101. (i) $(2^{N}, \cup)$

$\emptyset$ neutralni prvek: $\emptyset \cup A = A \cup \emptyset = A$

$\cup$ asociativní:

$(A \cup B) \cup C = A \cup (B \cup C)$

komutativní monoid

prvek $\{1\}$ nemá inverzní

(ii) $(\mathbb{N}, (\,,\,))$ $\quad (a, b)$ NSD

- asociativní

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

- komutativní

- n neutr. prvek

$\rightsquigarrow (n, a) = a \quad \forall a \in \mathbb{N}$

$\Rightarrow a \mid n \quad \forall a \in \mathbb{N}$

↳ neexistuje

pologrupa

(iii) $(\mathbb{N}, [\,,\,])$ $[a,b]$ NSN

- komutativní, asoc.
- neutrální prvek 1
  $[a,1] = [1,a] = a$
- $a = 3$ nemá inverzi

monoid

(iv) $(\{A \in Mat_{2,2}(\mathbb{R}) \mid A \text{ invertibilní}\}, +)$

A invert.
$-A$ invert.

$A + (-A) \notin$

není ani grupoid

(v) $(\{A \in Mat_{2,2}(\mathbb{R}) \mid A \text{ invertib}\}, \cdot)$

násobení matic

• uzavřené na násobení matic: $(AB)^{-1} = B^{-1} \cdot A^{-1}$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \downarrow \qquad \downarrow$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ inv. $\quad$ inv

• neutr. prvek $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

• inverse existují

• komutativní není

asociativní je

nekomutativní grupa

(vi) $(Mat_{2,2}(\mathbb{R}), -)$

↳ odčítání

• uzavřenost matic

• $A - B = -(B - A)$

není komutativní

• $A - (B - C) \neq (A - B) - C$

není asociativní

- $A - \begin{pmatrix}0&0\\0&0\end{pmatrix} = A$

  ↳ neutrální prvek zprava

- neutrální prvek <u>zleva</u> označme B,

$$B - A = A \qquad \forall A \in Mat_{2,2}(\mathbb{R})$$

$$B = 2A \qquad \forall A$$

↳ neexistuje

$\Rightarrow$ neutr. prvek zleva $\nexists$

grupoid

(vii) $(\{A \in Mat_{2,2}(\mathbb{Z}_2) \mid A \text{ inv.}\}, \cdot)$

nekomutativní grupa

$$\begin{pmatrix}1&1\\0&1\end{pmatrix} \cdot \begin{pmatrix}1&0\\1&1\end{pmatrix} = \begin{pmatrix}0&1\\1&1\end{pmatrix} \quad \neg \text{ vážně}$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \notin$$

(viii) $(\mathbb{Z}_6, \cdot)$

↳ násobení modulo 6

- $a \cdot b = b \cdot a$ kom.

  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ asoc.
- neutrální prvek $1 \in \mathbb{Z}_6$
- inverzní prvky?

  $1^{-1} = 1$

  2^{-1} neexistuje

  $a \in \mathbb{Z}_6$ má inverzi $b \in \mathbb{Z}_6$

  $a \cdot b \equiv 1 \mod 6$

$+ \cdot ? \cdot$ neutr.

+ podm. $\Rightarrow$ a liché, b liché

Obecněji: a má inverzi

mod $\mathbb{Z}_n \iff (a,n)=1$

V $\mathbb{Z}_6$ má inverzi pouze ± 1.

komutativní monoid

(ix) $(\mathbb{Z}_7 \setminus \{0\}, \cdot)$

- kom., asoc., neutrální prvek 1

- invertibilní prvky v $\mathbb{Z}_7$ vzhledem k násobení jsou 1, 2, 3, 4, 5, 6

komutativní grupa

10.2 Na množini

$$M = (\mathbb{R}\setminus\{0\})\times\mathbb{R}$$

definišemo operaciju

$$(x,y)\circ(u,v) = (xu,\ xv+y)$$

- $x \neq 0,\ u \neq 0 \Rightarrow x\cdot u \neq 0$

$$\left.\begin{array}{l}(x,y)\in M\\ (u,v)\in M\end{array}\right\} (x,y)\circ(u,v)\in M$$

