Permutace

Tomáš Roskovec

Definice. *Prosté zobrazení* $\Pi : M \to M$ *nazýváme* permutací na množině M.

Poznámka. Prosté zobrazení konečné množiny M na sebe samu je zřejmě také surjektivní. Proto budou permutace na konečných množinách bijekcemi.

Poznámka. (O prvním způsobu zápisu) Permutaci Π lze zapsat jako tabulku. Nejjednodušší formou zápisu je takzvaný *základní tvar*

$$\Pi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ r_1 & r_2 & r_3 & \cdots & r_n \end{pmatrix},$$

kde $\Pi(i) = r_i$.

Poznámka. Kvůli zpřehlednění zápisu může být v některých případech vhodnější přerovnat množinu M. Zvolíme $s_1, s_2, s_3, \ldots, s_n$ libovolné pořadí prvků množiny M a zapíšeme v takzvaném *obecném tvaru*

$$\Pi = \begin{pmatrix} s_1 & s_2 & s_3 & \cdots & s_n \\ t_1 & t_2 & t_3 & \cdots & t_n \end{pmatrix},$$

kde $\Pi(s_i) = t_i$.

Věta. *Na množině* $M = (1, 2 ... n)$ *lze najít právě* $n!$ *různých permutací.*

Důkaz. Indukcí podle n.

Definice. Samodružným prvkem permutace *rozumíme prvek* z*, pro který platí* $\Pi(z) = z$.

Definice. *Permutaci, jejíž všechny prvky jsou samodružné, nazýváme* identickou permutací Id *nebo také* jednotkovou permutací.

Definice. Inverzní permutací *k permutaci*

$$\Pi = \begin{pmatrix} s_1 & s_2 & s_3 & \cdots & s_k \\ t_1 & t_2 & t_3 & \cdots & t_k \end{pmatrix}$$

rozumíme permutaci

$$\Pi^{-1} = \begin{pmatrix} t_1 & t_2 & t_3 & \cdots & t_k \\ s_1 & s_2 & s_3 & \cdots & s_k \end{pmatrix}.$$

Definice. *Jsou-li permutace* Π_1 *a* Π_2 *na množině* M*,*

$$\Pi_1 = \begin{pmatrix} s_1 & s_2 & s_3 & \dots & s_k \\ t_1 & t_2 & t_3 & \dots & t_k \end{pmatrix}, \qquad \Pi_2 = \begin{pmatrix} t_1 & t_2 & t_3 & \dots & t_k \\ r_1 & r_2 & r_3 & \dots & r_k \end{pmatrix},$$

pak součinem permutací Π_1 *a* Π_2 *rozumíme permutaci*

$$\Pi = \begin{pmatrix} s_1 & s_2 & s_3 & \dots & s_k \\ r_1 & r_2 & r_3 & \dots & r_k \end{pmatrix}.$$

Tento vztah zapisujeme jako $\Pi = \Pi_2 \circ \Pi_1$*, někdy zkráceně jako* $\Pi_2\Pi_1$*.*

Poznámka. Narozdíl od obvyklého součinu[1] není součin permutací komutativní. Tedy rozhodně neplatí, že $\Pi_1\Pi_2 = \Pi_2\Pi_1$.

Definice. *Buď* $C = \{r_1 r_2 r_3 \dots r_k\}$*, kde* $k > 1$*, podmnožina množiny* M*. Pak* cyklem *rozumíme permutaci* Π *takovou, která splňuje*

$$\Pi(r_1) = r_2, \Pi(r_2) = r_3, \dots, \Pi(r_{k-1}) = r_k, \Pi(r_k) = r_1, \Pi(s) = s \text{ pro } \forall s \notin C.$$

Cyklus budeme nadále značit $(r_1 r_2 r_3 \dots r_k)$*.*

Definice. Délkou cyklu *rozumíme počet prvků* k*. Cyklus délky* 2 *nazýváme* transpozicí[2].

