4. Permutace

Definice 4.1. ***Permutací na množině*** *X rozumíme bijekci X na X, tj. prosté zobrazení X na X. Množinu všech permutací na množině X značíme S_X. Množinu všech permutací na množině $X = \{1, 2, \dots, n\}$ značíme S_n.*

V lineární algebře budeme pracovat jen s permutacemi na množině
$X = \{1, 2, \dots, n\}$ pro nějaké přirozené číslo n, tedy s prvky S_n. Je dobré si uvědomit, že pro konečné množiny platí následující tvrzení.

Tvrzení 4.2. *Buď n přirozené číslo, $X = \{1, 2, \dots, n\}$ a $f : X \to X$ zobrazení. Následující tvrzení jsou ekvivalentní.*

1. *f je na*
2. *f je prosté*
3. *f je permutace (tj. prosté a na)*

Důkaz. Je snadný. $\square$

Pro nekonečné množiny X (např. pro množinu všech přirozených čísel) předchozí tvrzení neplatí, viz příklady.

Permutaci $\pi \in S_n$ můžeme zapsat např. tabulkou – do horního řádku napíšeme čísla $1, \dots, n$ a do dolního řádku napíšeme obrazy (pod 1 bude $\pi(1)$, atd.). V dolním řádku bude samozřejmě každé z čísel $1, \dots, n$ a to právě jednou. Např.

$$\pi : \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \rho : \begin{pmatrix} 2 & 1 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

jsou zápisy permutací. Všimněte si, že $\pi = \rho$. Číslům i, pro něž $\pi(i) = i$, říkáme **samodružné prvky** permutace π. V našem případě máme jeden samodružný prvek, a to 2.

Příklady permutací

Identická permutace. Je to permutace, která má všechny prvky samodružné. Tabulkou:

$$id : \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

Transpozice i a j (i a j jsou různá přirozená čísla). Je to permutace π, pro niž $\pi(i) = j$, $\pi(j) = i$ a $\pi(k) = k$ pro $k \neq i, j$. Tabulkou:

$$\pi : \begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots \\ 1 & 2 & \dots & j & \dots & i & \dots \end{pmatrix}.$$

Cyklus délky d. Je to permutace π tvaru $\pi(i_1) = i_2$, $\pi(i_2) = i_3$, $\ldots$, $\pi(i_{d-1}) = i_d$, $\pi(i_d) = i_1$ a $\pi(k) = k$ jinak, kde $i_1, i_2, \ldots, i_d$ jsou navzájem různá přirozená čísla. Tabulkou:

$$\pi : \begin{pmatrix} i_1 & i_2 & \ldots & i_{d-1} & i_d & \ldots \\ i_2 & i_3 & \ldots & i_d & i_1 & \ldots \end{pmatrix}.$$

Transpozice je tedy cyklus délky 2. Cykly často zapisujeme seznamem $(i_1, i_2, \ldots, i_d)$. Takový zápis není jednozačný, např. (1234), (2341), (3412), (4123) jsou (všechny možné) zápisy stejného cyklu délky 4, totiž permutace

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

Dva cykly $(i_1, \ldots, i_d)$ a $(j_1, \ldots, j_e)$ nazýváme **nezávislé**, pokud jsou množiny $\{i_1, \ldots, i_d\}$ a $\{j_1, \ldots, j_e\}$ disjunktní.

Skládání permutací, inverzní permutace

Permutace můžeme skládat (někdy říkáme „násobit“) – skládáme je jako jakákoliv jiná zobrazení. Je jednoduché si rozmyslet, že složením dvou permutací na X je opět permutace na X (složení dvou prostých zobrazení je prosté, složení dvou zobrazení na je na). V našem kurzu skládáme *zprava do leva*, jak je to běžné u reálných funkcí (např. $\sin \cos x$ znamená nejprve proveď cos a potom sin). Skládání značíme znakem $\circ$, někdy se tento znak vynechává. Např. pro permutace

$$\pi : \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \rho : \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

máme

$$\pi \circ \rho = \begin{pmatrix} 1 & 2 & 3 \\ \pi(\rho(1)) & \pi(\rho(2)) & \pi(\rho(3)) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)$$

a

$$\rho \circ \pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132)$$

Zde vidíme, že skládání permutací není **komutativní**, tj. prohozením pořadí skládání se obecně změní výsledek. Důležitým příkladem, kdy dvě permutace komutují (tj. lze změnit pořadí při skládání) jsou nezávislé cykly.
Na druhou stranu je skládání zřejmě **asociativní**, tj. $(\pi_1 \circ \pi_2) \circ \pi_3 = \pi_1 \circ (\pi_2 \circ \pi_3)$. Díky tomu nemusíme při skládání více permutací psát závorky. Běžné je značení

$$\begin{aligned} \pi^0 &= id \\ \pi^i &= \underbrace{\pi \circ \pi \circ \ldots \circ \pi}_{i\times}, \quad i = 1, 2, \ldots \end{aligned}$$

Zřejmě $\pi \circ id = id \circ \pi = \pi$ pro libovolnou permutaci π.