M

$\Downarrow$

- asocijativnost

$$((x,y)\circ(u,v))\circ(a,b) =$$

$$(xu,\ xv+y)\circ(a,b) =$$

$$= (xua,\ \underline{xub + xv + y})$$

$$(x,y)\circ((u,v)\circ(a,b)) =$$

$$= (x,y)\circ(ua,\ ub+v) =$$

$$= (xu a,\ \underline{x(ub+v)+y})$$

asociativní

- není komutativní
- $(1,0)$ neutrální prvek

$$(1,0) \circ (u,v) = (u, v+0) = (u,v)$$

$$(x,y) \circ (1,0) = (x, \underbrace{x \cdot 0 + y}_{y}) = (x,y)$$

- inverzní prvky

$$(x,y) \circ \underbrace{(a,b)}_{(x,y)^{-1}} = (1,0)$$

$$(xa,\ xb+y)$$

$$(a,b) \circ (x,y) = (1,0)$$

$$(ax,\ ay+b)$$

$$\boxed{a = \frac{1}{x}}$$

$$\frac{1}{x} \cdot y + b = 0 \qquad xb + y = 0$$

$$b = -\frac{y}{x} \qquad b = -\frac{y}{x}$$

Zá'věr: $(x,y)^{-1} = \left(\frac{1}{x}, -\frac{y}{x}\right)$

nekomutativní grupa

10.3

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 6 & 7 & 8 & 9 & 5 & 4 & 2 \end{pmatrix} \in S_9$$

$$\sigma = (1,3,6,9,2) \circ (4,7,5,8)$$

$$\sigma = (3,1)(6,3)(6,9)(9,2)(4,7)(7,5)(5,8)$$

lichá perm.

10.4

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \dots & 3n-2 & 3n-1 & 3n \\ 2 & 3 & 1 & 5 & 6 & 4 & & 3n-1 & 3n & 3n-2 \end{pmatrix}$$

$$\in S_{3n}$$

počet inverzí: $\underbrace{(1+1)+(1+1)+\dots+(1+1)}_{n}$

$= 2n$ sudý počet

$$\operatorname{sgn}(\sigma_1) = 1$$

$$\sigma_2 = \left(\begin{array}{cccc|cccc} 1 & 2 & 3 \dots & n & n+1 & n+2 & n+3 \dots & 2n \\ 2 & 4 & 6 & 2n & 1 & 3 & 5 & 2n-1 \end{array}\right)$$

počet inverzí:

$$1+2+3+\dots+n = \frac{1}{2}n(n+1)$$

$$\operatorname{sgn}(\sigma_2) = \begin{cases} +1 & n \equiv 0 \mod 4 \\ & n \equiv -1 \mod 4 \\ -1 & n \equiv 1 \mod 4 \\ & n \equiv 2 \mod 4 \end{cases}$$

<u>10.5</u> $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 7 & 1 & 2 & 4 \end{pmatrix} \in S_7$

<u>Řád $\sigma \in S_7$</u>: je nejmenší $n \in \mathbb{N}$ t.ž. $\sigma^n = id = e$

$\sigma = (1,3,5) \circ (2,6) \circ (4,7)$

$(1,3,5)$ má řád 3 v S_7

$(2,6)$ a $(4,7)$ mají řád 2 v S_7

$\Rightarrow \sigma$ má řád 6

<u>Inverze k σ</u>: $(2,6)^{-1} = (2,6)$

$(4,7)^{-1} = (4,7)$

$$(1,3,5)^{-1} = (1,5,3)$$

$$\sigma^{-1} = (1,5,3) \circ (2,6) \circ (4,7)$$

Uniete σ^{2013}:

$$(2,6)^{2013} = \underbrace{(2,6)(2,6) \cdot - (2,6)}_{2013} = (2,6)$$

$$(4,7)^{2013} = (4,7)$$

$$(1,3,5)^{2013} = id$$

$$2013 \equiv 0 \mod 3$$

$$\sigma^{2013} = (2,6) \circ (4,7)$$

Ukoito rie σ mekunutkoje s transpozicu $(2,3) = \tau$

$$\sigma \circ \tau = (1,3,5) \circ (2,6) \circ (4,7) \circ (2,3)$$

$$= (4,7) \circ (2,5,1,3,6)$$

$\tau \circ \sigma = (2,3) \circ (1,3,5) \circ (2,6) \circ (4,7)$

$= (4,7) \circ (6,3,5,1,2)$

10.6: Dokažte, že neexistuje

(i) čtyřprvková

(ii) pětiprvková

nekomut. grupa.

(i) $G = \{e, a, b, c\}$

podgrupa generovaná prvkem a

je $\{a, a^2, a^3, \dots\} \subseteq G$

↳ podgrupa

$\cdot \{a, a^2 = e\}$

$\cdot \{a, a^2, \dots\} = G$
$\phantom{\{a, }\|$
$\phantom{\{a, }e$

$|G| = 4$

1, 2, 4

možné počty prvků v podgrupách

G komutativní

$\{e, a\} \leq G$

$\{e, b\} \leq G$

$\{e, c\} \leq G$

Podgrupy

$a^2 = e = b^2 = c^2$

$(ab)^2 = e$

$abab = e \quad /(\,)b$

$abab = e \quad /a(\,)$

$a^2bab = a \quad /(\,)a$

$\underbrace{}_{e} baba = a^2 = e$

$abab^2 = aba = b \quad /(\,)a$

$aba^2 = ab = ba$

komutují

$ac = ca$

$bc = cb$

(ii) 5.4: Tvrzení:

grupa je cyklická