bi}{c+di};\ a, b, c, d \in \mathbb{Z}, c + di \neq 0\right\}$. Pokud bychom chtěli být ale opravdu poctiví, pak bychom se na zlomky $\frac{a+bi}{c+di}$ měli dívat ne jako na komplexní čísla, ale jako na jisté ekvivalenční bloky reprezentované dvojicemi $(a+bi, c+di)$, s nimiž se počítá tak, jak bylo řečeno na přednášce, když jste se bavili o podílovém tělese. Označíme-li $Q$ toto formální podílové těleso, budeme přirozeně chtít ukázat, že je izomorfní tělesu $\mathbb{Q}(i)$.

Zadefinujeme si proto zobrazení $f : Q \to \mathbb{C}$ vztahem $f\left(\frac{a+bi}{c+di}\right) = \frac{a+bi}{c+di}$, kde se na pravé straně díváme na zlomek klasicky jako na komplexní číslo, ale v argumentu zobrazení $f$ jakožto na formální výraz.

Předně se musíme zeptat, zda je vůbec takto definované zobrazení korektní. Zda nezávisí na volbě reprezentanta ekvivalenčního bloku. K tomu si musíme připomenout, kdy v našem podílovém tělese $Q$, podle definice, platí $\frac{a+bi}{c+di} = \frac{a'+b'i}{c'+d'i}$. Zjistíme, že je to právě

tehdy, když $(a+bi)(c'+d'i) = (a'+b'i)(c+di)$ platí v $\mathbb{Z}[i]$. Souhrou naprosto předvídatelných okolností totéž platí pro zlomky v komplexních číslech. Z toho ihned vidíme nejen, že je zobrazení $f$ korektně definováno, ale také, že je prosté.

K tomu, abychom ověřili, že se jedná o homomorfismus okruhů, si musíme připomenout, jak jsou $0, 1$ a binární operace sčítání a násobení definovány v $Q$. Zjistíme, že $0 = \frac{0}{1}$ a $1 = \frac{1}{1}$, a tedy $f(0) = 0$ a $f(1) = 1$. Operace sčítání a násobení jsou (opět nikoliv čirou náhodou) definovány v tělese $Q$ právě tak jako sčítání a násobení zlomků. Dostáváme, že $f$ je prostý homomorfismus.

Jeho obrazem (chcete-li oborem hodnot) je právě množina všech komplexních čísel tvaru $\frac{a+bi}{c+di}$, kde $a, b, c, d \in \mathbb{Z}$. Po úpravě dostaneme $\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i \in \mathbb{Q}(i)$. Jelikož obraz homomorfismu $f$ je izomorfní kopie tělesa $Q$, jedná se jistě o podokruh tělesa $\mathbb{C}$ (jde dokonce o podtěleso). Tento podokruh obsahuje (pro volbu $b = d = 0$) všechna racionální čísla a zároveň i $i$ (pro volbu $a = d = 0$ a $b = c = 1$). Dohromady proto musí být tento podokruh roven tělesu $\mathbb{Q}(i)$.

**9.** Uvedu pouze výsledky pro kontrolu. Pro **(a)** máme podíl $x^2+3x+2$ a zbytek $-5x-1 \in \mathbb{Z}[x]$, resp. zbytek $4 \in \mathbb{Z}_5[x]$. V části **(b)** pak vyjde $x^9 + x^6 + x^5 + x^2 + 1$, zbytek 1.

**10.** Místo oboru $\mathbf{T}[x]$ můžeme uvažovat libovolný obor $\mathbf{R}$. Víme-li, že existuje $c \in R$ takové, že $cf = g$, a zároveň $d \in R$ takové, že $dg = f$, pak je $cdg = g$. Pokud je $g = 0$ nebo $f = 0$, pak $g = f = 0$ a můžeme volit $u = 1$. V opačném případě můžeme v rovnosti $cdg = g$ vykrátit nenulové $g$, čímž obdržíme $cd = 1$. Volbou $u = d$ pak máme $f = ug$, přičemž $u$ je invertibilním prvkem oboru $\mathbf{R}$. Ve speciálním případě, kdy $\mathbf{R} = \mathbf{T}[x]$, tedy dostáváme, že $u \in T$, $u \neq 0$ (polynom jiného než nulového stupně nad oborem k sobě nemá inverzní prvek).

