Grupa permutací

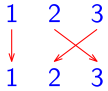
Definice: *Permutace* na množině $\{1, 2, \ldots, n\}$ je bijektivní zobrazení $p : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$.

Permutace může být popsána tabulkou,

i	1	2	3
$p(i)$	1	3	2

zkráceně jen 2. řádkem $(1, 3, 2)$,

pomocí bipartitního grafu,



podle grafu jeho cyklů $1 \circlearrowleft \; 2 \rightleftarrows 3$, jejich seznamem $(1)(2, 3)$,

nebo pomocí tzv. *permutační matice* $\boldsymbol{P}$

kde $(\boldsymbol{P})_{ij} = \begin{cases} 1 & \text{když } p(i) = j \\ 0 & \text{jinak} \end{cases}$ $\qquad \boldsymbol{P} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$

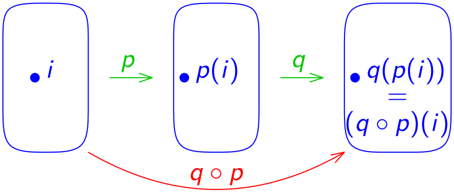
Pozorování: Pro matice $\boldsymbol{A}$ a $\boldsymbol{P}$ odpovídajících řádů, $\boldsymbol{PA}$ zamíchá řádky $\boldsymbol{A}$ podle p, zatímco $\boldsymbol{AP}$ mění pořadí sloupců:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 7 & 8 & 9 \\ 4 & 5 & 6 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \\ 4 & 6 & 5 \\ 7 & 9 & 8 \end{pmatrix}$$

Grupa permutací

Definice: *Permutace* na množině $\{1, 2, \ldots, n\}$ je bijektivní zobrazení $p : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$.

Pozorování: Množina S_n všech permutací na n prvcích s operací skládání $\circ$ tvoří *symetrickou grupu* $(S_n, \circ)$.
Zápis skládání: $(q \circ p)(i) = q(p(i))$.

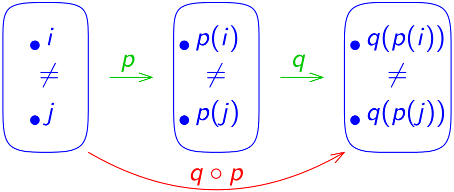


Grupa permutací

Definice: *Permutace* na množině $\{1, 2, \ldots, n\}$ je bijektivní zobrazení $p : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$.

Pozorování: Množina S_n všech permutací na n prvcích s operací skládání $\circ$ tvoří *symetrickou grupu* $(S_n, \circ)$.
Zápis skládání: $(q \circ p)(i) = q(p(i))$.

Důkaz: Složení dvou permutací je permutace:
$i \neq j \Rightarrow p(i) \neq p(j) \Rightarrow q(p(i)) \neq q(p(j))$ . . . $q \circ p$ je prosté.

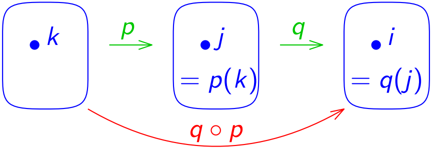


Grupa permutací

Definice: *Permutace* na množině $\{1, 2, \ldots, n\}$ je bijektivní zobrazení $p : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$.

Pozorování: Množina S_n všech permutací na n prvcích s operací skládání $\circ$ tvoří *symetrickou grupu* $(S_n, \circ)$.
Zápis skládání: $(q \circ p)(i) = q(p(i))$.

Důkaz: Složení dvou permutací je permutace:
$i \neq j \Rightarrow p(i) \neq p(j) \Rightarrow q(p(i)) \neq q(p(j))$ . . . $q \circ p$ je prosté.
$(\forall i\ \exists j : q(j) = i) \wedge (\forall j\ \exists k : p(k) = j) \Rightarrow (\forall i\ \exists k : q(p(k)) = i)$
. . . $q \circ p$ je „na“.



