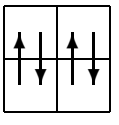
Matematický ústav Slezské univerzity v Opavě
Učební texty k přednášce ALGEBRA I, zimní semestr 2000/2001
Michal Marvan

4. Permutace

Definice. Buď M konečná množina. Bijekce $M \to M$ se nazývá *permutace* na množině M.

Je-li $p : M \to M$ permutace a je-li $m \in M$ libovolný prvek, pak obraz $p(m)$ prvku m obvykle značíme p_m.

Příklad. V králíkárně o čtyřech kotcích žijí čtyři králíci, po jednom v každém kotci. Majitel v pátek přestěhoval králíky z horního patra do spodního a naopak:

$p =$ 

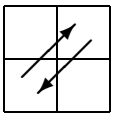
Buď M čtyřprvková množina kotců. Stěhování králíků je permutace na M právě tehdy, když po něm nebudou v žádném kotci dva králíci (injektivita) a žádný kotec nezůstane prázdný (surjektivita).

Označme $S(M)$ množinu všech permutací na množině M. Jsou-li $p, s : M \to M$ dvě permutace, pak jejich *složení* je permutace $s \circ p : M \to M$ daná známou formulí

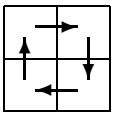
$$(s \circ p)(m) = s(p(m)).$$

Složení permutací je opět permutace, protože složení bijekcí je bijekce. Na množině $S(M)$ tak vzniká asociativní binární operace $S(M) \times S(M) \to S(M)$ *skládání permutací*.

Příklad. Majitel králíkárny z předchozího příkladu v sobotu opět stěhoval králíky:

$s =$ 

(dva králíci zůstali na místě). Ověřte, že

$s \circ p =$ 

Permutace $s \circ p$ vyjadřuje rozmístění králíků v sobotu ve srovnání s rozmístěním králíků ve čtvrtek.

Množina $S(M)$ je grupa vzhledem k binární operaci „$\circ$“. Jednotkovým prvkem je identické zobrazení $\mathrm{id}_M : M \to M$. Inverzní prvky jsou inverzní zobrazení. (Ověřte jako cvičení.)

Pro zjednodušení dalších úvah zvolme pevnou množinu o n prvcích, $I_n = \{1, \ldots, n\} \subset \mathbf{N}$. Množinu všech permutací na množině I_n označme prostě S_n.

Prvky libovolné n-prvkové množiny M můžeme označit indexy $1, \ldots, n$, takže $M = \{m_1, \ldots, m_n\}$. Místo o permutaci prvků m_i množiny M pak můžeme uvažovat o permutaci odpovídajících indexů i, tj. o permutaci na množině $I_n = \{1, \ldots, n\}$. Přechod k množině I_n proto není na úkor obecnosti.

Permutaci $t : I_n \to I_n$ můžeme zapsat různými způsoby. Běžně ji zapisujeme

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ t_1 & t_2 & \cdots & t_n \end{pmatrix}$$

[anebo, pro jednoduchost, jen $(t_1, t_2, \ldots, t_n)$, protože první řádek $(1, 2, \ldots, n)$ je vždy stejný].

Můžeme také kreslit názorné diagramy, například tak, že se množina I_n zobrazí dvakrát vedle sebe a vedou se spojnice mezi prvky i a t_i (viz následující příklad).

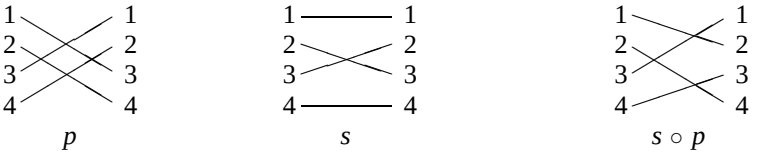
Příklad. Očíslujme kotce:

1	2
3	4

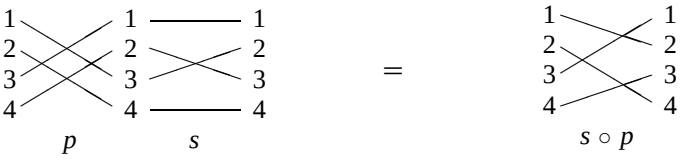
Permutace p, s a $s \circ p$ z předchozího příkladu jsou po řadě

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}, \quad s \circ p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}.$$

Totéž vyjádřeno diagramy:



Při navázání diagramů je názorně vidět, jak se permutace skládají:



Definice. Buď t permutace na množině $I_n = \{1, \ldots, n\}$. Nechť $i, j \in I_n$, přičemž $i < j$ a zároveň $t_i > t_j$. Pak řekneme, že pár (t_i, t_j) *tvoří inverzi*.

