Příklad 1. *Rozhodněte o uvedených množinách a operacích, jakou tvoří strukturu (grupoid, pologrupa, monoid, grupa), příp. diskutujte existenci jednostranných neutrálních prvků.*

1. $(2^{\mathbb{N}}, \cup)$, $(2^{\mathbb{N}}, \cap)$, $(2^{\mathbb{N}}, \setminus)$, $2^{\mathbb{N}}$ *s operací symetrický rozdíl*
2. $\mathbb{N}$ *s operací největší společný dělitel (resp. nejmenší spol. násobek)*
3. *regulární matice* 2×2 *nad* $\mathbb{R}$ *s operací sčítání*
4. *matice* 2×2 *nad* $\mathbb{R}$ *s operací sčítání*
5. *matice* 2×2 *nad* $\mathbb{R}$ *s operací odčítání*
6. *invertibilní matice* 2×2 *nad* $\mathbb{Z}_2$ *s operací násobení matic (zde navíc určete tzv. Cayleyho tabulku násobení)*
7. $(\mathbb{Z}_9, +)$, *resp.* $(\mathbb{Z}_5, +)$, $(\mathbb{Z}_9, \cdot)$, *resp.* $(\mathbb{Z}_5, \cdot)$, $(\mathbb{Z}_9 \setminus \{[0]_9\}, \cdot)$, *resp.* $(\mathbb{Z}_5 \setminus \{[0]_5\}, \cdot)$.
8. $\mathbb{Z}$ *s operací* $\circ$ *zadanou (pomocí běžných operací sčítání a násobení) předpisem* $x \circ y = x + (-1)^x y$.

1a) $(2^{\mathbb{N}}, \cup)$

$A \in 2^{\mathbb{N}} \iff A \subseteq \mathbb{N}$ (komutativní) grupoid

$A, B \subseteq \mathbb{N} \overset{?}{\Longrightarrow} A \cup B \subseteq \mathbb{N}$ ✓

$A, B, C \subseteq \mathbb{N} \overset{?}{\Longrightarrow} (A \cup B) \cup C \overset{?}{=} A \cup (B \cup C)$ ✓

pologrupa

$\exists E \subseteq \mathbb{N}$ takže $\forall A \subseteq \mathbb{N}: A \cup E = A$

$E \cup A = A$

ANO, $E = \emptyset$ je neutrální prvek

$\Rightarrow$ monoid

pro $A \subseteq \mathbb{N}$ lib. ex. A^{-1} takže $A \cup A^{-1} = E = \emptyset$!

NE, nejedná se proto o grupu

1b) $(2^{\mathbb{N}}, \cap)$

jedná se o komutativní pologrupy

- neutrální prvek: $\forall A \subseteq \mathbb{N}: \; A \cap E = A$

ANO, $E = \mathbb{N}$ je neutrální

- inverzní prvky: $\forall A \subseteq \mathbb{N} \; \exists A^{-1} \subseteq \mathbb{N}:$

$$A \cap A^{-1} = E = \mathbb{N}$$

$(2^{\mathbb{N}}, \cap)$ je komutativní monoid

1c) $(2^{\mathbb{N}}, \setminus)$

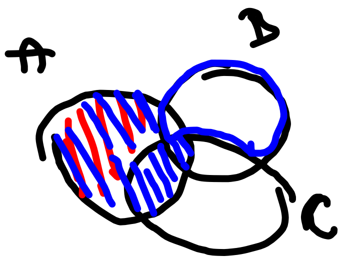
grupoid? $A, B \subseteq \mathbb{N} \overset{?}{\Longrightarrow} A \setminus B \subseteq \mathbb{N}$ ✓

$2^{\mathbb{N}} = \mathcal{P}(\mathbb{N})$

nekomutativní

pologrupa? $A, B, C \subseteq \mathbb{N} \overset{?}{\Longrightarrow} \underline{(A \setminus B) \setminus C} =$

$= \underline{A \setminus (B \setminus C)}$



$A = B = C = \{1\}$

$L = \emptyset, \quad P = \{1\}$

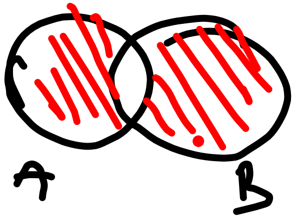
není asociativní

pravý neutrální prvek je $\emptyset$

levý neutrální neexistuje $(E \setminus A = A \quad \forall A \subseteq \mathbb{N})$

