Tvrzení: Buď $P$ pole. Pak $\forall a \in P$ platí:

(1) $a.0 = 0$

(2) $a.(-1) = -a$

(3) $a.(b-c) = a.b - a.c$

Důkaz:

III) $a + 0 = a$

(1) $a.0 \overset{III}{=} a.(0+0) =$

$\overset{IX}{=} a.0 + a.0$

$a.0 = a.0 + a.0\quad / -(a.0)$

$a.0 + [-(a.0)] = a.0 + [a.0 + [-(a.0)]]$

$\overset{IV}{0} = a.0 + \underset{0}{[a.0 + [-(a.0)]]}$

III $0 = a \cdot 0$

(2) $a \cdot 0 \overset{IV}{=} a \cdot (1 + (-1)) =$

$\overset{IX}{=} a \cdot 1 + a \cdot (-1)$

$a \cdot 0 = a \cdot 1 + a \cdot (-1)$

$0 \overset{VIII}{=}$ (since $a \cdot 0 = 0$)

$0 = a + a \cdot (-1) \;/ + (-a)$

$0 + (-a) = (a + a \cdot (-1)) + (-a)$

$0 \overset{III}{=} (a + a \cdot (-1)) + (-a)$

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

$-a \overset{I}{=} a + (-a) + a \cdot (-1)$

$-a = 0 + a \cdot (-1) \overset{IV}{=} a \cdot (-1) \overset{III}{=} a \cdot (-1)$

Tvrzení: Buď $P$ pole. Nechť prvky $a, b \in P$ splňují rovnost:

$a \cdot b = 0 \Rightarrow a = 0$ nebo $b = 0$.

Důkaz:

$a, b \in P \quad a \cdot b = 0$

? a) $b = 0 \Rightarrow a \cdot 0 = 0$ (viz předchozí tvrzení)

b) $b \neq 0$ $\quad a \cdot b = 0 \;/ \cdot b^{-1}$

$a \cdot b \cdot b^{-1} = 0 \cdot b^{-1}$

$a = 0$

Tvrzení: Je-li $P$ pole, pak $P^* = P \setminus \{0\}$ je grupa vzhledem k bin. op. násobení $\cdot$.

Důkaz: $P^* = P \setminus \{0\}$

Je $\cdot$ bin. op na $P^*$?

Důkaz sporem: $\exists\, a, b \in P^*$ takže

$a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$

$\Rightarrow$ spor $\Rightarrow$ $\cdot$ je bin. op. na $P^*$

$\dots \Rightarrow (P^*, \cdot, 1, {}^{-1})$ je kon. grupa. $\square$

Definice: Buď $P, Q$ pole. Buď $f: P \to Q$ zobrazení. Nechť $\forall a, b \in P$:

$$f(a +_P b) = f(a) +_Q f(b)$$

$$f(-_P a) = -_Q f(a)$$

$$f(0_P) = 0_Q$$

$$f(a \cdot_P b) = f(a) \cdot_Q f(b)$$

$$f(1_P) = 1_Q$$

$$a \neq 0: f(a^{-1}_P) = f(a)^{-1}_Q$$

Pak $f$ se nazývá hom. pol.

Příklad:

$z: \{0,1\} \to \mathbb{Z}_2$

$0 \mapsto [0]_2$

$1 \mapsto [1]_2$

izomorfismus polí

# Permutace

Definice: Buď $M$ konečná mn.

Bijekce $M \to M$ se

nazývá permutace na mn. $M$.

$M$ .. $n$ prvků

$S(M)$ .. $n!$ prvků

$I_n = \{1, \dots, n\}$ 1. zjednodušení

$S_n$

$I_3 = \{1,2,3\}$

$S_3 = \{p_1, \ldots, p_6\}$

$p_1 : I_3 \to I_3$, $1 \to 3$, $2 \to 2$, $3 \to 1$

2. zjednodušení

$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

3. zjednodušení

$p_1 = (3\,2\,1)$

$$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

skládání permutací:

$$p_1 \circ p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$= p_5$$

inverzní permutace:

$$p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$p_3^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = p_3$$

počet inverzí $p_5 = 1$

(3 2)