

Grupa permutací

Def (Permutace): Permutací množiny A nazveme libovolné bijektivní zobrazení $\sigma: A \rightarrow A$.

Pr. 1: 1.) $A = \mathbb{Z}$, $\sigma(n) = n+1 \Rightarrow \underline{\underline{\sigma \text{ je permutace } A}}$

σ je injektivní: $\sigma(n_1) = \sigma(n_2) \Rightarrow n_1+1 = n_2+1 \Rightarrow n_1 = n_2$.

σ je surjektivní: $\forall k \in \mathbb{Z} \exists n = k-1 \in \mathbb{Z}: \sigma(n) = \sigma(k-1) = k$

2.) A - libovolná neprázdná množina: $\sigma = \text{id}$, tzn. $\forall x \in A: \sigma(x) = x$

$\Rightarrow \underline{\underline{\sigma \text{ je permutace } A}}$

Věta: Necht' $\text{Perm } A = \{ \sigma: A \rightarrow A \mid \sigma \text{ je bijekce} \}$ (tzn. $\text{Perm } A$ je množina všech permutací množiny A) a $\circ$ je skládání zobrazení. Potom $(\text{Perm } A, \circ)$ je grupa.

Důkaz: 1.) uzavřenost: Složení dvou bijekcí je bijekce $\Rightarrow \forall \sigma_1, \sigma_2 \in \text{Perm } A: \sigma_1 \circ \sigma_2 \in \text{Perm } A$

2.) asociativita: Skládání zobrazení je asociativní.

3.) neutrální prvek: $\sigma = \text{id}: A \rightarrow A$ je bijekce $\Rightarrow \sigma = \text{id} \in \text{Perm } A$ a je to neutrální prvek vzhledem ke skládání zobrazení.

4.) inverzní prvky: $\forall \sigma \in \text{Perm } A \exists \sigma^{-1} \in \text{Perm } A: \sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \text{id}$
(protože σ je bijekce)

Poznámka: Dále se budeme zabývat grupami permutací konečných množin $A = \{a_1, a_2, \dots, a_n\}$. Pro jednoduchost zápisu, budeme prvek a_1 označovat symbolem 1, a_2 symbolem 2, $\dots$, a_n symbolem n . Tím budeme značit:

$$A = I_n = \{1, 2, \dots, n\}, \text{ Perm } A = S_n$$

Def (Transpozice): Zobrazení $T \in S_n$ je transpozicí v S_n právě tehdy, když:

$$(\exists j, k \in I_n : T(j) = k, T(k) = j) \wedge (\forall x \in I_n - \{j, k\} : T(x) = x)$$

Poznámka: Postupněme si, že $T^{-1} = T$, neboť $T \circ T = \begin{pmatrix} 1 & 2 & \dots & j & \dots & k & \dots & n \\ 1 & 2 & \dots & k & \dots & j & \dots & n \\ 1 & 2 & \dots & j & \dots & k & \dots & n \end{pmatrix} = \text{id}$.

Př: Tím transpozice „vymění“ jen dva prvky, ostatní nechal na místě. Např:

$$T_1 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{bmatrix} \in S_5 \quad \text{je transpozice}$$

$$T_2 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{bmatrix} \in S_5 \quad \text{je transpozice}$$

$$\sigma = T_2 \circ T_1 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{bmatrix} \quad \text{není transpozice, ale je to složení dvou transpozic.}$$

Problém: Lze každé $\sigma \in S_n$ napsat jako složení transpozic (dvou, tří, čtyř, $\dots$)?

Věta: Pro každou permutaci $\sigma \in S_n, n \geq 2$, existují transpozice $\tau_1, \tau_2, \dots, \tau_m \in S_n$ takové, že:

$$\sigma = \tau_1 \circ \tau_2 \circ \dots \circ \tau_m$$

Důkaz: Provedeme indukci podle n .

a) $n = 2$

$I_n = \{1, 2\} \Rightarrow S_2 = \{id, \tau\}$, kde $\tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ = transpozice a platí: $id = \tau \circ \tau$.

b) Indukční krok. Předpokládejme, že každou permutaci z S_{n-1} je možno složit z transpozic z S_{n-1} .