Ke každé permutaci můžeme (vzhledem k tomu že jde o bijekci) vytvořit permutaci inverzní – každému prvku přiřadíme jeho vzor. Inverzní permutaci k π značíme π^{-1}. Např.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}.$$

Zřejmě $\pi \circ \pi^{-1} = \pi^{-1} \circ \pi = id$ pro libovolnou permutaci π.

Připomeňme zde pojem grupy:

Grupa je čtveřice $(G, \circ, ^{-1}, 1)$, kde G je množina, $\circ$ je binární operace, $^{-1}$ je unární operace a $1 \in G$, která pro libovolné prvky $a, b, c \in G$ splňuje

$$\begin{array}{ll} a \circ (b \circ c) = (a \circ b) \circ c & \text{(asociativita)} \\ a \circ a^{-1} = a^{-1} \circ a = 1 & (a^{-1} \text{ je inverzní prvek k } a) \\ a \circ 1 = 1 \circ a = a & \text{(1 je jednotkový prvek)} \end{array}$$

Shrneme-li poznatky z této části, vidíme, že $(S_n, \circ, ^{-1}, id)$ je grupa.

Rozklad na cykly a transpozice

Nejvýhodnější způsob zápisu permutace je pomocí nezávislých cyklů.

Tvrzení 4.3. *Každou permutaci $\pi \in S_n$ lze rozložit na součin nezávislých cyklů délky alespoň 2. Tento rozklad je až na pořadí činitelů jednoznačný.*

Důkaz. Existence rozkladu: Indukcí podle počtu nesamodružných prvků k dokážeme: „Každou permutaci $\pi \in S_n$ s nejvýše k nesamodružnými prvky lze rozložit na součin nezávislých cyklů délky alespoň 2, přičemž žádný z cyklů neobsahuje samodružný prvek.“ Tvrzení je zřejmé pro $k = 0$ (použijeme 0 cyklů). Dále indukcí. Vezmeme libovolný nesamodružný prvek i_1 permutace π. Označíme $i_2 = \pi(i_1)$, $i_3 = \pi(i_2)$, ... Vezmeme nejmenší l takové, že $i_l = i_m$ pro nějaké $m < l$. Jelikož π je prosté, je zřejmě $m = 1$ (nakreslete si obrázek). Označme $\pi_1 = (i_1 i_2 \dots i_{l-1})$. V permutaci $\pi \circ \pi_1^{-1}$ je méně samodružných prvků než v permutaci π (samodružné jsou všechy samodružné prvky permutace π a navíc $i_1, \dots, i_{l-1}$). Tedy můžeme použít indukční předpoklad a rozložit $\pi \circ \pi_1^{-1}$ na součin nezávislých cyklů: $\pi \circ \pi_1^{-1} = \pi_2 \circ \pi_3 \circ \ldots \circ \pi_z$. Nyní $\pi = \pi_2 \circ \pi_3 \circ \ldots \circ \pi_z \circ \pi_1$ (vynásobili jsme předchozí rovnost permutací π_1 zprava) je hledaný rozklad (cykly π_1 a $\pi_{cokoliv>1}$ jsou skutečně nezávislé, protože žádný z cyklů π_2 $\dots \pi_z$ neobsahuje samodružné prvky permutace $\pi \circ \pi_1^{-1}$, tedy ani $i_1, \dots, i_{l-1}$)).

Jednoznačnost: Mějme dva rozklady permutace π na nezávislé cykly délky alespoň 2. Vyskytuje-li se číslo i v jednom rozkladu, pak je i nesamodružným prvkem, tedy se vyskytuje i v druhém rozkladu. V libovolném cyklu musí za číslem i následovat číslo $\pi(i)$, protože cykly jsou nezávislé. Odtud tvrzení okamžitě plyne. □

Důkaz předchozího tvrzení rovněž říká, jak danou permutaci π rozložit na nezávislé cykly. Postup budeme ilustrovat na permutaci

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

Nakreslíme levou závorku a libovolné číslo, např. 1. Vedle čísla 1 napíšeme jeho obraz $\pi(1) = 3$. Vedle 3 opět jeho obraz $\pi(3) = 7$, dále $\pi(7) = 2$. Nyní $\pi(2) = 1$ tedy závorku uzavřeme. Máme (1372). Levou závorkou zahájíme nový cyklus a zvolíme libovolné číslo, které se ještě doposud neobjevilo, např. 4. Protože $\pi(4) = 5$ a $\pi(5) = 4$, na papíře se skví (1372)(45). Teď začneme např. s číslem 6, protože ale $\pi(6) = 6$, závorku rovnou uzavřeme. Nakonec $\pi(8) = 9$, $\pi(9) = 8$. Tedy $\pi : (1372)(45)(6)(89)$. Samodružné prvky do rozkladu většinou nepíšeme, tedy lépe

$$\pi : (1372)(45)(89).$$

Procvičte si invertování a skládání permutací zapsaných rozkladem na nezávislé cykly.

