Permutace

X - množina

$S(X)$ - permutace na X

S_n - permutace na $\{1, 2, \ldots, n\}$

$$S_3: \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1,3)$$

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

$$S_5: \quad (1,4,3,2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 3 & 5 \end{pmatrix}$$

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

$(S(X), \circ)$ - grupa

$$\left[(1,3,4,5)^{-1} \circ (1,7,3,2) \circ (1,3,7,2)^{-1} \right]^3 =$$

$$= \left[(5,4,3,1) \circ (1,7,3,2) \circ (2,7,3,1) \right]^3 =$$

$$= (2,1,5,4,3,7)^3 =$$

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

$\boxed{\text{MAT 04}}$

2

$$[(1,2,3)\circ(1,4,5)]^3 \neq (1,2,3)^3 \circ (1,4,5)^3$$

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

$$(1,4,5,2,3)^3 \qquad\qquad \underline{id}$$

$$\|$$

$$\underline{\underline{(1,2,4,3,5)}}$$

$$(A\circ B)^2 = A\circ B\circ A\circ B$$

$$A^2\circ B^2 = A\circ A\circ B\circ B$$

$$(1,2,4,5,6,3,7)^{100} =$$

$$= (1,2,4,5,6,3,7)^2 \qquad \text{protože} \quad 100 = 14\cdot 7+2$$

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

$$(1,2,3,5,6) = \overset{1}{(1,6)}\circ\overset{2}{(1,5)}\circ\overset{3}{(1,3)}\circ\overset{4}{(1,2)} \quad - \underline{\text{sudá}}$$

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

$$\underline{\text{lichá}}$$

$$\underline{\text{transpozice}}$$

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

$(\mathbb{Z}_n, \cdot)$ není grupa

$(\mathbb{Z}_n \setminus \{0\}, \cdot)$ grupa $\Leftrightarrow$ n - prvočíslo

$\mathbb{Z}_n^*$ -- množina invertibilních prvků ze $\mathbb{Z}_n$

$(\mathbb{Z}_n^*, \cdot)$ grupa

Př: 4^{-1} v $(\mathbb{Z}_{15}, \cdot)$

hledáme x t.ž. $4 \cdot x = 15q + 1$, tj. $x = 4^{-1}$

Euklidův alg.

$$15 = 3 \cdot 4 + 3$$
$$4 = 1 \cdot 3 + 1$$

$$1 = 4 - 1 \cdot 3 = 4 - 1 \cdot (15 - 3 \cdot 4) =$$
$$= 4 - 15 + 3 \cdot 4 =$$
$$= 4 \cdot 4 - 15$$

$$\underset{x}{4} \cdot 4 = 15 + 1$$

$\boxed{15 = 0 \mod 15}$!

$x = 4$

Př

MAT 04

5

17^{-1} v $\mathbb{Z}_{181}$

$$181 = 10 \cdot 17 + 11$$
$$17 = 1 \cdot 11 + 6$$
$$11 = 1 \cdot 6 + 5$$
$$6 = 1 \cdot 5 + 1$$

$$1 = 6 - 1 \cdot 5$$
$$= 6 - 1 \cdot (11 - 1 \cdot 6) =$$
$$= 6 - 11 + 6 =$$
$$= 2 \cdot 6 - 11 =$$
$$= 2 \cdot (17 - 11) - 11 =$$
$$= 2 \cdot 17 - 3 \cdot 11 =$$
$$= 2 \cdot 17 - 3 \cdot (181 - 10 \cdot 17) =$$
$$= 2 \cdot 17 - 3 \cdot 181 + 30 \cdot 17 =$$
$$= -3 \cdot 181 + 32 \cdot 17$$