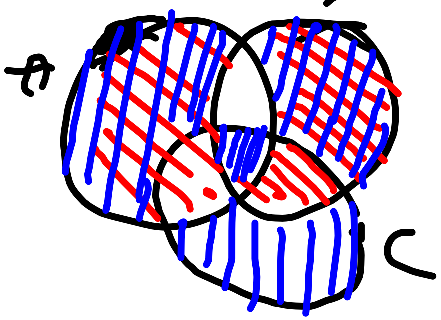
1d) $(2^{|\mathbb{N}|}, \div)$

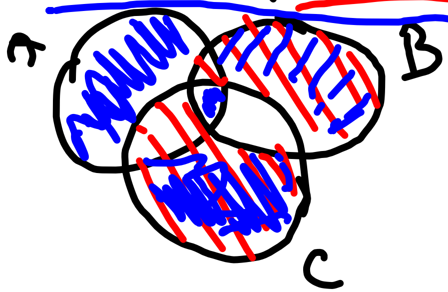
$$A \div B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$$



(komutativní)

- grupoid ✓
- pologrupa? $(A \div B) \div C = A \div (B \div C)$ ✓





- neutrální prvek? $A \div E = A$

  $E = \emptyset$
- inverzní prvky? pro lib. $A \subseteq \mathbb{N}\ \exists A^{-1}: A \div A^{-1} = E = \emptyset$

  $A \div A = \emptyset$

$\Rightarrow$ komutativní grupa

2) a) $\mathbb{N}$ s operací gcd

grupoid, komutativní, asociativní

$(a,(b,c)) = ((a,b),c) = (a,b,c)$

neutrální $\exists$ $(e,a) = (a,e) = a$

(splňuje $e=0$, ale z def. $0 \notin \mathbb{N}$)

není monoid

Pozn. ani v $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ s operací gcd

neexistují inverze

b) lcm (nejm. spol. násobek)

$[e,a] = a$ pro $e=1$ $\Rightarrow$ kom. monoid

neexistují inverze

3) reg. matice 2×2 nad $\mathbb{R}$, sčítání matic

nejde o grupoid !

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ není reg.}$$

4) matice 2×2 nad $\mathbb{R}$, sčítání matic

grupoid, komutativní, asociativní

neutrální prvek $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

opačný prvek k A je $-A$

$\Rightarrow$ kom. grupa

POZN: reg. matice 2×2 nad $\mathbb{R}$, násobení matic tvoří nekomutativní grupu

5) matice 2×2 nad $\mathbb{R}$ s odčítáním

je grupoid, ale není asociativní

$$A - (B - C) \overset{?}{=} (A - B) - C$$

$$B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = A$$

$$L = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \quad P = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

levý neutrální neex., pravý neutrální je $O = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

6) reg. matice 2×2 nad $\mathbb{Z}_2$, s násobením

invertibilní

$$A=\begin{pmatrix}1&1\\1&0\end{pmatrix},\quad B=\begin{pmatrix}1&1\\0&1\end{pmatrix},\quad C=\begin{pmatrix}1&0\\1&1\end{pmatrix},\quad D=\begin{pmatrix}0&1\\1&1\end{pmatrix},$$

$$E=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad \begin{pmatrix}0&1\\1&0\end{pmatrix}=F \dots$$ všechny invertibilní matice nad $\mathbb{Z}_2$

grupoid (nekomutativní), asociativní, monoid,

grupa

řád		E	F	A	B	C	D
1	E	E	F	A	B	C	D
2	F	F	E	C	D	A	B
3	A	A	B	D	C	F	E
2	B	B	A	F	E	D	C
2	C	C	D	B	A	E	F
3	D	D	C	E	F	B	A

$$F\cdot F = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\cdot\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E$$

$$F\cdot A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\cdot\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = C$$

$$A\cdot F = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\cdot\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = B$$