Každý cyklus lze napsat jako součin transpozic (viz příklady), tedy rovnou máme:

Tvrzení 4.4. *Každou permutaci lze napsat jako součin transpozic.*

Znaménko permutace

Množinu S_n, $n > 1$ lze rozdělit na dvě stejně velké části (viz příklady) – množinu sudých permutací a množinu lichých permutací.

Věta a definice 4.5. *Ať $\pi \in S_n$. Následující tvrzení jsou ekvivalentní:*

1. *V rozkladu π na nezávislé cykly je sudý počet cyklů sudé délky.*
2. *π lze rozložit na sudý počet transpozic.*
3. *π má sudý počet inverzí, tj. počet dvojic $1 \neq i < j \leq n$, pro které $\pi(i) > \pi(j)$, je sudý.*

Pokud π splňuje jednu z těchto podmínek (tedy všechny), říkáme, že π je ***sudá****. V opačném případě říkáme, že π je* ***lichá****. Znaménko permutace definujeme*

$$\operatorname{sgn} \pi = \begin{cases} 1 & \textit{pokud } \pi \textit{ je sudá} \\ -1 & \textit{pokud } \pi \textit{ je lichá} \end{cases}$$

Než přistoupíme k důkazu, několik poznámek.

- Negace prvního tvrzení v předchozí větě zní: …lichý počet cyklů sudé délky
- Platí
$$\operatorname{sgn} \pi = \prod_{1 \leq i < j \leq n} \frac{\pi(i) - \pi(j)}{i - j}.$$
To vyplývá z toho, že počet -1 ve výrazu vpravo (po přeskupení) je přesně počet inverzí.
- Rozklad na transpozice není jednoznačný. Z této věty ale plyne, že parita (=sudost či lichost) počtu transpozic je v každém rozkladu stejná.

Důkaz. Uvažujme libovolnou permutaci ρ a transpozici (a, b). Ukážeme, že permutace ρ a $(a, b) \circ \rho$ mají opačnou paritu počtu cyklů sudé délky. Uvažujme rozklad $\rho = \rho_1 \circ \ldots \circ \rho_k$ na nezávislé cykly, přičemž do rozkladu přidáme i cykly délky 1 - samodružné prvky. Máme dvě možnosti: buď se a a b vyskytují ve stejném cyklu, řekněme ρ_1, nebo ve dvou různých cyklech, řekněme ρ_1, ρ_2. Podívejme se na první možnost: $\rho_1 = (a, c_1, c_2, \ldots, c_i, b, d_1, \ldots, d_j)$. Pak

$$(a, b) \circ \rho = (a, c_1, c_2, \ldots, c_i) \circ (b, d_1, d_2, \ldots, d_j) \circ \rho_2 \circ \ldots \circ \rho_k,$$

přičemž cykly na pravé straně jsou nezávislé (nakreslete si obrázek!). Takže, pokud je ρ_1 sudé délky, tak vziknou dva cykly buď oba sudé délky nebo oba liché délky. Pokud je ρ_1 liché délky, vzikne jeden cyklus sudé délky a jeden cyklus liché délky. V obou případech je parita počtu cyklů v sudé délky v permutacích ρ a $(a, b) \circ \rho$ opačná. V případě, že se a a b vyskytují v různých cyklech, složením s (a, b) se tyto cykly spojí (ověřte!) a parita bude opět opačná.

(2) $\Rightarrow$ (1): Vezmeme rozklad $\pi = \pi_1 \circ \ldots \circ \pi_{2k}$ na transpozice. Permutace π_{2k} má lichý počet cyklů sudé délky, totiž jeden. Podle předchozího $\pi_{2k-1} \circ \pi_{2k}$ má sudý počet cyklů sudé délky, $\pi_{2k-2} \circ (\pi_{2k-1} \circ \pi_{2k})$ má lichý počet cyklů sudé délky, $\ldots$, $\pi_1 \circ \ldots \pi_{2k}$ má sudý počet cyklů sudé délky (indukce).

$\neg$(2) $\Rightarrow$ $\neg$(1): Analogicky.

(2) $\Leftrightarrow$ (3): Zatím jen náznak – lze postupovat podobně jako v důkazu (2) $\Leftrightarrow$ (1). Nejprve se dokáže, že parita počtu inverzí v permutaci ρ a $(a, b) \circ \rho$ je opačná a důkaz se dokončí stejně. □

Znaménko permutace a grupové operace:

Tvrzení 4.6. *Nechť* $\pi, \rho \in S_n$. *Pak*

1. $\operatorname{sgn} id = 1$
2. $\operatorname{sgn} (\pi^{-1}) = \operatorname{sgn} \pi$
3. $\operatorname{sgn} (\pi \circ \rho) = \operatorname{sgn} \pi \cdot \operatorname{sgn} \rho$.

Důkaz. Je snadný. Například takto:

1. Identická permutace má 0 cyklů sudé délky.
2. Inverzní permutace má stejný počet cyklů stejné délky jako permutace původní.
3. Je vidět z rozkladu na transpozice – složením rozkladů permutací π a ρ na transpozice, vznikne rozklad $\pi \circ \rho$ na transpozice.

□