Dohodněme se, že restrikci $\varphi \in S_n$ na I_{n-1} budeme značit φ^* .

Uvažujme libovolné $\sigma \in S_n$.

I.) $\sigma(n) = n$

Potom $\sigma = \begin{pmatrix} 1 & 2 & \dots & (n-1) & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n-1) & n \end{pmatrix}$ a σ^* je permutace prvků z $I_{n-1} \Rightarrow$

$\Rightarrow \sigma^* \in S_{n-1} \Rightarrow$ podle předpokladu $\exists \tau_1^*, \dots, \tau_m^* \in S_{n-1} : \sigma^* = \tau_1^* \circ \dots \circ \tau_m^*$

Platí $\forall i \in \{1, \dots, m\}$ definovat $\tilde{\tau}_i(x) = \begin{cases} \tau_i^*(x) & \Leftrightarrow x \in I_{n-1} \\ n & \Leftrightarrow x = n \end{cases} \Rightarrow \sigma = \tilde{\tau}_1 \circ \dots \circ \tilde{\tau}_m$

II.) $\sigma(n) = k \neq n$

$\Rightarrow$ Vermíme $\tau \in S_n : \tau(k) = n$. Potom $(\tau \circ \sigma)(n) = \tau(\sigma(n)) = n$

$\Rightarrow (\tau \circ \sigma)^* \in S_{n-1} \Rightarrow \exists$ transp. $\tau_1^*, \dots, \tau_m^* \in S_{n-1} : (\tau \circ \sigma)^* = \tau_1^* \circ \dots \circ \tau_m^*$

$\Rightarrow \forall i \in \{1, \dots, m\}$ def. $\tilde{\tau}_i(x) = \begin{cases} \tau_i^*(x) & \Leftrightarrow x \in I_{n-1} \\ n & \Leftrightarrow x = n \end{cases} \Rightarrow \tau \circ \sigma = \tilde{\tau}_1 \circ \dots \circ \tilde{\tau}_m \Rightarrow$

$$\sigma = \tau^{-1} \circ \tilde{\tau}_1 \circ \dots \circ \tilde{\tau}_m$$

"transpozice τ "

□

Def_{inf m}($\sigma \Delta_m$): Nechť $\sigma \in S_m$. Označme $\Delta_m = \prod_{\substack{a, b \in \{1, \dots, m\} \\ a > b}} (a - b)$ a

$$\sigma \Delta_m = \prod_{\substack{a, b \in \{1, \dots, m\} \\ a > b}} (\sigma(a) - \sigma(b))$$

Pr_{inf}: Uvažujme $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \in S_4$ (je to transpozice). Potom:

$$\Delta_4 = (4-3)(4-2)(4-1)(3-2)(3-1)(2-1)$$

$$\sigma \Delta_4 = (4-3)(4-1)(4-2)(3-1)(3-2)(1-2) = (-1) \cdot \Delta_4$$

Def_{inf m}($\varepsilon(\sigma)$): Definujme zobrazení $\varepsilon: S_m \rightarrow \mathbb{R} - \{0\}$ předpisem:

$$\varepsilon(\sigma) = \frac{\sigma \Delta_m}{\Delta_m}$$

Pr_{inf}: Vermene-li σ z předchozího příkladu, vidíme, že $\varepsilon(\sigma) = -1$.

Uvažujme transpozici $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$. Potom:

$$\Delta_4 = (4-3)(4-2)(4-1)(3-2)(3-1)(2-1)$$

$$\tau \Delta_4 = (4-1)(4-2)(4-3)(1-2)(1-3)(2-3) = (-1) \Delta_4$$

$$\Rightarrow \varepsilon(\tau) = \frac{\tau \Delta_4}{\Delta_4} = -1$$

Dokažeme, že pro libovolnou transpozici $\tau \in S_m$ je $\varepsilon(\tau) = -1$.