**11.** Opět pouze výsledky pro kontrolu. **(a)** $\mathrm{NSD}(f, g) = 2 = (2x+1)f+(x^2+x+2)g$ v $\mathbb{Z}_3[x]$ a $\mathrm{NSD}(f, g) = x+3 = f+(4x+1)g$ v $\mathbb{Z}_5[x]$. **(b)** $\mathrm{NSD}(f, g) = 7x-14 = (-x-2)f+(x+3)g$. Samozřejmě, vzhledem k tomu, že NSD je určen až na násobek invertibilním prvkem, lze místo $2 \in \mathbb{Z}_3[x]$ v **(a)** dostat jako výsledek i 1, místo $x + 3 \in \mathbb{Z}_5[x]$ zase např. $2x + 1$ či $3x + 4$. Nakonec v části **(b)** lze za NSD vzít i $x - 2$, ovšem pak budete potřebovat Bézoutovy koeficienty, které neleží v $\mathbb{Z}[x]$.

**12.** Jistě $x = y = z = w = 0$ je řešením. Říkejme mu třeba nulové. Předpokládejme, že existuje ještě nějaké jiné. Pak jistě $w \neq 0$. Dále uvažujme nějaké řešení s nejmenší možnou kladnou hodnotou $|w|$. Využijeme nápovědu, abychom dostali, že $x^2 + y^2 + z^2 \equiv 7w^2 \pmod 8$. To lze ekvivalentně upravit (přičtením $w^2$ k oběma stranám) na $8 \mid x^2 + y^2 + z^2 + w^2$. Vzpomeneme si na cvičení z minula, kde jsme si všimli, že $a^2 \equiv 1 \pmod 8$ pro libovolné $a$ liché. Analogicky vypozorujeme, že $a^2 \equiv 0 \pmod 8$ nebo $a^2 \equiv 4 \pmod 8$, pokud je $a$ sudé.

Z posledně zmíněného snadno vyplývá, že aby $8 \mid x^2 + y^2 + z^2 + w^2$, musí být všechna čísla $x, y, z, w$ sudá. To ovšem znamená, že v původním vztahu $x^2 + y^2 + z^2 = 15w^2$ můžeme obě strany vydělit čtyřmi, čímž dostaneme, že i $(x/2, y/2, z/2, w/2)$ je (nenulovým) celočíselným řešením. To je spor s uvažovanou minimalitou hodnoty $|w|$. Žádné nenulové celočíselné řešení zadané rovnice proto neexistuje.

**13.** K důkazu potřebujeme i operaci sčítání a distributivitu; se samotným násobením si nevystačíme. Pro $a, b \in R$ budeme počítat $(a + b)^2$. Dostaneme

$$a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b,$$

kde využíváme v první a poslední rovnosti booleovskost okruhu. Po odečtení $a + b$ obdržíme $0 = ab + ba$, což dává $ab = -(ba)$. Toto musí platit pro všechna $a, b \in R$, tedy i

pro volbu $a = b$, která ústí v $a = a^2 = -(a^2) = -a$. To je ale opět vlastnost všech prvků $a \in R$. Speciálně i pro libovolný součin $ba$ obdržíme $ba = -(ba)$. Dáme-li vše dohromady, máme kýžené $ab = ba$.

**14.** Pro $n = 0$ dokazovaný vztah triviálně platí. Buď dále $n > 0$. Označíme-li $\sigma : R \to R$ zobrazení definované vztahem $\sigma(a) = a^p$, pak je jistě $(a+b)^{p^n}$ pouhou $n$-násobnou aplikací zobrazení $\sigma$ na prvek $a + b$, tj. $(a+b)^{p^n} = \sigma^n(a+b)$. Stačí proto, abychom dokázali, že $(a+b)^p = a^p + b^p$. Zbytek plyne přímočaře indukcí.

Nepřekvapivě užijeme binomickou formuli: $(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$. Můžeme ji ale vůbec použít? Počítáme v nějakém blíže nespecifikovaném oboru $\mathbf{R}$. Jak tam chápeme kombinační číslo? Jelikož binomická formule je jen výsledkem vícenásobné aplikace distributivity (a ovšem i asociativity a komutativity sčítání a násobení), není kombinační číslo ničím jiným, než součtem odpovídajícího počtu jedniček. Z definice $\binom{p}{k} = \frac{p!}{k!(p-k)!} \in \mathbb{N}$, přičemž vzhledem k tomu, že $p$ je prvočíslo, nemůže se $p$ v čitateli zkrátit s žádným činitelem z jmenovatele, pokud $0 < k < p$. Jinak řečeno, pro $0 < k < p$ máme $p | \binom{p}{k}$, což v oboru charakteristiky $p$ znamená, že $\binom{p}{k} = 0$. Z binomické formule proto zbývá $(a+b)^p = a^p + b^p$.