Počet inverzí (tj. párů $t_i > t_j$ kde $i < j$) označíme $\operatorname{inv} t$. Dostáváme zobrazení $\operatorname{inv} : S_n \to \mathbf{N} \cup \{0\}$.

Příklad. Vyjmenujme inverze v předchozím příkladu:

$$\begin{aligned} p &: (3,1),\ (3,2),\ (4,1),\ (4,2), && \operatorname{inv} s = 4; \\ s &: (3,2), && \operatorname{inv} p = 1; \\ s \circ p &: (2,1),\ (4,1),\ (4,3), && \operatorname{inv}(s \circ p) = 3. \end{aligned}$$

Počty inverzí lze také snadno určit z diagramů jako počty průsečíků čar.

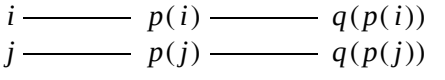
Obecně platí: $\operatorname{inv}(s \circ p) = \operatorname{inv} s + \operatorname{inv} p -$ sudé číslo:

Tvrzení. *Buďte p, q permutace na množině I_n. Pak existuje celé číslo k takové, že platí*

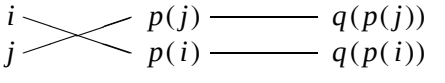
$$\operatorname{inv}(q \circ p) = \operatorname{inv} q + \operatorname{inv} p + 2k.$$

Důkaz. Pro každou dvouprvkovou podmnožinu $\{ i, j \} \subseteq I_n$ označme i menší z obou prvků, takže $i < j$. Vždy nastane právě jeden ze čtyř případů:

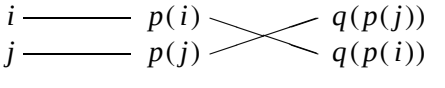
(i) $p(i) < p(j), \quad q(p(i)) < q(p(j))$:



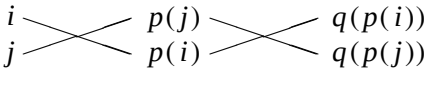
(ii) $p(i) > p(j), \quad q(p(i)) > q(p(j))$:



(iii) $p(i) < p(j), \quad q(p(i)) > q(p(j))$:



(iv) $p(i) > p(j), \quad q(p(i)) < q(p(j))$:



Označme po řadě $N_{(\mathrm{i})}, N_{(\mathrm{ii})}, N_{(\mathrm{iii})}, N_{(\mathrm{iv})}$ počet výskytů dvojice $\{ i, j \} \subseteq I_n$ uvedeného druhu. Pár $\{ i, j \}$ přispívá jednou inverzí k $\operatorname{inv} p$ v případech (ii) a (iv), protože právě v těchto případech jdou $p(j), p(i)$ v opačném pořadí než i, j. Proto platí

$$\operatorname{inv} p = N_{(\mathrm{ii})} + N_{(\mathrm{iv})}.$$

Podobně pár $\{ i, j \}$ přispívá jednou inverzí k $\operatorname{inv} q$ v případech (iii) a (iv), protože právě v těchto případech jdou $q(p(i), q(p(j))$ v opačném pořadí než $p(i), p(j)$:

$$\operatorname{inv} q = N_{(\mathrm{iii})} + N_{(\mathrm{iv})}.$$

A konečně $\{ i, j \}$ přispívá jednou inverzí k $\operatorname{inv}(q \circ p)$ v případech (ii) a (iii), protože právě v těchto případech jdou $q(p(i), q(p(j))$ v opačném pořadí než i, j:

$$\operatorname{inv}(q \circ p) = N_{(\mathrm{ii})} + N_{(\mathrm{iii})}.$$

Pak

$$\begin{aligned} \operatorname{inv}(q \circ p) &= N_{(\mathrm{ii})} + N_{(\mathrm{iii})} = (N_{(\mathrm{ii})} + N_{(\mathrm{iv})}) + (N_{(\mathrm{iii})} + N_{(\mathrm{iv})}) - 2N_{(\mathrm{iv})} \\ &= \operatorname{inv} p + \operatorname{inv} q - 2N_{(\mathrm{iv})}. \end{aligned}$$

Vidíme, že tvrzení platí, přičemž $k = -N_{(\mathrm{iv})} \in \mathbf{Z}$.

