Algebra I – úlohy k procvičení – 9.12.2020 – řešení

1. Dokažte, že
$$H = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix};\ n \in \mathbb{Z} \right\}$$
je cyklická podgrupa grupy $GL(2, \mathbb{R})$.

   Řešení. Pro $n \in \mathbb{Z}$ je $\begin{vmatrix} 1 & n \\ 0 & 1 \end{vmatrix} = 1 \neq 0$, takže $H \subseteq GL(2, \mathbb{R})$. Ukážeme, že H je podgrupa grupy $GL(2, \mathbb{R})$. Je třeba ukázat tři věci:

   (a) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in H$:
   To je zřejmé.

   (b) $A \in H \Longrightarrow A^{-1} \in H$:
   Nechť $A \in H$. Chceme: $A^{-1} \in H$.
   Je $A = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ pro nějaké $n \in \mathbb{Z}$. Ukážeme, že $A^{-1} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$. Pak bude jasné, že $A^{-1} \in H$.
$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

   (c) $A, B \in H \Longrightarrow AB \in H$: Nechť $A, B \in H$. Chceme: $AB \in H$.
   Je $A = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & l \\ 0 & 1 \end{pmatrix}$, kde $k, l \in \mathbb{Z}$.
$$AB = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & l \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & l+k \\ 0 & 1 \end{pmatrix} \in H$$
   Nyní ukážeme, že grupa H je cyklická. K tomu postačí ukázat, že $\mathbb{Z} \cong H$ (protože $\mathbb{Z}$ je cyklická grupa). Definujme $\varphi : \mathbb{Z} \longrightarrow H$ takto:
$$\varphi(n) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

(pro $n \in \mathbb{Z}$)
Zřejmě φ je bijekce. Ukážeme ještě, že φ je homomorfismus:
Nechť $k, l \in \mathbb{Z}$. Chceme: $\varphi(k+l) = \varphi(k) \cdot \varphi(l)$.

$$\varphi(k) \cdot \varphi(l) = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & l \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & l+k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & k+l \\ 0 & 1 \end{pmatrix} = \varphi(k+l)$$

2. Nechť G je grupa, $a \in G$. Předpokládejme, že prvek a^{28} má řád 10 a prvek a^{22} má řád 20. Určete řád prvku a.

   Řešení. Řád prvku a označme d.

   $$(a^{28})^{10} = 1,\ a^{280} = 1,\ (a^{22})^{20} = 1,\ a^{440} = 1$$

   Protože $a^{280} = 1$, máme $d|280$. Protože $a^{440} = 1$, máme $d|440$. Z $d|280$ a $d|440$ vyplývá, že $d|NSD(280, 440)$. Je $NSD(280, 440) = 40$, takže $d|40$. Je $40 = 2^3 \cdot 5$, takže $d|2^3 \cdot 5$, $d \in \{1, 2, 4, 8, 5, 10, 20, 40\}$.

   - $d = 1$: $a^1 = 1$, $a = 1$, $a^{28} = 1$, a^{28} má řád 1, spor
   - $d = 2$: $a^2 = 1$, $a^{28} = (a^2)^{14} = 1^{14} = 1$, a^{28} má řád 1, spor
   - $d = 4$: $a^4 = 1$, $a^{28} = (a^4)^7 = 1^7 = 1$, a^{28} má řád 1, spor
   - $d = 8$: $a^8 = 1$, $(a^{28})^2 = a^{56} = (a^8)^7 = 1^7 = 1$, a^{28} má řád nejvýše 2, spor
   - $d = 5$: $a^5 = 1$, $(a^{28})^5 = (a^5)^{28} = 1^{28} = 1$, a^{28} má řád nejvýše 5, spor
   - $d = 10$: $a^{10} = 1$, $(a^{22})^{10} = (a^{10})^{22} = 1^{22} = 1$, a^{22} má řád nejvýše 10, spor
   - $d = 20$: $a^{20} = 1$, $(a^{22})^{10} = a^{220} = (a^{20})^{11} = 1^{11} = 1$, a^{22} má řád nejvýše 10, spor

   Závěr: $d = 40$, tj. prvek a má řád 40.

