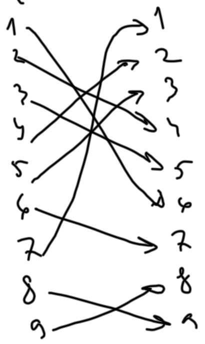
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 5 & 2 & 3 & 7 & 1 & 9 & 8 \end{pmatrix} = (1,6,7)(2,4)(3,5)(8,9)$$



bijekce = injekce + surjekce

$BI = IN + SUR$

Nemá pevný bod

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = (1,2,3)\circ\cancel{(4)}$$

$\Longrightarrow (1,2,3)$

3 2-13:56

$(1,3,5,2) = (1,2)\circ(1,5)\circ(1,3)$

$\|$

$(3,5,2,1)$

$\|$

$(5,2,1,3)$

$\|$

$(2,1,3,5)$

$1 \to 3$

$3 \to 1 \to 5$

$5 \to 1 \to 2$

$2 \to 1$

$(a_1, \dots, a_k) = (a_1,a_k)\circ\dots\circ(a_1,a_3)\circ(a_1,a_2)$

3 2-14:22

$(\mathbb{Z}_2,+)$

$+$	$[0]$	$[1]$
$[0]$	0	1
$[1]$	1	0

$(\{1,-1\},\cdot)$

$\cdot$	1	-1
1	1	-1
-1	-1	1

$0 \mapsto 1$

$1 \mapsto -1$

$(\mathbb{Z}_2\times\mathbb{Z}_2,+) = \{[0,0],[0,1],[1,0],[1,1]\}$

$\not\parallel$

$(\mathbb{Z}_4,+) = \{[0]_4,[1]_4,[2]_4,[3]_4\}$

3 2-14:29

inverze permutace σ:

(i,j), kde $i<j$, $\sigma(i)>\sigma(j)$

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

5 inverzí $((1,2),(1,3),(1,4),(1,5),(1,7))$

3 inverze $((2,4),(2,5),(2,7))$

3 inverze $((3,4),(3,5),(3,7))$

1 $((4,7))$ 1 $((5,7))$ 1 $((6,7))$ 1 $((8,9))$

15 inverzí

lichá perm.

3 2-14:42

Př: f ... viz dříve

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

$$h = f\circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 7 & 3 & 6 & 8 & 1 & 9 & 5 & 2 \end{pmatrix}$$

$= (1,4,6)(2,7,9)\cancel{(3)}(5,8)$

② $f \dots -1$; $g \dots +1$, $h \dots -1$

$h = f\circ g \Rightarrow \operatorname{sgn} h = \operatorname{sgn} f \cdot \operatorname{sgn} g = -1\cdot 1 = -1$

③ $f^{2011} = \underbrace{f\circ f\circ f\circ \dots \circ f}_{2011} = \left((1,6,7)(2,4)(3,5)(8,9)\right)^{2011}$

$= (1,6,7)^{2011}\circ(2,4)^{2011}\circ(3,5)^{2011}\circ(8,9)^{2011} = (1,6,7)(2,4)(3,5)(8,9)$