Definice. Definujme *signum* (znaménko) permutace $s \in S_n$ předpisem

$$\operatorname{sgn} s = (-1)^{\operatorname{inv} s}.$$

Vidíme, že sgn je zobrazení $S_n \to \{ -1, 1 \}$.

Pro signum složené permutace odvodíme vztah, který již neobsahuje neurčité sudé číslo $2k$:

Tvrzení. *Pro libovolné permutace* $p, q \in S_n$ *platí*

$$\operatorname{sgn}(q \circ p) = \operatorname{sgn} q \cdot \operatorname{sgn} p.$$

Důkaz. $\operatorname{sgn}(q \circ p) = (-1)^{\operatorname{inv}(q\circ p)} = (-1)^{\operatorname{inv} q \,+\, \operatorname{inv} p \,+\, 2k} = (-1)^{\operatorname{inv} q} \cdot (-1)^{\operatorname{inv} p} \cdot (-1)^{2k} = (-1)^{\operatorname{inv} q} \cdot (-1)^{\operatorname{inv} p} = \operatorname{sgn} q \cdot \operatorname{sgn} p.$

Tím je ověřeno, že sgn je homomorfismus pologrup, ale každý pologrupový homomorfismus mezi grupami je homomorfismus grup. Tudíž, sgn je homomorfismus grup $(S_n, \circ, \mathrm{id}, ^{-1}) \to (\{-1, 1\}, \cdot, 1, ^{-1})$.

Zbavit se neurčitého sčítance $2k$ můžeme i tak, že přejdeme ke sčítání v poli $\mathbf{Z}_2$.

Tvrzení. *Pro libovolná* $k, l \in \mathbf{Z}$ *platí*

$$[k + l]_2 = [k]_2 + [l]_2$$

(sčítání vpravo je v $\mathbf{Z}_2$*).*

Důkaz. Cvičení.

Definice. Buď $s : I_n \to I_n$ permutace. Prvek

$$|s| = [\operatorname{inv} s]_2 \quad \in \mathbf{Z}_2$$

se nazývá *parita* permutace s.

Tvrzení. *Buďte* p, q *permutace na množině* I_n. *Pak*
(1) $|q \circ p| = |q| + |p|$ *v* $\mathbf{Z}_2$.
(2) $|\mathrm{id}| = 0$ *v* $\mathbf{Z}_2$.
(3) $|q^{-1}| = |q|$ *v* $\mathbf{Z}_2$.

Důkaz. Cvičení. Návod: viz analogické formule pro sgn.

Mezi paritou a signem je jednoznačný vztah, který výstižně zapisujeme

$$\operatorname{sgn} s = (-1)^{|s|}.$$

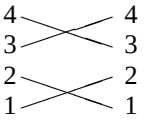
Parita 0 se nazývá „sudá," parita 1 se nazývá „lichá."

Vraťme se k permutacím na obecné množině M. Počet inverzí a tedy i signum a paritu takové permutace stanovíme tak, že očíslujeme prvky v M a stanovíme paritu odpovídající permutace na množině I_n. Vzniká ovšem otázka, zda potom parita nezávisí na volbě očíslování.

Příklad. V našem příkladu s králíky můžeme prvky množiny M (kotce) očíslovat i jinak, například

1	3
2	4

Páteční permutace p potom má jen dvě inverze



oproti čtyřem v původním očíslování. Parita ovšem zůstává sudá.

Tvrzení. *Parita a signum permutace $s \in S(M)$ nezávisí na očíslování prvků množiny M.*

Důkaz. Očíslování prvků množiny M je vlastně bijekce

$$I_n \xrightarrow{u} M, \quad i \mapsto u_i \in M,$$

taková, že $M = \{ u_1, u_2, \ldots, u_n \}$. Buď s permutace na množině M. Buď $s^u \in S_n$ permutace, která při očíslování u odpovídá permutaci s. Máme

$$s^u = u^{-1} \circ s \circ u : \quad I_n \xrightarrow{u} M \xrightarrow{s} M \xrightarrow{u^{-1}} I_n.$$

[Vskutku, prvek s číslem i se při permutaci u zobrazí na prvek s číslem $s^u(i)$. To ale znamená, že $u(s^u(i)) = s(u(i))$ pro každé číslo $i \in I_n$, a tedy $u \circ s^u = s \circ u$; odtud $s^u = u^{-1} \circ s \circ u$.]