$$F\cdot B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = D$$

$$F\cdot C = F\,(F\cdot A) = (F\cdot F)\cdot A = E\cdot A = A$$

$$F\cdot D = F\cdot(F\cdot B) = (F\cdot F)\cdot B = E\cdot B = B$$

$$B\cdot F = (A\cdot F)\cdot F = A\cdot E = A$$

$$C\cdot F = F\cdot A\cdot F = F\cdot B = D$$

$$A\cdot A = F(C\cdot F)\cdot C = FDC = B\cdot C$$

$$A\cdot A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\cdot\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = D$$

$$A \cdot B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = C$$

$$AC = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = F$$

$$BA = BFC = A \cdot C = F$$

$$B \cdot B = AFAF = ACF = A \cdot D = E$$

7) $(\mathbb{Z}_9, +)$, $(\mathbb{Z}_5, +)$

$\mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$

$[a]_5 = \{k \in \mathbb{Z};\ k \equiv a\,(5),$ tj. $5 \mid k-a\}$.

$[1232]_5 = [2]_5$ (neboť $1232 \equiv 2\,(5)$)

komut. grupoid, asociativní, neutr. prvek $[0]_5$

opačný k $[a]_m$ je $[-a]_m = [m-a]_m$

$\Rightarrow$ kom. grupa

$(\mathbb{Z}_m, \cdot)$ pro $m = 5, 9$

kom. pologrupa, jednotkovým prvkem je $[1]_m$,

k $[0]_m$ neex. inverzní $\Rightarrow$ nejde o grupu!

$(\mathbb{Z}_5 \setminus \{[0]_5\}, \cdot)$

$(\mathbb{Z}_5^*, \cdot)$ je grupoid, protože

$5 \nmid a \wedge 5 \nmid b \Rightarrow 5 \nmid a \cdot b$

(obměna: $5 \mid a \cdot b \Rightarrow 5 \mid a \vee 5 \mid b$)

inverze – pro lib. $[a]_5 \in \mathbb{Z}_5^*$ ex.

$[b]_5$ tak, že $[a]_5 \cdot [b]_5 = [a \cdot b]_5 = [1]_5$

a	1	2	3	4
a^{-1}	1	3	2	4

$(\mathbb{Z}_9 \setminus \{[0]\}, \cdot)$ není grupoid

$[3]_9 \cdot [3]_9 = [0]_9 \notin \mathbb{Z}_9^*$

8) $(\mathbb{Z}, \circ)$

$$x \circ y = x + (-1)^x \cdot y$$

je to grupoid, $x \circ y \in \mathbb{Z}$

$$\left.\begin{array}{l} 1 \circ 3 = 1 + (-1)^1 \cdot 3 = 1 - 3 = -2 \\ 3 \circ 1 = 3 + (-1)^3 \cdot 1 = 3 - 1 = 2 \end{array}\right\} \text{není kom.}$$

asociativita ?

$$(x \circ y) \circ z = (x + (-1)^x \cdot y) \circ z = \cancel{x + (-1)^x \cdot y} + (-1)^{x + (-1)^x \cdot y} \cdot z$$

$\overset{?}{=}$ ||

$$x \circ (y \circ z) = x \circ (y + (-1)^y \cdot z) = \cancel{x + (-1)^x (y + (-1)^y \cdot z)}$$

$$(-1)^{x + (-1)^x \cdot y} \cdot \cancel{z} = (-1)^x \cdot (-1)^y \cdot \cancel{z} \Leftrightarrow \cancel{x} + (-1)^x \cdot y \equiv \cancel{x} + y \pmod 2$$

je to asociativní! ✓

neutr. prvek?

$$x = x \circ e = e \circ x$$

$$x = x + (-1)^x \cdot e \qquad x = e + (-1)^e \cdot x$$

$e = 0$ vyhovuje

inverzní prvek?

$x \in \mathbb{Z}$ libovolné!

ANO ex. $\forall x \in \mathbb{Z}$

$$y = x^{-1} = \begin{cases} x & \text{pro } 2 \nmid x \\ -x & \text{pro } 2 \mid x \end{cases}$$

$$x \circ y = y \circ x = 0$$

$$x + (-1)^x \cdot y = 0 \qquad y + (-1)^y \cdot x = 0$$

$2 \mid x \Rightarrow y = -x \longrightarrow y + x = 0$ ✓

$2 \nmid x \Rightarrow y = x \longrightarrow y - x = 0$ ✓