$(q \circ p)(k) = q(p(k)) = q(j) = i$

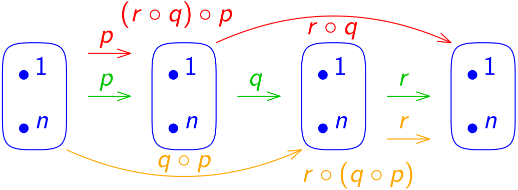
Grupa permutací

Definice: *Permutace* na množině $\{1, 2, \ldots, n\}$ je bijektivní zobrazení $p : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$.

Pozorování: Množina S_n všech permutací na n prvcích s operací skládání $\circ$ tvoří *symetrickou grupu* $(\mathrm{S}_n, \circ)$.
Zápis skládání: $(q \circ p)(i) = q(p(i))$.

Důkaz: Složení dvou permutací je permutace:
$i \neq j \Rightarrow p(i) \neq p(j) \Rightarrow q(p(i)) \neq q(p(j))$ … $q \circ p$ je prosté.
$(\forall i\ \exists j : q(j) = i) \wedge (\forall j\ \exists k : p(k) = j) \Rightarrow (\forall i\ \exists k : q(p(k)) = i)$
… $q \circ p$ je „na“.

Skládání je asociativní: $(r \circ q) \circ p = r \circ (q \circ p)$.



$((r \circ q) \circ p)(i)$

$= r(q(p(i))) =$

$(r \circ (q \circ p))(i)$

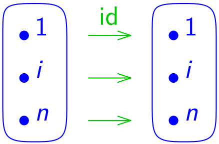
Grupa permutací

Definice: *Permutace* na množině $\{1, 2, \ldots, n\}$ je bijektivní zobrazení $p : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$.

Pozorování: Množina S_n všech permutací na n prvcích s operací skládání $\circ$ tvoří *symetrickou grupu* $(\mathsf{S}_n, \circ)$.
Zápis skládání: $(q \circ p)(i) = q(p(i))$.

Důkaz: Složení dvou permutací je permutace:
$i \neq j \Rightarrow p(i) \neq p(j) \Rightarrow q(p(i)) \neq q(p(j))$ ... $q \circ p$ je prosté.
$(\forall i\ \exists j : q(j) = i) \wedge (\forall j\ \exists k : p(k) = j) \Rightarrow (\forall i\ \exists k : q(p(k)) = i)$
... $q \circ p$ je „na“.
Skládání je asociativní: $(r \circ q) \circ p = r \circ (q \circ p)$.

Identita $\mathrm{id} \in \mathsf{S}_n$ daná $\forall i : \mathrm{id}(i) = i$, je neutrální prvek.



Grupa permutací

Definice: *Permutace* na množině $\{1, 2, \dots, n\}$ je bijektivní zobrazení $p : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$.

Pozorování: Množina S_n všech permutací na n prvcích s operací skládání $\circ$ tvoří *symetrickou grupu* $(\mathrm{S}_n, \circ)$.
Zápis skládání: $(q \circ p)(i) = q(p(i))$.

Důkaz: Složení dvou permutací je permutace:
$i \neq j \Rightarrow p(i) \neq p(j) \Rightarrow q(p(i)) \neq q(p(j))$ $\quad\dots$ $q \circ p$ je prosté.
$(\forall i\ \exists j : q(j) = i) \wedge (\forall j\ \exists k : p(k) = j) \Rightarrow (\forall i\ \exists k : q(p(k)) = i)$
$\dots$ $q \circ p$ je „na“.
Skládání je asociativní: $(r \circ q) \circ p = r \circ (q \circ p)$.

Identita $\mathrm{id} \in \mathrm{S}_n$ daná $\forall i : \mathrm{id}(i) = i$, je neutrální prvek.

