1. Test 07/08 zimní semestr

Příklad 1. *Euklidovým algoritmem najděte celá čísla k, l taková, že $NSD(81, 24) = k \cdot 81 + l \cdot 24$.*

Řešení. Platí

$$\begin{aligned} \mathbf{81} &= 3 \cdot \mathbf{24} + \mathbf{9} \\ \mathbf{24} &= 2 \cdot \mathbf{9} + \mathbf{6} \\ \mathbf{9} &= 1 \cdot \mathbf{6} + \mathbf{3} \\ \mathbf{6} &= 2 \cdot \mathbf{3} + \mathbf{0}, \end{aligned}$$

tedy $NSD(81, 24) = 3$. Zpětně dopočteme čísla k, l.

$\mathbf{3} = \mathbf{9} - 1 \cdot \mathbf{6} = \mathbf{9} - 1 \cdot (\mathbf{24} - 2 \cdot \mathbf{9}) = (-1) \cdot \mathbf{24} + 3 \cdot \mathbf{9} = (-1) \cdot \mathbf{24} + 3 \cdot (\mathbf{81} - 3 \cdot \mathbf{24}) = 3 \cdot \mathbf{81} - 10 \cdot \mathbf{24}$.

Řešením je $(k, l) = (3, -10)$ (všech řešení je samozřejmě nekonečně mnoho).

Poznámky. Skupina ve 14:00 měla nepatrně jiné zadání $NSD(105, 24) = 3 \cdot 105 - 13 \cdot 24$.

Příklad 2. *Operace $\odot$ algebry $\mathbb{A} = \{0, 1, 2, 3\}(\odot)$ je dána následující tabulkou*

$\odot$	0	1	2	3
0	2	0	0	2
1	3	1	1	3
2	2	2	0	2
3	1	3	1	1

.

(a) Najděte všechny podalgebry algebry $\mathbb{A}$.

(b) Najděte všechny kongruence algebry $\mathbb{A}$.

Řešení.

(a) Nejprve si všimneme, že pro libovolnou podalgebru B (resp. její nosnou množinu) platí

(i) $0 \in B$ právě když $2 \in B$ (protože $0 \odot 0 = 2$ a $2 \odot 2 = 0$, což dokazuje obě implikace),

(ii) z $3 \in B$ plyne $1 \in B$ (protože $3 \odot 3 = 1$).

Probereme jednotlivé případy podle počtu prvků. Hledanou podalgebru budeme značit B

– **Prázdná množina** je podalgebrou (pokud jí vůbec považujeme za algebru).
– **Jednoprvké podalgebry.** Z (i) a (ii) plyne, že jedinou možností je $B = \{2\}$. To je skutečně podalgebra (neboť $2 \odot 2 = 2$).
– **Dvouprvkové podalgebry.** Z (i) plyne, že pokud $0 \in B$ nebo $2 \in B$, pak $\{0, 2\} \in B$. Z tabulky vidíme, že $\{0, 2\}$ je podalgebra. Zbývá jediná možnost, a to $B = \{1, 3\}$. To je rovněž podalgebra.
– **Tříprvkové podalgebry.** Zřejmě $0 \in B$ nebo $2 \in B$ (díky počtu prvků), čili $\{0, 2\} \in B$ (opět jsme použili (i)). Zbývají dvě možnosti – $B_1 = \{0, 1, 2\}$ a $B_2 = \{0, 2, 3\}$. B_2 není podalgebra podle (ii), B_1 není podalgebra, protože $1 \odot 0 = 3$.
– **Čtyřprvková možina** je podalgebrou.

Podalgebry $\mathbb{A}$ jsou $(\emptyset), \{2\}, \{0, 2\}, \{1, 3\}, \{0, 1, 2, 3\}$.

(b) Využijeme toho, že ekvivalence $\sim$ je kongruencí algebry $\mathbb{A}$ právě tehdy, když

$$(*) \qquad (\forall a, b, c \in \mathbb{A})\ a \sim b \Rightarrow c \odot a \sim c \odot b \ \&\ a \odot c \sim b \odot c.$$

Pokud $0 \sim 1$ pak $2 = 0 \odot 0 \sim 1 \odot 0 = 3$ a též $2 = 0 \odot 0 \sim 0 \odot 1 = 0$, tedy $\sim$ je triviální kongruence. Z $0 \sim 3$ vyplývá $0 = 0 \odot 2 \sim 3 \odot 2 = 1$, tedy opět $\sim$ je triviální. Podobně zjistíme, že na triviální kongruenci vede $1 \sim 2$ i $2 \sim 3$ a také, že z $0 \sim 2$ vyplývá $1 \sim 3$ a naopak z $1 \sim 3$ plyne $0 \sim 2$. Zbývá jediná netriviální kongruence – kongruence s rozkladovými třídami $\{0, 2\}, \{1, 3\}$. Zkontrolováním podmínky $(*)$ zjistíme, že jde skutečně o kongruenci.

Kongruence $\mathbb{A}$ jsou $\{\{0\}, \{1\}, \{2\}, \{3\}\}, \{\{0, 2\}, \{1, 3\}\}, \{\{0, 1, 2, 3\}\}$. (Vypsali jsme rozklady určené kongruencemi.)

Poznámky. Skupina ve 14:00 měla prvky přeznačené $2 \leftrightarrow 3$.