Ukázali jsme, že $\sigma$ zachovává sčítání. Zároveň jistě $\sigma(1) = 1$ a $\sigma(ab) = (ab)^p = a^p b^p = \sigma(a)\sigma(b)$. Zobrazení $\sigma$ je tedy endomorfismem oboru $\mathbf{R}$. Navíc je prosté, jelikož $\sigma(a) = \sigma(b)$ implikuje $0 = a^p - b^p = a^p + (-b)^p$, kde poslední rovnost jistě platí pro $p$ liché a platí i pro $p = 2$, jelikož v tom případě $b = -b$; máme proto $0 = \sigma(a) + \sigma(-b) = \sigma(a-b) = (a-b)^p$, což je v oboru možné pouze pokud $a - b = 0$.

Všimněte si, že toto tvrzení nám pro konečné těleso $\mathbf{T}$ charakteristiky $p$ usnadňuje úpravy v $\mathbf{T}[x]$. Kupříkladu pro $p = 3$ máme $(x^2 + x + 1)^3 = x^6 + x^3 + 1$.

**15.** Buď $0 \neq f \in \mathbf{R}[x]$, kde $\mathbf{R}$ je obor. Dokazujeme indukcí podle stupně polynomu $f$. Je-li tento stupeň roven 0, pak tvrzení jistě platí.

Předpokládejme, že stupeň polynomu $f$ je $n > 0$. Nemá-li $f$ v $\mathbf{R}$ žádný kořen, tvrzení triviálně platí. Ať je tedy $a \in R$ kořenem polynomu $f$. Vydělíme (algoritmem dělení polynomů se zbytkem) $f$ kořenovým činitelem $x - a$. Dostaneme $f = (x-a)g$ pro nějaký $g \in \mathbf{R}[x]$ stupně $n-1$. Uvažujme nyní libovolný kořen $b \in R$ polynomu $f$. Dosazením dostáváme $0 = f(b) = (b-a)g(b)$. Jelikož je $\mathbf{R}$ obor, musí být buď $b - a = 0$, nebo $g(b) = 0$. Proto je $b$ buď kořenem polynomu $g$, kterých je z indukčního předpokladu nejvýše $n-1$, nebo $b = a$. Dostáváme, že $f$ má v $\mathbf{R}$ nejvýše $n$ kořenů.

**16.** Uvažujeme zobrazení $d : \mathbb{Q}[x] \to \mathbb{Q}[\pi]$ takové, že $d(\sum_{k=0}^{n} a_k x^k) = \sum_{k=0}^{n} a_k \pi^k$. V argumentu zobrazení $d$ máme polynom s racionálními koeficienty, zatímco na pravé straně je (po dosazení) součet součinů $a_k \pi^k$ přes $k$ jdoucí od 0 do $n$ spočtený v okruhu $\mathbb{Q}[\pi]$.

Není těžké ověřit, že $d$ je homomorfismus okruhů. Říká se mu *dosazovací*. Tato terminologie se používá kdykoliv do polynomů nad nějakým okruhem dosazujeme prvek z jeho (komutativního) nadokruhu. Ověření toho, že $d$ je skutečně homomorfismus, se redukuje na pozorování, že operace dosazení do polynomu komutuje se sčítáním a násobením (a že $d(1) = 1$).

V obrazu homomorfismu $d$ se nachází jak $\pi = d(x)$, tak libovolné $q \in \mathbb{Q}$, jelikož $q = d(q)$. Zároveň je obraz jistě uzavřený na operace sčítání a násobení, pročež musí být roven celému $\mathbb{Q}[\pi]$. Konečně $d$ je prosté. Kdyby totiž $d(f) = d(g)$, pro nějaké $f \neq g$, pak $d(f-g) = (f-g)(\pi) = 0$, což by byl spor s předpokladem, že $\pi$ není kořenem žádného nenulového polynomu s racionálními koeficienty.