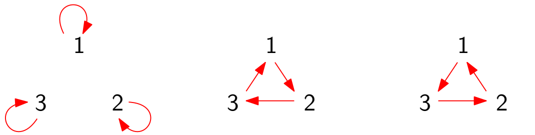
Inverzní permutace se získá obrácením šipky:
$p(i) = j \Leftrightarrow p^{-1}(j) = i$.

$$\boxed{\bullet\, i} \underset{p^{-1}}{\overset{p}{\rightleftarrows}} \boxed{\bullet\, j}$$

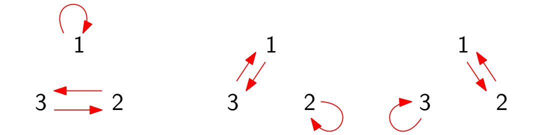
Grupa S_3

Nosná množina:

$$\{(1,2,3),(1,3,2),(3,2,1),(2,1,3),(2,3,1),(3,1,2)\} =$$
$$\{ \quad \mathrm{id} \quad , \quad p_1 \quad , \quad p_2 \quad , \quad p_3 \quad , \quad r_+ \quad , \quad r_- \quad \}$$



$\mathrm{id} = (1,2,3)$ $\quad r_+ = (2,3,1)$ $\quad r_- = (3,1,2)$



$p_1 = (1,3,2)$ $\quad p_2 = (3,2,1)$ $\quad p_3 = (2,1,3)$

$r_{+/-}$ ... vzestupná/sestupná *rotace*

p_i ... permutace s *pevným bodem i*

Grupa S_3

Nosná množina:

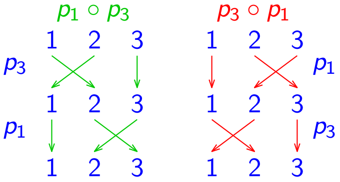
$$\{(1,2,3),(1,3,2),(3,2,1),(2,1,3),(2,3,1),(3,1,2)\} =$$
$$\{\quad \mathrm{id} \quad , \quad p_1 \quad , \quad p_2 \quad , \quad p_3 \quad , \quad r_+ \quad , \quad r_- \quad \}$$

Operace skládání:

$\circ$	id	p_1	p_2	p_3	r_+	r_-
id	id	p_1	p_2	p_3	r_+	r_-
p_1	p_1	id	r_+	r_-	p_2	p_3
p_2	p_2	r_-	id	r_+	p_3	p_1
p_3	p_3	r_+	r_-	id	p_1	p_2
r_+	r_+	p_3	p_1	p_2	r_-	id
r_-	r_-	p_2	p_3	p_1	id	r_+

Inverzní prvky:

p	id	p_1	p_2	p_3	r_+	r_-
p^{-1}	id	p_1	p_2	p_3	r_-	r_+



Skládání *není* komutativní: $p_1 \circ p_3 = r_- \neq r_+ = p_3 \circ p_1$

$(1,3,2) \circ (2,1,3) = (3,1,2) \neq (2,3,1) = (2,1,3) \circ (1,3,2)$.

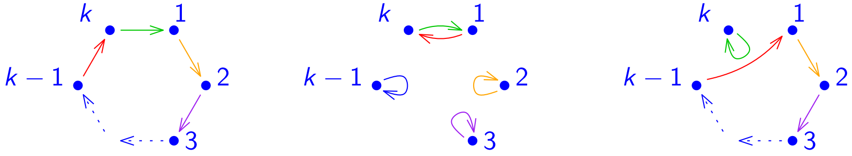
Vlastnosti permutací

Definice: *Pevný bod* je $i : p(i) = i$, t.j. triviální cyklus délky 1.

Definice: *Transpozice* má pouze jeden netriviální cyklus o délce 2.

Pozorování: Jakoukoliv permutaci lze rozložit na transpozice.

Důkaz: Cyklus $(1, \dots, k)$ lze rozložit např. podle:
$$(1, 2, \dots, k) = (1, k) \circ (1, 2, \dots, k-1) = (1, k) \circ (1, k-1) \circ \dots \circ (1, 2)$$



$(1, 2, \dots, k) \quad = \quad (1, k) \quad \circ \quad (1, 2, \dots, k-1)$

Vlastnosti permutací

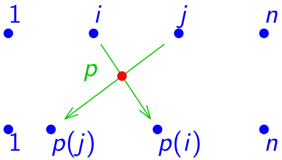
Definice: *Pevný bod* je $i : p(i) = i$, t.j. triviální cyklus délky 1.