3. Nechť G je grupa, $a, b \in G$. Jestliže řády prvků a, b jsou nesoudělné, pak $\langle a \rangle \cap \langle b \rangle = \{1\}$. Dokažte.

   Řešení. Nechť k je řád prvku a, l je řád prvku b; $k, l \in \mathbb{Z}^+$.

   Předpokládejme, že $k \perp l$. Chceme: $\langle a \rangle \cap \langle b \rangle = \{1\}$.

   - $\{1\} \subseteq \langle a \rangle \cap \langle b \rangle$: To je zřejmé.
   - $\langle a \rangle \cap \langle b \rangle \subseteq \{1\}$: Buď $x \in \langle a \rangle \cap \langle b \rangle$. Chceme: $x = 1$.
     Grupa $\langle a \rangle$ má řád k. Z toho plyne, že $x^k = 1$.
     Grupa $\langle b \rangle$ má řád l. Z toho plyne, že $x^l = 1$.
     Řád prvku x označme d. Je $d \in \mathbb{Z}^+$.

Protože $x^k = 1$, máme $d|k$.
Protože $x^l = 1$, máme $d|l$.
Jelikož $k \perp l$, je $d = 1$.
Tudíž $x^1 = 1$, $x^1 = x$, $x = 1$.

4. Dokažte, že žádná grupa nemůže mít přesně dva prvky řádu 2.

Řešení. Sporem. Nechť G je grupa, která má přesně dva prvky řádu 2. Tyto prvky označme a, b. Jsou dvě možnosti:

(a) $ab = ba$:

$$(ab)^2 = abab = aabb = a^2b^2 = 1 \cdot 1 = 1,\ (ab)^2 = 1$$

Tedy ab má řád 1 nebo 2.

- ab má řád 1:

$$\begin{aligned} ab &= 1 \\ aab &= a \cdot 1 \\ a^2b &= a \\ 1 \cdot b &= a \\ b &= a \end{aligned}$$

  Spor.
- ab má řád 2:
  Pak $ab = a$ nebo $ab = b$.
  Jestliže $ab = a$, pak $b = 1$, spor (b má řád 2).
  Jestliže $ab = b$, pak $a = 1$, spor (a má řád 2).

(b) $ab \neq ba$:

$$(aba)^2 = abaaba = aba^2ba = ab{\cdot}1{\cdot}ba = abba = ab^2a = a{\cdot}1{\cdot}a = aa = a^2 = 1,\ (aba)^2 = 1$$

Tedy aba má řád 1 nebo 2.

- aba má řád 1:

$$\begin{aligned} aba &= 1 \\ aaba &= a \cdot 1 \\ a^2ba &= a \\ 1 \cdot ba &= a \\ ba &= a \\ b &= 1 \end{aligned}$$

Spor.

- aba má řád 2:
  Pak $aba = a$ nebo $aba = b$. Uvidíme, že oba případy dávají spor.
  Nechť $aba = a$. Pak

$$\begin{aligned} aba &= a \\ ab &= 1 \\ abb &= 1 \cdot b \\ ab^2 &= b \\ a \cdot 1 &= b \\ a &= b \end{aligned}$$

  Spor.
  Nechť $aba = b$. Pak

$$\begin{aligned} aba &= b \\ abaa &= ba \\ aba^2 &= ba \\ ab \cdot 1 &= ba \\ ab &= ba \end{aligned}$$

  Spor.

5. Uveďte příklad grupy, která není cyklická, a přitom všechny její vlastní podgrupy jsou cyklické.

Poznámka: Podgrupa H grupy G se nazývá vlastní, pokud $H \neq G$.

Řešení. $\mathbb{Z}_2 \times \mathbb{Z}_2$