Věta : Necht' $\tau \in S_n$ je transpozice. Potom $\varepsilon(\tau) = -1$.

Důkaz: Uvažujme transpozici $\tau \in S_n$, kde $\tau(j) = k$, $\tau(k) = j$, $j > k$
a $r \in \{1, 2, \dots, n\} - \{j, k\}$. Potom $\tau(r) = r$ a platí:

I.) Jestliže $r > j > k$, pak:

$$(\tau(r) - \tau(j))(\tau(r) - \tau(k)) = (r - k)(r - j) = (r - j)(r - k)$$

II.) Jestliže $j > r > k$, pak:

$$(\tau(j) - \tau(r))(\tau(r) - \tau(k)) = (k - r)(r - j) = (j - r)(r - k)$$

III.) Jestliže $j > k > r$, pak:

$$(\tau(j) - \tau(r))(\tau(k) - \tau(r)) = (k - r)(j - r) = (j - r)(k - r)$$

IV.) Navíc:

$$(\tau(j) - \tau(k)) = (k - j) = (-1)(j - k)$$

Z I.) II.) III.) IV.) plyne, že:

$$\tau \Delta_n = \prod_{\substack{a, b \in \{1, \dots, n\} \\ a > b}} (\tau(a) - \tau(b)) = (-1) \prod_{\substack{a, b \in \{1, \dots, n\} \\ a > b}} (a - b) = (-1) \Delta_n$$

Věta: Necht' $\sigma, \tau \in S_n$. τ je transpozice. Potom

$$\sigma \circ \tau \Delta_n = -\sigma \Delta_n$$

Důkaz: Uvažujme transpozici $\tau(j)=k, \tau(k)=j, j > k$
a $n \in \{1, 2, \dots, n\} - \{j, k\}$. Potom $\tau(n)=n$ a platí:

I.) Jestliže $n > j > k$, pak:

$$\begin{aligned} (\cancel{\sigma \circ \tau}(n) - \cancel{\sigma \circ \tau}(j))(\cancel{\sigma \circ \tau}(n) - \cancel{\sigma \circ \tau}(k)) &= (\sigma(n) - \sigma(j))(\sigma(n) - \sigma(k)) = \\ &= (\sigma(n) - \sigma(j))(\sigma(n) - \sigma(k)) \Rightarrow \\ &\Rightarrow \text{můžeme „škrtnout } \tau \text{“} \end{aligned}$$

II.) Jestliže $j > n > k$, pak:

$$\begin{aligned} (\sigma \circ \tau(j) - \sigma \circ \tau(n))(\sigma \circ \tau(n) - \sigma \circ \tau(k)) &= (\sigma(k) - \sigma(n))(\sigma(n) - \sigma(j)) = \\ &= (\sigma(j) - \sigma(n))(\sigma(n) - \sigma(k)) \\ &\Rightarrow \text{můžeme „škrtnout } \tau \text{“} \end{aligned}$$

III.) Jestliže $j > k > n$, pak:

$$\begin{aligned} (\sigma \circ \tau(j) - \sigma \circ \tau(n))(\sigma \circ \tau(k) - \sigma \circ \tau(n)) &= (\sigma(k) - \sigma(n))(\sigma(j) - \sigma(n)) = \\ &= (\sigma(j) - \sigma(n))(\sigma(k) - \sigma(n)) \\ &\Rightarrow \text{můžeme „škrtnout } \tau \text{“} \end{aligned}$$

$$\text{IV.) Navíc } (\sigma \circ \tau(j) - \sigma \circ \tau(k)) = (\sigma(k) - \sigma(j)) = -(\sigma(j) - \sigma(k))$$

z I.) II.) III.) IV.) a protože pro $a, b \in \{1, 2, \dots, n\} - \{j, k\}$: $\sigma \circ \tau(a) = \sigma(a), \sigma \circ \tau(b) = \sigma(b) \Rightarrow$

$$\sigma \circ \tau \Delta_n = \prod_{\substack{a, b \in \{1, \dots, n\} \\ a > b}} (\sigma \circ \tau(a) - \sigma \circ \tau(b)) = - \prod_{\substack{a, b \in \{1, \dots, n\} \\ a > b}} (\sigma(a) - \sigma(b)) = -\sigma \Delta_n$$

