

Algebra I – úlohy k procvičení – 14.10.2020 – řešení

1. Nechť G je grupa, ve které $(ab)^2 = a^2b^2$ pro všechna $a, b \in G$. Dokažte, že grupa G je komutativní.

ŘEŠENÍ. Zvolme libovolně $a, b \in G$. Chceme: $ab = ba$. Víme: $(ab)^2 = a^2b^2$. Takže $abab = aabb$. Krátíme zleva prvkem a a dostaneme $bab = abb$. Krátíme zprava prvkem b a dostaneme $ba = ab$.

2. Nechť G je konečná neprázdná množina s asociativní operací $*$. Nechť pro všechna $a, x, y \in G$ platí:

- jestliže $a * x = a * y$, pak $x = y$
- jestliže $x * a = y * a$, pak $x = y$

Dokažte, že množina G spolu s operací $*$ je grupa.

ŘEŠENÍ. Pro $u, v \in G$ pišme stručně uv místo $u * v$.

Nejdříve ukážeme, že operace $*$ má neutrální prvek.

Zvolme libovolně $a \in G$ (to můžeme, protože $G \neq \emptyset$).

Nechť množina G má n prvků (n je kladné celé číslo). Nechť $G = \{g_1, g_2, \dots, g_n\}$.

Prvky $ag_1, ag_2, \dots, ag_n$ jsou vzájemně různé. Zdůvodnění: Zvolme $i, j \in \{1, 2, \dots, n\}$, $i \neq j$. Chceme ukázat, že $ag_i \neq ag_j$. Předpokládejme, že $ag_i = ag_j$. Krátíme prvkem a zleva (dle zadání lze v G krátit zleva i zprava libovolným prvkem) a dostaneme $g_i = g_j$, což je spor, protože $i \neq j$. Nutně tedy $ag_i \neq ag_j$.

Množina $\{ag_1, ag_2, \dots, ag_n\}$ má n prvků (protože prvky $ag_1, ag_2, \dots, ag_n$ jsou vzájemně různé), množina G má n prvků a také $\{ag_1, ag_2, \dots, ag_n\} \subseteq G$. Z toho samozřejmě plyne, že $\{ag_1, ag_2, \dots, ag_n\} = G$.

Je $a \in G$, takže $a \in \{ag_1, ag_2, \dots, ag_n\}$, $a = ag_i$ pro nějaké $i \in \{1, 2, \dots, n\}$. Položme $e = g_i$. Je tedy $a = ae$.

Ukážeme, že e je neutrální prvek operace $*$.

Nechť $x \in G$. Chceme: $ex = x$, $xe = x$.

Je $a = ae$, takže $ax = aex$, což dává $x = ex$ (zleva jsme krátili prvkem a).

Z $a = ae$ máme $aa = aea$ a po krácení zleva dostaneme $a = ea$.

Je $a = ea$, takže $xa = xea$, což dává $x = xe$ (zprava jsme krátili prvkem a).

Zbývá nám ukázat, že pro každé $a \in G$ existuje $b \in G$ splňující $ab = e$ a $ba = e$.

Víme již, že pro libovolně zvolené $a \in G$ je $\{ag_1, ag_2, \dots, ag_n\} = G$. Je $e \in G$, takže $ag_j = e$ pro nějaké $j \in \{1, 2, \dots, n\}$.

Položme $b = g_j$. Pak $ab = e$. Zbývá ukázat, že $ba = e$. Počítejme:

$$aba = ea = a = ae, \quad aba = ae$$

Po krácení prvkem a zleva dostáváme $ba = e$.

3. Uveďte příklad neprázdné množiny A s operací $*$ tak, aby současně platilo:

- operace $*$ je asociativní
- pro všechna $a, x, y \in A$ platí: jestliže $a * x = a * y$, pak $x = y$
- pro všechna $a, x, y \in A$ platí: jestliže $x * a = y * a$, pak $x = y$
- A spolu s operací $*$ není grupa

ŘEŠENÍ. Položme $A = \mathbb{Z}^+$, $u * v = u \cdot v$ (pro libovolná $u, v \in \mathbb{Z}^+$). Ukážeme, že jsou splněny všechny čtyři body ze zadání.

- operace $\cdot$ je asociativní, protože operace násobení celých čísel je asociativní
- Nechť $a, x, y \in \mathbb{Z}^+$, $a \cdot x = a \cdot y$. Chceme: $x = y$. Máme $ax = ay$, $ax - ay = 0$, $a(x - y) = 0$. Je tedy $a = 0$ nebo $x - y = 0$. Protože $a \in \mathbb{Z}^+$, je $a \neq 0$ a tedy $x - y = 0$, $x = y$.
- Nechť $a, x, y \in \mathbb{Z}^+$, $x \cdot a = y \cdot a$. Chceme: $x = y$. Máme $xa = ya$, $xa - ya = 0$, $(x - y)a = 0$. Je tedy $x - y = 0$ nebo $a = 0$. Protože $a \in \mathbb{Z}^+$, je $a \neq 0$ a tedy $x - y = 0$, $x = y$.
- Operace násobení kladných celých čísel má neutrální prvek, totiž číslo 1. Předpokládejme, že $\mathbb{Z}^+$ spolu s operací násobení je grupa. Je $2 \in \mathbb{Z}^+$. Existuje tedy $x \in \mathbb{Z}^+$, $2 \cdot x = 1$. Z toho plyne, že číslo 1 je sudé, spor. Takže $\mathbb{Z}^+$ spolu s operací násobení není grupa.

