Příklad:

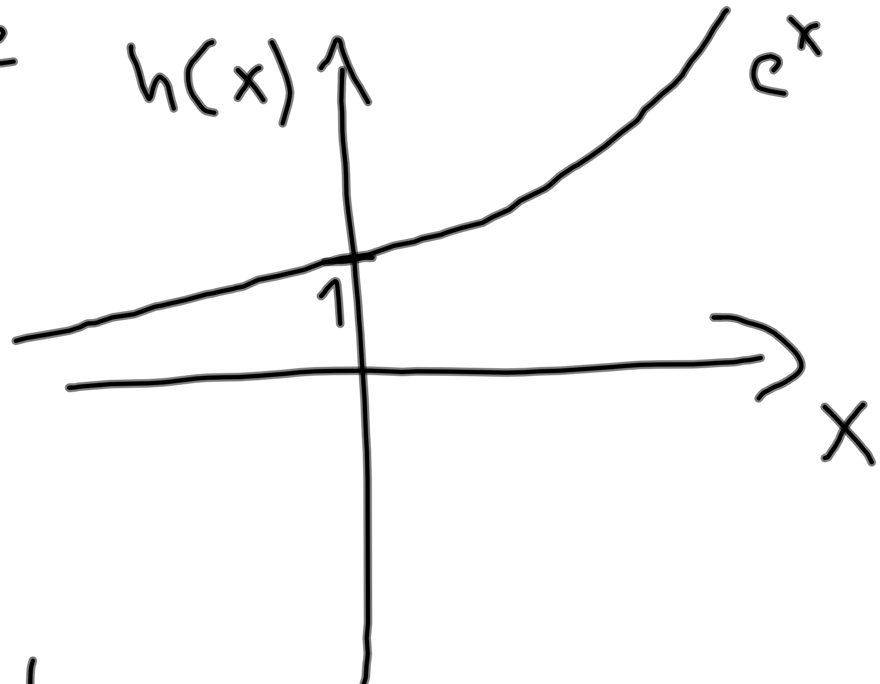
$$h : (\mathbb{R}, +, 0, -) \to (\underbrace{\cancel{\mathbb{R}}}_{}^{\mathbb{R}\setminus\{0\}}, \cdot, 1, {}^{-1}),$$

$$[h(x) = a^x \quad \forall x \in \mathbb{R}^+]$$

Řešení $\quad x \longmapsto a^x \quad \forall x \in \mathbb{R}, \forall a \in \mathbb{R}^+, a \neq 1$

1. $(\mathbb{R}, +, 0, -)$ je grupa (kom.)
2. $(\mathbb{R}\setminus\{0\}, \cdot, 1, {}^{-1})$ je grupa (kom.)

$a = e$



$\forall\, x, y \in \mathbb{R}:$

$L = h(x+y) = a^{x+y}$

$P = h(x) \cdot h(y) = a^x \cdot a^y = a^{x+y}$

$\Rightarrow L = P \Rightarrow h$ je hom. pologrup

$$h(0) = a^0 = 1$$

$$L = h(-x) = a^{-x}$$

$$P = \left(h(x)\right)^{-1} = \frac{1}{h(x)} = \frac{1}{a^x} = a^{-x}$$

$\Rightarrow L = P$

$\Rightarrow h$ je hom. grup

$$h: \mathbb{R} \to \mathbb{R} \setminus \{0\}, \; x \mapsto a^x$$

$$a \in \mathbb{R}^+, \; a \neq 1$$

injektivita:

$$\forall x_1, x_2 \in \mathbb{R}: \; h(x_1) = h(x_2) \Rightarrow$$

$$\log_a / \quad a^{x_1} = a^{x_2} \Rightarrow \log_a a^{x_1} = \log_a a^{x_2}$$

$$\Rightarrow x_1 \cdot \underbrace{\log_a a}_{1} = x_2 \cdot \underbrace{\log_a a}_{1} \Rightarrow x_1 = x_2$$

$\Rightarrow h$ je injektivní

Surjektivita:

? $\forall y \in \mathbb{R} \setminus \{0\} \ \exists x \in \mathbb{R}$ takže

$h(x) = y$.

$h(x) = y \qquad \forall y \in \mathbb{R} \setminus \{0\}$

$\log_a / \ a^x = y$

$\log_a a^x = \log_a y \qquad \forall y \in \mathbb{R}^+$

$x \cdot \log_a a = \log_a y$

$x = \log_a y \qquad \Rightarrow h$ není sur.