Parita permutace $s : M \to M$ v očíslování u pak je $|s^u| = |u^{-1} \circ s \circ u|$, parita téže permutace v jiném očíslování $v : I_n \to M$ je $|s^v| = |v^{-1} \circ s \circ v|$. Snadno najdeme vztah mezi s^v a s^u:

$$\begin{aligned} s^v &= v^{-1} \circ s \circ v \\ &= v^{-1} \circ u \circ u^{-1} \circ s \circ u \circ u^{-1} \circ v \\ &= v^{-1} \circ u \circ s^u \circ u^{-1} \circ v \\ &= (v^{-1} \circ u) \circ s^u \circ (v^{-1} \circ u)^{-1}. \end{aligned}$$

Přitom zobrazení $v^{-1} \circ u : I_n \to I_n$ je bijekce, a tedy permutace na I_n, a proto můžeme použít známý vztah $|p \circ q| = |p| + |q|$. Dostaneme

$$|s^v| = |v^{-1} \circ u| + |s^u| + |(v^{-1} \circ u)^{-1}| = |v^{-1} \circ u| + |s^u| + |v^{-1} \circ u| = |s^u|,$$

což se mělo dokázat.

Nejjednodušší netriviální permutace jsou transpozice.

Definice. *Transpozice* je permutace, při níž se vymění dva prvky a ostatní zůstanou na místě.

Cvičení. Ukažte, že libovolná transpozice má lichou paritu.

Problém k řešení. Ukažte, že libovolná permutace je složením konečného počtu transpozic; přitom sudá (lichá) permutace je složením sudého (lichého) počtu transpozic.

Parity permutací se používá při některých důkazech neexistence či nemožnosti.

Cvičení. V tabulce o 4×4 políčkách se pohybuje 15 kostek a jedna díra. Je dovoleno přesunout kostku na místo díry, pokud s ní sousedí. Ukažte, že z počátečního rozestavení Z nelze dojít k rozestavení K, je-li

$Z =$

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

$K =$

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

Návod: 1) Jednotlivé pozice v tabulce označujme dvojicemi (i, j), $i = 1, \ldots, 4$, $j = 1, \ldots, 4$. Buď $M = \{1, 2, 3, 4\} \times \{1, 2, 3, 4\}$ množina všech pozic. Přesouváním kostek vytváříme permutace na množině M. Rozestavení Z považujme za identickou permutaci. Dokažte, že každý tah ve shodě s pravidly je transpozicí.

2) Zaveďme zobrazení $d : S(M) \to \{0, 1\}$ předpisem: Je-li při permutaci s díra na pozici $(i, j) \in M$, pak $d(s) = [i + j]_2$. Dokažte, že pro každou permutaci s dosaženou ve shodě s pravidly platí

$$|s| = d(s)$$

[předpokládáme, že díra původně stojí na pozici $(4, 4)$, takže $d(\mathrm{id}) = 0$].

3) Nakonec ukažte, že $|K| \neq d(K)$.

Cvičení. Z pohledu matematika, Rubikova kostka sestává z 20 krychliček, rozložených ve vrcholech krychle (8 vrcholových krychliček) a ve středech hran krychle (12 hranových krychliček). Je dovoleno otáčet jednotlivými stěnami krychle. Ukažte, že při dovolené manipulaci s Rubikovou kostkou nelze vyměnit mezi sebou dva vrcholy tak, aby všechny ostatní krychličky zůstaly na místě. (K obarvení nepřihlížíme.)

Návod: Jelikož se při manipulaci s kostkou nemísí vrcholové a hranové krychličky, jde o současně prováděné permutace na množině V vrcholových krychliček a na množině H hranových krychliček. Ukažte, že otočení jednou stěnou je permutace liché parity jak na V, tak na H. Ukažte, že během dovolené manipulace s kostkou jsou parita permutace na V a parita permutace na H stále stejné.

Cvičení. (a) Ukažte, že na n-prvkové množině je $n!$ permutací.

(b) Je-li $n > 1$, pak právě polovina z nich je sudých a polovina je lichých. Dokažte.

Návod: (a) Indukcí vzhledem k n. (b) Složení s libovolnou pevně zvolenou transpozicí dává bijekci mezi množinou sudých a množinou lichých permutací.