Opakování:

LA 1 29/10/24

Definice: **Binární operace** na množině T je zobrazení z $T \times T$ do T.

Definice: **Grupa** je dvojice $(G, \square)$, kde G je množina a $\square$ je binární operace na G, splňující následující axiomy:
1. $\forall a,b,c \in G: (a \square b) \square c = a \square (b \square c)$ **asoc.**
2. $\exists\, n \in G\ \forall a \in G: a \square n = n \square a = a$ **neutrální prvek**
3. $\forall a \in G\ \exists\, b \in G: a \square b = b \square a = n$ **inverzní prvek**

Pokud navíc platí:

4. $\forall a,b \in G: a \square b = b \square a$ **komutativita**

je G **Abelova** (komutativní) grupa

Příklad: G ... množina všech **otočení roviny** kolem počátku
$\square$ ... skládání otočení

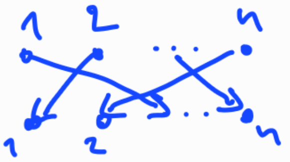
neutrální prvek – otočení o $0°$
inverzní prvek k otočení o $\alpha°$: otočení o $360° - \alpha°$

PERMUTACE

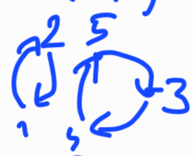
Def: **Permutace** množiny X je vzájemně jednoznačné zobrazení (tzv. bijekce) $\pi: X \to X$

S_n ... množina všech permutací množiny $\{1,2,\dots,n\}$

Reprezentace:
- **dvouřádkový zápis**: $\begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$
- **šipkami**:



- **rozklad na cykly** $(1,2)(3,4,5)$



Skládání permutací: jako u zobrazení: Pro $p, q \in S_n$, $p \circ q$ definujeme předpisem: $p \circ q(i) = p(q(i))\ \forall i$

$(S_n, \circ)$ je grupa.

dk:
- skládání $\circ$ je bin. operace na S_n
- $\circ$ je asociativní
- neutrální prvek – identita
- inverzní prvek k π – inverzní zobrazení

není komutativní – rozmyslet si ■

Def: Dvojice (i, j) je <u>inverze</u> permutace $\pi \in S_n$, pokud $i < j$ & $\pi(i) > \pi(j)$

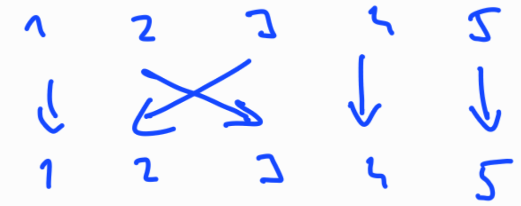
(~ prohození pořadí ~ křížení šipek)

$I(\pi)$ ... množina všech inverzí π

<u>znaménko permutace π</u>: $\mathrm{sgn}(\pi) = (-1)^{|I(\pi)|} = \begin{cases} +1 & \text{sudá} \\ -1 & \text{lichá} \end{cases}$

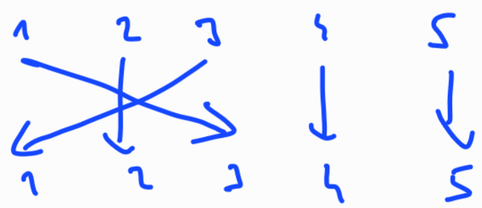
<u>transpozice</u> ... permutace prohazující dva prvky

Př: π:



$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix}$$

π':



tj. jediný cyklus délky 2, jinak délka 1

Definice: Těleso je množina T spolu se dvěmi binárními operacemi $+$ (sčítání) a $\cdot$ (násobení) splňujícími následující podmínky (axiomy):

1. $(T, +)$ je Abelova grupa s neutrálním prvkem 0; inverzní prvek k a značíme $-a$
2. $(T \setminus \{0\}, \cdot)$ je Abelova grupa s neutrálním prvkem 1; inverzní prvek k a značíme a^{-1}
3. $\forall a, b, c \in T : a \cdot (b + c) = a \cdot b + a \cdot c$ (distributivita).

Př. $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ s obvyklými $+$ a $\cdot$ NE tělesa: $\mathbb{N}, \mathbb{Z}$

$T = \{0, 1\}$

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

- ověřte si

nejmenší těleso - vždy musí být aspoň 0 a 1, $0 \neq 1$

Pozn. 1 axiomy - rozhraní

Metavěta: Vše o maticích platí pro libovolné těleso!!! nejen $\mathbb{R}$

Pozn 3 Odvozené binární operace:

$\forall a, b \in T : a - b = a + (-b)$ odčítání

$\forall a \in T, b \in T \setminus \{0\} : a / b = a \cdot b^{-1}$ dělení

Tvrzení 1: 1. Prvky 0 a 1 jsou určeny jednoznačně.

2. $\forall a \in T$, $-a$ určeno jednoznačně, $\forall a \in T \setminus \{0\}$, a^{-1} též.