□

Poznámka: Každou permutaci $\sigma \in S_n$ lze složit z transpozic,
ale ne nutně jediným způsobem! Například:

$$\sigma = \left(\begin{array}{c} \boxed{1 \ 2 \ 3 \ 4 \ 5} \\ \boxed{1 \ 3 \ 2 \ 4 \ 5} \\ \boxed{1 \ 3 \ 4 \ 2 \ 5} \end{array} \right\} \tilde{\tau}_1 = \left(\begin{array}{c} \boxed{1 \ 2 \ 3 \ 4 \ 5} \\ \boxed{1 \ 4 \ 3 \ 2 \ 5} \\ \boxed{1 \ 3 \ 4 \ 2 \ 5} \end{array} \right\} \tilde{\tau}_2 \Rightarrow$$

$$\sigma = \tilde{\tau}_2 \circ \tilde{\tau}_1 = \tilde{\tau}_3 \circ \tilde{\tau}_2, \text{ kde } \tilde{\tau}_1, \tilde{\tau}_2, \tilde{\tau}_3 \text{ jsou navzájem} \\ \text{různé transpozice.}$$

Věta: Necht' $\sigma \in S_n$ a $\sigma = \alpha_1 \circ \alpha_2 \circ \dots \circ \alpha_r = \beta_1 \circ \beta_2 \circ \dots \circ \beta_s$, kde
 $\alpha_1, \alpha_2, \dots, \alpha_r, \beta_1, \beta_2, \dots, \beta_s$ jsou transpozice z S_n . Potom
(r i s je sudé), nebo (r i s je liché).

Důkaz: Číslo $\varepsilon(\sigma) = \frac{\sigma \Delta_n}{\Delta_n}$ je pro dané σ určeno jednoznačně,
platí: $\sigma \Delta_n = \varepsilon(\sigma) \Delta_n$ a podle dříve dokázaného:

$$a) \sigma = \alpha_1 \circ \alpha_2 \circ \dots \circ \alpha_r \Rightarrow$$

$$\sigma \Delta_n = (\alpha_1 \circ \alpha_2 \circ \dots \circ \alpha_{r-1}) \circ \alpha_r \Delta_n = -(\alpha_1 \circ \alpha_2 \circ \dots \circ \alpha_{r-1}) \Delta_n = (-1)^r \Delta_n$$

$$b) \sigma = \beta_1 \circ \beta_2 \circ \dots \circ \beta_s \Rightarrow \text{analogicky:}$$

$$\sigma \Delta_n = (-1)^s \Delta_n$$

Z a.) a b.) plyne, že $\varepsilon(\sigma) = (-1)^r = (-1)^s \Rightarrow r$ i s jsou obě sudá čísla,
nebo obě lichá čísla

Def (Sudé a liché permutace): Permutaci $\sigma \in S_n$ nazveme

a) Sudou permutací $\Leftrightarrow \varepsilon(\sigma) = 1$

b) Lichou permutací $\Leftrightarrow \varepsilon(\sigma) = -1$

Množinu všech sudých permutací z S_n budeme značit A_n .