Příklad 3. *Najděte podalgebru B algebry $\mathbb{C}(+)$ generovanou množinou $\{-1, 2i\}$.*

Řešení. Protože $-1 \in B$, je také $-2 = (-1) + (-1) \in B$. Protože $-1, -2 \in B$, máme $-3 = (-2) + (-1) \in B$. Je vidět, že indukcí lze dokázat $-n \in B$ pro libovolné $n \in \mathbb{N}$. Podobně nahlédneme, že $2ki \in B$ pro libovolné $k \in \mathbb{N}$. Pro libovolná $k, n \in \mathbb{N}$ máme $-n \in B$ a $2ki \in B$ tedy i $-n + 2ki \in B$. Dokázali jsme, že

$$\begin{aligned} B &\supseteq \{-n \mid n \in \mathbb{N}\} \cup \{2ki \mid k \in \mathbb{N}\} \cup \{-n + 2ki \mid 2ki - n \in \mathbb{N}\} \\ &= \{-n + 2ki \mid k, n \in \mathbb{N}_0\} - \{0\}. \end{aligned}$$

Snadno ověříme, že množina na pravé straně inkluze je uzavřená na operaci $+$, tedy

$$B = \{-n + 2ki \mid k, n \in \mathbb{N}_0\} - \{0\}.$$

Poznámky. Skupina ve 14:00 měla množinu $\{-3, 2i\}$

Příklad 4. *Zjistěte, zda platí následující.*

(a) $\mathbb{C}(+) \cong \mathbb{R}(+) \times \mathbb{R}(+)$.

(b) $\mathbb{C}(\cdot) \cong \mathbb{R}(\cdot) \times \mathbb{R}(\cdot)$.

Řešení.

(a) Tvrzení platí. Dokážeme že zobrazení $f : \mathbb{C}(+) \to \mathbb{R}(+) \times \mathbb{R}(+)$ dané vztahem $f(a + bi) = (a, b)$ je izomorfismus. Je tedy třeba ověřit, že f je homomorfismus a bijekce.

Bijektivita f je zřejmá. Pro důkaz kompatibility s operací vezmeme libovolné $a + bi, c + di \in \mathbb{C}$, spočítáme

$$\begin{aligned} f((a + bi) + (c + di)) &= f((a + c) + (b + d)i) = (a + c, b + d) \\ f(a + bi) + (c + di) &= (a, c) + (b, d) = (a + b, c + d) \end{aligned}$$

a jsme hotovi.

(b) Tvrzení neplatí. V $\mathbb{C}(\cdot)$ lze odmocňovat libovolné číslo, kdežto v $\mathbb{R}(+) \times \mathbb{R}(+)$ nelze (například nelze odmocnit $(-1, -1)$). Formálněji: tvrzení

$$(\forall x)\ (\exists y)\ y \cdot y = x$$

platí v algebře na levé straně a nikoliv v algebře na pravé straně. Platnost uvedené formule se přitom libovolným izomorfismem přenáší.

Alternativně lze např. použít skutečnost, že v $\mathbb{C}(\cdot)$ existují libovolné primitivní odmocniny (např čtvrtá). Formálněji: tvrzení

$$(\exists x)\ (x \cdot x \cdot x \cdot x = x)\ \&\ (x \cdot x \cdot x \neq x)$$

platí v $\mathbb{C}(\cdot)$ (např pro $x = i$), ale neplatí v druhé algebře.

Příklad 5. *Najděte všechny homomorfismy $\mathbb{Z}(f) \to \mathbb{Z}(g)$, kde unární operace f, g jsou dány předpisy*

$$f(x) = x + 1, \quad g(x) = \begin{cases} x - 1 & \text{když } x \geq 2 \\ 1 & \text{když } x = 1 \end{cases}$$

Řešení. Označme h libovolný homomorfismus $\mathbb{Z}(f) \to \mathbb{Z}(g)$. Pro libovolné $x \in \mathbb{Z}$ platí $h(f(x)) = g(h(x))$, neboli

$$(*) \qquad h(x+1) = h(x) - 1, \text{ pokud } h(x) \geq 2, \quad h(x+1) = 1, \text{ pokud } h(x) = 1$$

Předpokládejme, že pro nějaké číslo $a \in \mathbb{Z}$ je $h(a) \neq 1$. Pokud $h(a) \neq 2$, pak využitím $(*)$ dostáváme $h(a+1) = h(a) - 1$. Buď $h(a+1) \neq 2$, nebo opět použijeme $(*)$ a zjistíme, že $h(a+2) = h(a) - 2$. Takto zřejmě nalezneme $b \in \mathbb{Z}$ takové, že $h(b) = 2$. Nyní aplikací $(*)$ zjistíme $h(b+1) = 1$, dále $1 = h(b+2) = h(b+3) = \ldots$. Rovněž zjistíme, že $h(b-1) = 3$, $h(b-2) = 4$, $\ldots$. Máme tedy

$$h(x) = \begin{cases} 1 & \text{pokud } x > b \\ b - x + 2 & \text{pokud } x \geq b \end{cases}.$$

Snadno ověříme, že takto definované h je skutečně homomorfismus pro libovolné $b \in \mathbb{Z}$. Nalezli jsme tedy všechny homomorfismy, které nejsou konstantní s hodnotou 1. Zbývá zobrazení $h(x) = 1, x \in \mathbb{Z}$, které je rovněž homomorfismem.