Definice: *Transpozice* má pouze jeden netriviální cyklus o délce 2.

Pozorování: Jakoukoliv permutaci lze rozložit na transpozice.

Důkaz: Cyklus $(1, \ldots, k)$ lze rozložit např. podle:
$(1, 2, \ldots, k) = (1, k) \circ (1, 2, \ldots, k-1) = (1, k) \circ (1, k-1) \circ \cdots \circ (1, 2)$

Definice: *Inverze* v p je dvojice $(i, j) : i < j$ a $p(i) > p(j)$.



Vlastnosti permutací

Definice: *Pevný bod* je $i : p(i) = i$, t.j. triviální cyklus délky 1.

Definice: *Transpozice* má pouze jeden netriviální cyklus o délce 2.

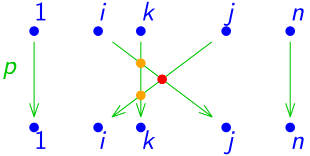
Pozorování: Jakoukoliv permutaci lze rozložit na transpozice.

Důkaz: Cyklus $(1, \ldots, k)$ lze rozložit např. podle:
$(1, 2, \ldots, k) = (1, k) \circ (1, 2, \ldots, k-1) = (1, k) \circ (1, k-1) \circ \cdots \circ (1, 2)$

Definice: *Inverze* v p je dvojice $(i, j) : i < j$ a $p(i) > p(j)$.

Definice: *Znaménko* permutace p je $\mathrm{sgn}(p) = (-1)^{\#\text{inverzí } p}$.
Permutace s kladným znaménkem jsou *sudé*; se záporným *liché*.

Pozorování: Každá transpozice (i, j) má záporné znaménko.



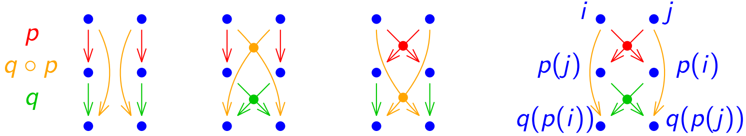
$\#$ inverzí $= 2(j - i - 1) + 1$

Znaménko složené permutace

Věta: Pro libovolné $p, q \in \mathrm{S}_n : \mathrm{sgn}(q \circ p) = \mathrm{sgn}(p)\,\mathrm{sgn}(q)$.

Důkaz: $\#$inverzí $(q \circ p) = \#$inverzí $p \;+\; \#$inverzí $q \;-$

$$- \; 2|\{(i,j) : i < j \wedge p(i) > p(j) \wedge q(p(i)) < q(p(j))\}|$$



inverze v $q \circ p$ odpovídá inverzi v p nebo v q

inverze v p a q se navzájem vyruší

Důsledky:

$\mathrm{sgn}(p^{-1}) = \mathrm{sgn}(p)$,

. . . neboť $\mathrm{sgn}(p)\,\mathrm{sgn}(p^{-1}) = \mathrm{sgn}(p^{-1} \circ p) = \mathrm{sgn}(\mathrm{id}) = 1$

$\mathrm{sgn}(p) = (-1)^{\#\text{transpozic libovolného rozkladu } p \text{ na transpozice}}$

$\mathrm{sgn}(p) = (-1)^{\#\text{sudých cyklů } p}$

. . . *sudé* cykly se rozloží na *lichý* počet transpozic.

Kvíz — řešení

Je-li u některých otázek více možností správných, vyberte všechny.