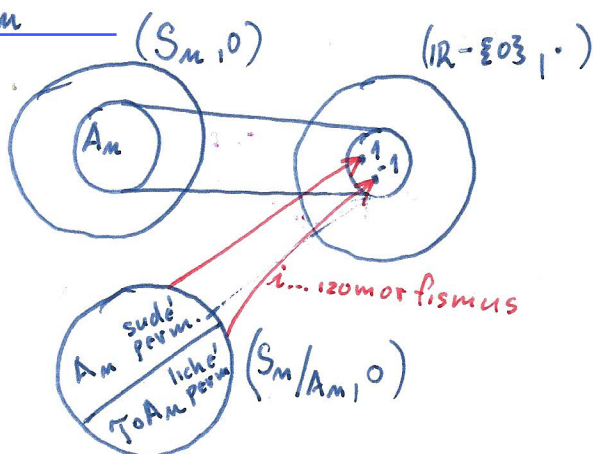
Poznámka: Zjistili jsme, že každou permutaci $\sigma \in S_n$ je možné složit z transpozic. Je to možné udělat různými způsoby, ale daná permutace σ je vždy složením sudého počtu transpozic ($\Leftrightarrow \varepsilon(\sigma) = 1$), nebo je vždy složením lichého počtu transpozic.

Věta: Zobrazení $\varepsilon: S_n \rightarrow \mathbb{R}, n \geq 2$ je homomorfismem grup $(S_n, \circ)$ do grup $(\mathbb{R} \setminus \{0\}, \cdot)$ a platí:

a) $\varepsilon(S_n) = \{-1, 1\}$

b) $(\text{Ker } \varepsilon, \circ) = (A_n, \circ)$ je normální podgrupa v $(S_n, \circ)$

c) $S_n / A_n = \{A_n, \tau \circ A_n\}$, kde $\tau \in S_n$ je transpozice



Důkaz: $\forall \sigma_1 = \alpha_1 \circ \dots \circ \alpha_r, \sigma_2 = \beta_1 \circ \dots \circ \beta_s$, kde α_i, β_j jsou transpozice :

$$\varepsilon(\sigma_1 \circ \sigma_2) = \frac{\alpha_1 \circ \dots \circ \alpha_r \circ \beta_1 \circ \dots \circ \beta_s (\Delta_n)}{\Delta_n} = (-1)^{r+s} = (-1)^r \cdot (-1)^s = \varepsilon(\sigma_1) \cdot \varepsilon(\sigma_2) \Rightarrow \varepsilon \text{ je homomorf.}$$

a) $\forall \sigma \in S_n \exists$ transpozice $\tau_1, \tau_2, \dots, \tau_m \in S_n : \sigma = \tau_1 \circ \tau_2 \circ \dots \circ \tau_m$.

$$\Rightarrow \varepsilon(\sigma) = \frac{\sigma \Delta_n}{\Delta_n} = \frac{\tau_1 \circ \tau_2 \circ \dots \circ \tau_m \Delta_n}{\Delta_n} = \frac{(-1)^m \Delta_n}{\Delta_n} = (-1)^m \in \{-1, 1\}$$

$$\Rightarrow \varepsilon(S_n) \subseteq \{-1, 1\}$$

Navíc $\varepsilon(\tau) = -1$ (τ je transpozice), $\varepsilon(\tau \circ \tau) = 1 \Rightarrow \{-1, 1\} \subseteq \varepsilon(S_n)$

b) $\text{Ker } \varepsilon = \{\sigma \in S_n \mid \varepsilon(\sigma) = 1\} = A_n$

Navíc bylo dříve dokázáno, že jádro homomorfismu tvoří normální podgrupou.

c) $\varepsilon: S_n \rightarrow \mathbb{R}$ je homomorfismus. Dříve bylo dokázáno, že

$$S_n / \text{Ker } \varepsilon = S_n / A_n \cong \varepsilon(S_n) = \{-1, 1\}$$

$\Rightarrow$ Rozklad S_n / A_n je dvojprvkový a jistě do něj patří $A_n = \text{id} \circ A_n$

Uvažujme libovolnou transpozici $\tau \in S_n$. Pak $\tau \circ A_n \in S_n / A_n$

a protože $\tau \notin A_n$ jistě platí $\tau \circ A_n \neq A_n \Rightarrow$

$$S_n / A_n = \{\sigma \circ A_n \mid \sigma \in S_n\} = \{A_n, \tau \circ A_n\}$$

Def. (Alternující grupa): Grupu $(A_n, \circ)$ nazýváme alternující grupou.

(A_n je to grupa všech sudých permutací z S_n .)