Důkaz: platí už pro grupy

1. předpokl., že existují nulové prvky 0 a $\bar{0}$. Pak $0 = 0 + \bar{0} = \bar{0}$; obdobně pro $1, \bar{1}$: $1 = 1 \cdot \bar{1} = \bar{1}$.
2. předpokl. dva opačné prvky k a, $-a$, $\overline{-a}$:

$$-a = -a + 0 = -a + (a + \overline{-a}) = \underbrace{(-a + a)}_{=0} + \overline{(-a)} = \overline{-a}$$

pro a^{-1} stejně.

Tvrzení 2: 1. $\forall a \in T: \ 0 \cdot a = a \cdot 0 = 0$ (ani první: není jasná)

2. $\forall a \in T: \ (-1) \cdot a = -a$

3. Pokud $a \cdot b = 0$, pak $a = 0$ nebo $b = 0$.

Důkaz: 1. $0 \cdot a = 0 \cdot a + (0 \cdot a - 0 \cdot a) = (0 \cdot a + 0 \cdot a) - 0 \cdot a =$

$= (0 + 0) \cdot a - 0 \cdot a = 0 \cdot a - 0 \cdot a = 0$

obdobně $a \cdot 0 = 0$

2. $(-1) \cdot a + a = (-1 + 1) \cdot a = 0 \cdot a = 0$,

tj. $(-1) \cdot a$ má vlastnosti $(-a)$; díky jednoznačnosti (Tvrzení 1)

$(-1) \cdot a = -a$.

3. sporem: předp. $a \neq 0$ & $b \neq 0$. Pak $\exists \, a^{-1}, b^{-1}$.

$$\underline{1} = 1 \cdot 1 = (a \cdot a^{-1}) \cdot (b \cdot b^{-1}) \underset{\text{asoc., komut.}}{=} \overbrace{(a \cdot b)}^{=0} \cdot (a^{-1} \cdot b^{-1}) \underset{\text{dle bodu 1}}{=} \underline{0} \text{ spor}$$

∎

Př. $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$

pro $c \in \mathbb{Z}$, $c \bmod n$ značí $d \in \mathbb{Z}_n$ tž. n dělí $c - d$

zavedme: $\forall a, b \in \mathbb{Z}_n$: $a \oplus b = (a + b \bmod n)$

$a \odot b = (a \cdot b \bmod n)$

tzv. hodinová aritmetika: 10 hod. + 3 hod. = 1 hodina pro $n = 12$

Kdy je $(\mathbb{Z}_n, \oplus, \odot)$ těleso?

Věta: $\mathbb{Z}_n$ je těleso $\Leftrightarrow$ n je prvočíslo.

Důkaz: $\Rightarrow$ sporem: předp. $n = a \cdot b$ pro $a, b > 1$

pak $a \odot b = 0$ – spor s Tvrzení 2, bod 3.

$\Leftarrow$ nutno ověřit všechny axiomy

1. $(\mathbb{Z}_n, \oplus)$ grupa – snadné ✓

3. distributivita ✓

2. $(\mathbb{Z}_n \setminus \{0\}, \odot)$ grupa: neutrální prvek 1 ✓

inverzní ?

? $\forall a \in \mathbb{Z}_n \setminus \{0\} \; \exists a^{-1}$ tz. $a \cdot a^{-1} = 1$?

Čísla $1 \odot a, 2 \odot a, \ldots, (n-1) \odot a$ jsou navzájem různá.

dk. sporem: kdyby $c \odot a = d \odot a$ pro $c \neq d$,

tak $0 = c \odot a - d \odot a = (c-d) \odot a$

$\Rightarrow$ dle Tvrzení 2, bod 3 $c - d = 0$ nebo $a = 0$ -

- ani jedno neplatí - spor $\blacksquare$

$\Rightarrow$ máme $n-1$ různých nenulových čísel a $\mathbb{Z}_n$ -

- jedno z nich musí být 1,

tj pro nějaké $b \in \{1, \ldots, n-1\}$ platí $a \odot b = 1$. $\blacksquare$

Pozn. Existenční důkaz - víme, že $\exists a^{-1}$, nevíme, které to je.

Věta (malá Fermatova) Buď n prvočíslo a buď $a \in \mathbb{Z}_n$, $a \neq 0$. Pak $\underbrace{a \odot a \odot \cdots \odot a}_{\text{součin } n-1 \text{ čísel } a} = 1$ $\quad (a^{n-1} = 1 \bmod n)$

Důkaz: podle výše platí:

$$\{1, 2, \ldots, n-1\} = \{1 \odot a, 2 \odot a, \ldots, (n-1) \odot a\}$$

$\Rightarrow$ součin čísel obou množin je stejný:

$$\underbrace{1 \odot 2 \odot \cdots \odot (n-1)}_{=b} = 1 \odot a \odot 2 \odot a \odot \cdots \odot (n-1) \odot a \overset{\text{asoc. komut.}}{=}$$

$$= \underbrace{1 \odot 2 \odot \cdots \odot (n-1)}_{=b} \odot \underbrace{a \odot \cdots \odot a}_{n-1 \text{ krát}}$$

Víme: $\exists b^{-1}$ tz. $b^{-1} \cdot b = 1$

$\Rightarrow 1 = a \odot a \odot \cdots \odot a$. $\blacksquare$

Důsledek: $a^{-1} = a^{n-2}$ inverzní prvek a