Pozn.: Pro nahrazení

$\mathbb{R} \setminus \{0\}$ mn. $\mathbb{R}^+$

je zobrazení h surjektivní

$h : \mathbb{R} \to \mathbb{R}^+, \; x \mapsto a^x$

$a \in \mathbb{R}^+, \; a \neq 1$

Príklad: Dokážte, že $(S, \cdot, 1)$ je podmonoidom k $(\mathbb{Z} - \{0\}, \cdot, 1)$. S je mn. lichých čísel.

Řešení: $(\mathbb{Z} \setminus \{0\}, \cdot, 1)$ je monoid

1. $S \subset \mathbb{Z} \setminus \{0\}$ ✓

$S = \{ z \in \mathbb{Z} / z = 2k+1, k \in \mathbb{Z} \}$

Pozn: $A \subset B \iff \forall a \in A$ platí, že $a \in B$

$a \in A \Rightarrow a \in B \quad \forall a \in A$

$$\frac{s \in S}{2 \in \mathbb{Z} \wedge 1 \in \mathbb{Z}} \Rightarrow s = 2k+1, k \in \mathbb{Z}, \wedge$$

a navíc je $+$ a $\cdot$ bin. op na $\mathbb{Z}$ $\Rightarrow$

$(s=)\ 2k+1 \in \mathbb{Z}$

zbývá ukázať, že $2k+1 \neq 0$

Důkaz sporem: předp., že $\exists\, k \in \mathbb{Z}$, takové, že $2k+1=0$.

$$2k=-1$$
$$k=-\frac{1}{2} \quad \text{avšak} \quad -\frac{1}{2} \notin \mathbb{Z}$$
$$\Rightarrow \text{spor} \Rightarrow 2k+1 \neq 0 \quad \forall k \in \mathbb{Z}$$
$$\Rightarrow s \in \mathbb{Z} \setminus \{0\} \quad \forall s \in S$$
$$\Rightarrow S \subset \mathbb{Z} \setminus \{0\}$$

2. je $\cdot$ bin. op. na S?

$\forall\ s_1, s_2 \in S$

$\underline{s_1 \cdot s_2} = \underbrace{(2k_1+1)}_{s_1} \cdot (2k_2+1)$

$= 4k_1k_2 + 2k_1 + 2k_2 + 1 =$

$= 2 \cdot \underbrace{(2k_1k_2 + k_1 + k_2)}_{\in \mathbb{Z} \ = \bar{k}} + 1$

$= 2 \cdot \bar{k} + 1 \Rightarrow s_1 \cdot s_2 \in S \Rightarrow \cdot$ je bin. op. na S

3. $1 \overset{?}{\in} S$

$\forall s \in S: \; s = 2k+1, \; k \in \mathbb{Z}$

ovšem pro $k=0$ je $s=1$

$\Rightarrow 1 \in S$

$\Rightarrow (S, \cdot, 1)$ je podm. monoidu

$(\mathbb{Z} \setminus \{0\}, \cdot, 1)$

$\square$

Title: 11. 23-10:57 dop. (10 of 12)

Permutace.

Tvrzení: Buďte p, q permutace na I_n. Pak $\exists$ celé číslo k takové, že platí

$$\mathrm{inv}(p \circ q) = \mathrm{inv}\, q + \mathrm{inv}\, p + 2k$$

Definice: $\mathrm{sgn}: S_n \to \{-1, 1\}$, $p \mapsto (-1)^{\mathrm{inv}\, p}$.

$$\underline{\mathrm{sgn}(p\circ q)} = (-1)^{\mathrm{inv}(p\circ q)} =$$

$$= (-1)^{\mathrm{inv}\,p + \mathrm{inv}\,q + 2k} =$$

$$= \underbrace{(-1)^{\mathrm{inv}\,p}}_{= \mathrm{sgn}\,p} \cdot \underbrace{(-1)^{\mathrm{inv}\,q}}_{\mathrm{sgn}\,q} \cdot \underbrace{(-1)^{2k}}_{= 1}$$

$$= \underline{\mathrm{sgn}\,p \cdot \mathrm{sgn}\,q}$$

$$\mathrm{sgn}: (S_n, \circ, \mathrm{id}, {}^{-1}) \to (\{-1, 1\}, \cdot, 1, {}^{-1})$$

$$p \mapsto (-1)^{\mathrm{inv}\,p}$$