$$\boxed{17^{-1} = 32}$$

Pr

MAT 04

$(\mathbb{Z}_{10},+)$ Najděte všechny podgrupy

$\langle 0\rangle = \{0\}$

$\langle 1\rangle = \mathbb{Z}_{10}$

$\langle 2\rangle = \{0,2,4,6,8\}$

$\langle 3\rangle = \{0,3,6,9,2,5,8,1,4,7\} = \mathbb{Z}_{10}$

$\langle 4\rangle = \{0,4,8,2,6\}$

$\langle 5\rangle = \{0,5\} = 5\cdot\mathbb{Z}_{10}$

$\langle 6\rangle = \{0,6,2,8,4\} = 2\cdot\mathbb{Z}_{10}$

$A \subseteq \mathbb{Z}_{10}$ podgrupa, pak $|A| \mid |\mathbb{Z}_{10}| \Rightarrow |A| = 1, 2, 5, 10.$

$$\begin{tikzcd}
 & \mathbb{Z}_{10} \arrow[dl, no head] \arrow[dr, no head] & \\
2\cdot\mathbb{Z}_{10} \arrow[dr, no head] & & 5\cdot\mathbb{Z}_{10} \arrow[dl, no head] \\
 & \{0\} &
\end{tikzcd}$$

Normální podgrupy

$H \subseteq G$ podgrupa

$aH = \{ah \mid h \in H\}$

$a \in G$

$aH = bH \Leftrightarrow a \in bH \Leftrightarrow a^{-1}b \in H$

$H \lhd G$ (normální podgrupa)

$\forall a \in G, h \in H.\ a^{-1}ha \in H \Leftrightarrow aH = Ha \quad \forall a \in G$

Př

$$G = \left(\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{Q}) \right\}, \cdot \right)$$

$$H = \left(\left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{Q}) \right\}, \cdot \right)$$

$\hookrightarrow$ regulární matice řádu 2 nad $\mathbb{Q}$

---

1) $H \lhd G$:

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} \frac{1}{a} & -\frac{b}{a} \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b+x \\ 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & \frac{b+x}{a} - \frac{b}{a} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \frac{x}{a} \\ 0 & 1 \end{pmatrix} \in H \quad \checkmark$$

MAT 04

7

$$G/H = \{ gH \mid g \in G \}$$

2) $G/H \cong (\mathbb{Q}^*, \cdot)$

$$\varphi : \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \cdot H \longmapsto a$$

i) korektnost zobrazení, $g_1 H = g_2 H \Rightarrow$

$\Rightarrow \varphi(g_1 H) = \varphi(g_2 H)$:

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} H = \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} H \Leftrightarrow$$

$$\Leftrightarrow \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \in H \Leftrightarrow$$

$$\Leftrightarrow \begin{pmatrix} \frac{1}{a} & -\frac{b}{a} \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \in H \Leftrightarrow \begin{pmatrix} \frac{c}{a} & \frac{d-b}{a} \\ 0 & 1 \end{pmatrix} \in H \Leftrightarrow$$

$$\Leftrightarrow \frac{c}{a} = 1 \Leftrightarrow \underline{\underline{c = a}}, \text{ tj.}$$

$$\varphi\left(\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} H\right) = a$$

$$\varphi\left(\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} H\right) = \underline{\underline{c = a}}$$

✓

ii) φ injekce:

$$\varphi\left(\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} H\right) = \varphi\left(\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} H\right)$$

$$\underset{a}{\shortparallel} \qquad\qquad \underset{c}{\shortparallel}$$

$$a = c \iff \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} H = \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} H \quad \text{viz } 7$$

iii) φ surjekce:

$a \in \mathbb{Q}^*$, pak $\varphi\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} H\right) = a$ ✓

iv) homomorfismus:

$$\varphi\left(\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} H \cdot \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} H\right) = \varphi\left(\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} H\right) =$$

$$= \varphi\left(\begin{pmatrix} ac & ad+b \\ 0 & 1 \end{pmatrix} H\right) = \underline{ac}$$

$$\varphi\left(\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} H\right) \cdot \varphi\left(\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} H\right) =$$

$$a \cdot c = \underline{ac}$$ ✓

φ je izomorfismus G/H a $(\mathbb{Q}^*, \cdot)$.