1. Kolik je permutací z S_n, které mají dané obrazy dvou prvků?
   a) $(n-2)!$ b) $\frac{1}{2}(n-1)!$ c) $(n-1)!$ d) n^{n-2}
2. Pravda nebo lež?
   Každá permutační matice řádu n umocněná na n-tou dá $\mathbf{I}_n$.
3. Pravda nebo lež? Je-li $\boldsymbol{P}$ permutační matice pro π, pak součin $\boldsymbol{AP}$ přerovná sloupce matice $\boldsymbol{A}$ podle permutace π^{-1}.
4. Mějme permutaci se třemi cykly délek 1, 3 a 5 a její rozklad na transpozice. Kolik členů může mít tento rozklad?
   a) 2 b) 3 c) 6 d) 9 e) 10 f) 15 g) 100 h) 9!
5. Je-li $\mathrm{sgn}(p) = 1$ a $\mathrm{sgn}(q) = -1$, pak $p \circ q$ má alespoň jeden:
   a) pevný bod b) cyklus délky dvě c) lichý cyklus
   d) sudý cyklus e) sudý cyklus a alespoň jeden lichý cyklus
6. Pravda nebo lež?
   Na Rubikově dvanáctistěnu nelze regulérními tahy vyměnit pozice dvou rohových kostek a ostatní nechat na místě.

Komentář k řešení kvízu

1. Třetí prvek má $n-2$ možných obrazů, čtvrtý $n-3$, atd.
2. Už pro ukázku $\boldsymbol{P}$ k permutaci $(1,3,2)$ platí $\boldsymbol{P}^3 = \boldsymbol{P} \neq \mathbf{I}_3$.
3. Záměna sloupců v $\boldsymbol{A}$ podle π^{-1} odpovídá záměně řádků v $\boldsymbol{A}^T$ a je dáno vztahem $(\boldsymbol{P}_{\pi^{-1}}\boldsymbol{A}^T)^T = \boldsymbol{A}\boldsymbol{P}^T_{\pi^{-1}} = \boldsymbol{A}\boldsymbol{P}^{-1}_{\pi^{-1}} = \boldsymbol{A}\boldsymbol{P}_\pi$.
$\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}\begin{pmatrix}1&2&3\\4&5&6\\7&8&9\end{pmatrix} = \begin{pmatrix}4&5&6\\7&8&9\\1&2&3\end{pmatrix}$, $\begin{pmatrix}1&2&3\\4&5&6\\7&8&9\end{pmatrix}\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix} = \begin{pmatrix}3&1&2\\6&4&5\\9&7&8\end{pmatrix}$
4. Cykly délky 3, resp. 5 vyžadují alespoň 2, resp. 4 transpozice. Rozklad lze prodloužit o sudý počet členů opakováním téže transpozice. Parita ovšem musí být zachována.
5. Protože $\operatorname{sgn}(p \circ q) = -1$, má $p \circ q$ lichý počet sudých cyklů. Ostatní neplatí např. pro $p = \mathrm{id}$ a $q = p \circ q = (2,3,4,1)$.
6. Každý tah odpovídá permutaci 20 rohových kostek. Každá má jediný netriviální cyklus délky 5, a tudíž i kladné znaménko. Výměna dvou rohových kostek je transpozice. Má záporné znaménko a nelze ji složit z permutací s kladnými znaménky.

Otázky k porozumění tématu přednášky

- Jaký je vztah transpozice permutační matice a její inverze?
- Lze každou permutaci umocnit tak, že dostaneme identitu?
- Lze v důkazu skládání permutací nahradit ověření vlastnosti, že složené zobrazení je surjektivní, jiným argumentem?
- Je složení dvou bijekcí na nekonečné množině opět bijekce?
- Lze pro každou permutaci $p \neq \mathrm{id}$ najít q takovou, aby $p \circ q \neq q \circ p$?
- Uvažme geometrické transformace čtverce (osové souměrnosti, rotace apod.) reprezentované permutacemi vrcholů.
  Má některá záporné znaménko? Jak je tomu u krychle?
- Platí, že znaménko permutace p je kladné, právě když p je druhou mocninou nějaké permutace q, čili $p = q \circ q$?