Definice. *Řekneme, že dva* cykly $(s_1 s_2 s_3 \dots s_k)$ *a* $(r_1 r_2 r_3 \dots r_l)$ *jsou* nezávislé, *jestliže*

$$s_i \neq r_j, \forall i, j : 1 \leq i \leq k, 1 \leq j \leq l.$$

Poznámka. Při součinu dvou nezávislých cyklů nezáleží na pořadí.

Věta. *Každou permutaci* Π *lze rozložit na součin nezávislých cyklů. Tento rozklad je až na pořadí jednoznačný.*

Věta. *Každou permutaci* Π *lze rozložit v součin transpozic. Je-li speciálně* $\Pi = (r_1 r_2 \dots r_k)$ *cyklus, je* $\Pi = (r_1 r_k)(r_1 r_{k-1}) \dots (r_1 r_2)$*.*

Věta. *Buď* $T_1 T_2 \dots T_k = S_1 S_2 \dots S_l = \Pi$ *dva různé rozklady permutace na součin transpozic. Pak čísla* k *a* l *mají stejnou paritu.*

Definice. *O permutaci* Π *řekneme, že je* sudá, *jestliže ji lze rozložit na součin sudého počtu transpozic. O permutaci* Π *řekneme, že je* lichá, *jestliže ji lze rozložit*

---

1 Například při součinu dvou reálných čísel se $a \cdot b = b \cdot a$.

2 Jedná se totiž o prohození dvou prvků.

na součin lichého počtu transpozic. Znaménko permutace $\operatorname{sgn}\Pi$ *definujeme jako* $\operatorname{sgn}\Pi = 1$ *pro sudou a* $\operatorname{sgn}\Pi = -1$ *pro lichou permutaci.*

Věta. *Pro permutace* Π_1, Π_2 *na stejné množině* M *platí*

(i) $\operatorname{sgn}(\Pi_1\Pi_2) = \operatorname{sgn}\Pi_1 \cdot \operatorname{sgn}\Pi_2$,
(ii) $\operatorname{sgn}\Pi_1^{-1} = \operatorname{sgn}\Pi_1$.

Definice. *Inverzí na množině* M *rozumíme dvojici* $i, j \in M$, *pro kterou platí* $i < j$ *a* $\Pi(i) > \Pi(j)$.

Poznámka. Znaménko permutace lze také spočítat jako $\operatorname{sgn}\Pi = (-1)^k$, kde za k dosadíme buď počet cyklů sudé délky v rozkladu Π nebo počet inverzí permutace.

Definice. Řádem permutace *rozumíme nejmenší* $k \in \mathbb{N}$ *takové, že* $\Pi^k = \mathrm{Id}$.

Příklad. Spočtěte znaménko permutace

$$\Pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 \\ 7 & 17 & 3 & 13 & 4 & 15 & 6 & 11 & 14 & 1 & 5 & 12 & 16 & 2 & 10 & 8 & 9 \end{pmatrix}.$$

Příklad. Určete řád permutace

$$\Pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 \\ 7 & 17 & 3 & 13 & 4 & 15 & 6 & 11 & 14 & 1 & 5 & 12 & 16 & 2 & 10 & 8 & 9 \end{pmatrix}.$$

Příklad. Dokažte, že existují

(i) sudé permutace sudého řádu,
(ii) sudé permutace lichého řádu,
(iii) liché permutace sudého řádu a
(iv) liché permutace lichého řádu.

Příklad. Kolik existuje permutací s n prvky, které jsou cyklem.

Příklad. Kolik nejvýše inverzí může být v permutaci s n prvky.

Příklad. Kolik minimálně transpozic potřebujeme na vytvoření libovolné permutace s n prvky.

Příklad. Určete počet inverzí permutace

$$\Pi_1 = \begin{pmatrix} 1 & 2 & 3 & \cdots & k \\ a_1 & a_2 & a_3 & \cdots & a_k \end{pmatrix},$$

známe-li počet inverzí permutace

$$\Pi_2 = \begin{pmatrix} 1 & 2 & 3 & \cdots & k \\ a_k & a_{k-1} & a_{k-2} & \cdots & a_1 \end{pmatrix}.$$