4. (a) Najděte všechny prvky řádu 3 v grupě $\mathbb{C}$ (s operací sčítání).
(b) Najděte všechny prvky řádu 3 v grupě $\mathbb{C}^\times$ (s operací násobení).

ŘEŠENÍ.

(a) Necht $x \in \mathbb{C}$, x má řád 3. Pak

$$\begin{aligned}x + x + x &= 0 \\3x &= 0 \\x &= 0\end{aligned}$$

Ovšem 0 nemá řád 3, má řád 1.

Závěr: V grupě $\mathbb{C}$ (s operací sčítání) neexistuje žádný prvek řádu 3.

(b) Necht $x \in \mathbb{C}^\times$, x má řád 3. Pak

$$\begin{aligned}x \cdot x \cdot x &= 1 \\x^3 &= 1\end{aligned}$$

Necht $x = a + bi$, $a, b \in \mathbb{R}$.

$$\begin{aligned}x^3 &= (a + bi)^3 \\&= a^3 + 3a^2bi + 3a(bi)^2 + (bi)^3 \\&= a^3 + 3a^2bi - 3ab^2 - b^3i \\&= (a^3 - 3ab^2) + (3a^2b - b^3)i\end{aligned}$$

Je tedy $a^3 - 3ab^2 = 1$ a $3a^2b - b^3 = 0$.

$$\begin{aligned}3a^2b - b^3 &= 0 \\b \cdot (3a^2 - b^2) &= 0\end{aligned}$$

Jsou dvě možnosti:

i. $b = 0$:

$$\begin{aligned}a^3 - 3a \cdot 0^2 &= 1 \\a^3 &= 1 \\a &= 1\end{aligned}$$

Je $x = 1 + 0 \cdot i = 1$; ovšem 1 nemá řád 3, ale má řád 1.

ii. $3a^2 - b^2 = 0$: Je $b^2 = 3a^2$ a tedy

$$\begin{aligned}a^3 - 3ab^2 &= 1 \\a^3 - 3a(3a^2) &= 1 \\a^3 - 9a^3 &= 1 \\-8a^3 &= 1 \\a^3 &= -\frac{1}{8} \\a &= -\frac{1}{2}\end{aligned}$$

$$b^2 = 3 \cdot \left(-\frac{1}{2}\right)^2 = 3 \cdot \frac{1}{4} = \frac{3}{4}, \quad b_1 = \frac{\sqrt{3}}{2}, \quad b_2 = \frac{-\sqrt{3}}{2}$$

$$x_1 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i, \quad x_2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$$

$$x_1 \neq 1$$

$$x_1^2 = \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)^2 = \frac{1}{4} - \frac{\sqrt{3}}{2}i - \frac{3}{4} = -\frac{2}{4} - \frac{\sqrt{3}}{2}i = -\frac{1}{2} - \frac{\sqrt{3}}{2}i \neq 1$$

$$x_1^3 = x_1 \cdot x_1^2 = \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right) = 1$$

Ukázali jsme, že x_1 má řád 3.

$$x_2 \neq 1$$

$$x_2^2 = \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)^2 = \left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)^2 = \frac{1}{4} + \frac{\sqrt{3}}{2}i - \frac{3}{4} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i \neq 1$$

$$x_2^3 = x_2 \cdot x_2^2 = \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right) \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = 1$$

Ukázali jsme, že x_2 má řád 3.

Závěr: V grupě $\mathbb{C}^\times$ (s operací násobení) existují přesně dva prvky řádu 3, a to

$$-\frac{1}{2} + \frac{\sqrt{3}}{2}i, \quad -\frac{1}{2} - \frac{\sqrt{3}}{2}i$$

5. Nechť G je konečná grupa. Dokažte, že existuje kladné celé číslo k splňující

$$a^k = 1$$

pro všechna $a \in G$.

ŘEŠENÍ. Nechť G má řád n . Je $n \in \mathbb{Z}^+$. Položme $k = n!$. Zvolme libovolně $a \in G$. Víme z přednášky (Tvzení 1.2.7.), že každý prvek grupy G má konečný řád menší nebo rovný číslu n . Má tedy prvek a řád d , přičemž d je celé číslo, $1 \leq d \leq n$. Je

$$k = n! = 1 \cdot 2 \cdots (d-1) \cdot d \cdot (d+1) \cdots n$$

Položme $l = 1 \cdot 2 \cdots (d-1) \cdot (d+1) \cdots n$, tj. $l = \frac{n!}{d}$. Je $l \in \mathbb{Z}$, $dl = k$. Počítejme:

$$a^k = a^{dl} = (a^d)^l = 1^l = 1, \quad a^k = 1$$