3 2-14:50

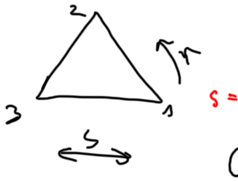
Pozor!,

$(a\cdot b)^2 \neq a^2\cdot b^2$

$\|$ $\qquad\qquad$ $\|$

$a\cdot b\cdot a\cdot b \neq a\cdot a\cdot b\cdot b$

3 2-14:57



$r = (1,2,3)$

$s = O_{|},\ O_{\backslash},\ O_{/}$

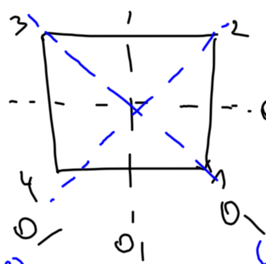
$\quad = (1,3)\quad (2,3)\quad (1,2)$

$D_6 = \{id, r, r^2 = r^{-1}, O_{|}, O_{\backslash}, O_{/}\}$

$= \{id, r, r^2 = r^{-1}, s, r\circ s, s\circ r\}$

$= \langle r, s \mid r^3 = id, s^2 = id, s\circ r = r^{-1}\circ s\rangle$

3 2-15:06



$O_{-} = (1,2)(3,4)$

$O_{/}$ $(1,3)$ $\quad O_{|}$ $(1,4)(2,3)$ $\quad O_{\backslash}$ $(2,4)$

$r = (1,2,3,4),\ \underline{\underline{r^2}},\ r^3,\ r^4 = id$

$(1,3)(2,4)$ $\quad V_4 = \{id, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$

3 2-15:13

Snadno:

"$\Rightarrow$" $a,b\in H \overset{②}{\Rightarrow} b^{-1}\in H \overset{①}{\Rightarrow} a\circ b^{-1}\in H$

"$\Leftarrow$" $a,b\in H \overset{\text{Podm.}}{\Rightarrow} \underbrace{a\circ a^{-1}}_{e_G}\in H \overset{\text{Podm.}}{\Rightarrow} e_G\circ a^{-1}\in H$, tj. ②

$\qquad\qquad\qquad\qquad\qquad\qquad\quad \| \; a^{-1}$

$a,b\in H \overset{②}{\Rightarrow} b^{-1}\in H \overset{\text{Podm.}}{\Rightarrow} a\circ\underbrace{(b^{-1})^{-1}}_{b}\in H$

POZN: $\forall a\in G: (a^{-1})^{-1} = a$

$a\circ a^{-1} = a^{-1}\circ a = e_G \Rightarrow a$ je inverze k a^{-1}

3 2-15:22

Př: $G = (\mathbb{Z}, +)$

$H \subseteq G$ je podgrupa $\Leftrightarrow$

$\Leftrightarrow \forall a,b\in H: a-b\in H$

Př: $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$

$\forall A,B\in SL_n(\mathbb{R})$

$A\cdot B^{-1}\in SL_n(\mathbb{R}) \Leftrightarrow \det(A\cdot B^{-1}) =$

$= \underline{\det A}\cdot\underline{(\det B)}^{-1} = 1\cdot 1 = 1$ ✓

3 2-15:29

POZN: inverze v obecné grupě

$(a\circ b)^{-1} = b^{-1}\circ a^{-1}$, protože

$(a\circ b)\circ(b^{-1}\circ a^{-1}) \overset{\text{asoc.}}{=} a\circ\underbrace{(b\circ b^{-1})}_{e}\circ a^{-1} = e$

$(b^{-1}\circ a^{-1})\circ(a\circ b) = e$

3 2-15:36

$m\mathbb{Z} = \{m\cdot z;\ z\in\mathbb{Z}\}$

$m\in\mathbb{Z}$ $\quad 0\cdot\mathbb{Z} = \{0\}$ $\quad 2\cdot\mathbb{Z} = \{0, 2, -2, \dots\}$

$1\cdot\mathbb{Z} = \mathbb{Z}$

- $m\mathbb{Z}$ je podgrupa, neboť pro $a,b\in m\mathbb{Z}$ $\exists a_1, b_1\in\mathbb{Z}: a = m\cdot a_1, b = m\cdot b_1$; $a-b = m\cdot(a_1-b_1) \in m\mathbb{Z}$

- H podgrupa $(\mathbb{Z},+) \Rightarrow \exists m\in\mathbb{Z}: H = m\cdot\mathbb{Z}$

Položme $m := \min\{h\in H;\ h\in\mathbb{N}\}$ *

$\Rightarrow H = m\cdot\mathbb{Z}$ ($m\mathbb{Z}\subseteq H$ zřejmé; $H\subseteq m\mathbb{Z}$: $h\in H\setminus m\mathbb{Z}$: $h = q\cdot m + z$ $\underline{0<z<m}$ $\Rightarrow z\in H$ SPOR! *

3 2-15:38