

Symetrická grupa  $S_n$  (grupa permutací)

$S_n =$  grupa  $\forall$  permutací  $n$ -prvkové množiny - prvky  $1, \dots, n$  uspořádané do určitého očíslování

Pak  $n$ -prvková permutace lze zapsat jako  $\begin{pmatrix} 1 & 2 & \dots & n \\ p_1 & p_2 & \dots & p_n \end{pmatrix}$  kde  $p_i$  je číslo určitého objektu, který byl v  $i$ -tém místě

• Máme identickou permutaci (žádné přestěhování)  $e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$

inverzní permutaci  $g = \begin{pmatrix} 1 & 2 & \dots & n \\ p_1 & p_2 & \dots & p_n \end{pmatrix} \rightarrow g^{-1} = \begin{pmatrix} p_1 & \dots & p_n \\ 1 & \dots & n \end{pmatrix}$   $g g^{-1} = e$

neboť složením dvou permutací dostaneme jinou permutaci  $g_1 = \begin{pmatrix} 1 & 2 & \dots & n \\ p_1 & \dots & p_n \end{pmatrix}, g_2 = \begin{pmatrix} p_1 & \dots & p_n \\ q_1 & \dots & q_n \end{pmatrix} \Rightarrow g_2 g_1 = \begin{pmatrix} 1 & \dots & n \\ q_1 & \dots & q_n \end{pmatrix}$

• Řád grupy permutací je  $n!$

• Cayleyho teorema: Každá konečná grupa řádu  $n$  je izomorfní nějaké podgrupě symetrické grupy  $S_n$ . (každému  $h \in G$  přiřadí se  $(g_1, g_2, \dots, g_n)$   $(h g_1, h g_2, \dots, h g_n)$ )  
 $\Rightarrow$  v principu by šlo stačit se zabývat pouze touto grupou, ale prakticky je to příliš těžkopádné

• Cykly - hledáme  $\forall$  permutaci řetězce, např.  $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 1 & 5 & 3 \end{pmatrix}$  obsahuje cykly  $(1 \rightarrow 2 \rightarrow 4 \rightarrow 1) = (124)$   
 $(3 \rightarrow 6 \rightarrow 3) = (36)$   
 tj.  $g$  lze zapsat jako  $g = (124)(36) = (241)(36) = (36)(124)$   
 tj. nezáleží na pořadí cyklů, ani na tom, který prvek cyklus začne

• Transpozice = permutace obsahující jen jeden cyklus délky 2, tj.  $g = (ij)$   
 - každý cyklus (permutace) lze vyjádřit jako součet transpozic  
 např.  $(123) = (13)(12)$  a obecně  $(12 \dots n) = (1n) \dots (13)(12)$  -  $n-1$  transpozic

Polybiův důkaz

že daná permutace se vždy rozloží na sudý (lichý) počet transpozic  
 - jde-li permutace rozložit na sudý počet transpozic  $\rightarrow$  sudá permutace  
 na lichý počet  $\rightarrow$  lichá permutace

• Třídy sdružených prvků - všechny permutace, které mají stejný počet cyklů stejné délky tvoří třídu sdruž. prvků

necht'  $g = \begin{pmatrix} 1 & \dots & n \\ p_1 & \dots & p_n \end{pmatrix}$  a  $h = \begin{pmatrix} 1 & \dots & n \\ q_1 & \dots & q_n \end{pmatrix}$   $h^{-1} = \begin{pmatrix} q_1 & \dots & q_n \\ 1 & \dots & n \end{pmatrix}$   $h g h^{-1}$  zde se přehazují celé sloupce!  
 pokud  $p_i = j$ , pak  $j$  nahore bude nahr.  $q_j$  a  $p_i = j$  dole též  $q_j = q p_i$   
 $\Rightarrow$  zachovávat se struktura cyklů, neboť permutuje-li horní a dolní řádek stejně, nemá to vliv na délku cyklů  
 např.  $g = (12)(345)$   $h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}$   
 $h g h^{-1} = (43)(152) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 1 & 5 \end{pmatrix}$   $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$

# Cvičení: Grupa permutací

1) Dokažte pravidlo pro rozklad cyklu (nebo obráceně složením cyklu, které mají jeden společný prvek)

$$(*) \quad (a \dots bcd \dots e) = (a \dots bc)(cd \dots e)$$

Řešení: ~~První~~ Přijm' rozepsání 2 permutací na pravé straně

$$\begin{pmatrix} a \dots bcd \dots e \\ \dots bcd \dots ea \end{pmatrix} \begin{pmatrix} a \dots bcd \dots e \\ a \dots b d \dots ec \end{pmatrix} = (a \dots bcd \dots e) \quad \checkmark$$

2) Dokažte že lib. permutaci lze ~~středně~~ zapsat jako součin transpozic typu  $(12), (23), \dots, (n-1n)$ , tj. typu  $(i \ i+1)$ ,  $i=1, \dots, n-1$

Řešení: 1) Pomocí pravidla (\*) lze libovolný cyklus rozložit na transpozice

(např.  $(2415) = (24)(41)(15) = (24)(14)(15)$ )

takže stačí najít rozklad transpozice  $(j \ j+k)$ , kde  $k > 1$  a  $j+k \leq n$

To lze ~~indukcí~~ postupně takto:  $(j \ j+k) = (j \ j+k-1)(j+k-1 \ j+k)$

neboť jde o sdružení, tj. záměnu  $j+k-1$  a  $j$

a pokračujeme s  $(j \ j+k-1), (j \ j+k-2) \dots$  až dostaneme  $k$  transpozic  $(j \ j+1)$ .

Všimněme si ještě, že budeme dostávat vedle sebe ~~transpozice~~ <sup>např.</sup> transpozice

$$\# \quad (j+k-2 \ j+k-1)(j \ j+k-2)(j+k-1 \ j+k)(j \ j+k-2)(j+k-2 \ j+k)$$

$\Rightarrow$

$$(j \ j+k) = (j \ j+1)(j+1 \ j+2) \dots (j+k-1 \ j+k)(j+k-2 \ j+k-1)(j+k-3 \ j+k-2) \dots (j \ j+1)$$

(např.  $(25) = (23)(34)(45)(34)(23) = (2345)(432)$ )

2) z příkladu je patrné, že stačí ukázat, že  $(j \ j+k) = (j \ j+1 \dots \ j+k)(j+k-1 \dots \ j)$

což je zřejmé z rozepsání

$$(j \ j+k) = \left\{ \begin{matrix} 1 \dots j-1 \ j \ j+1 \dots j+k-1 \ j+k \dots n \\ 1 \dots j-1 \ j+k-1 \ j \dots j+k-2 \ j+k \dots n \\ 1 \dots j-1 \ j+k \ j+1 \dots j+k-1 \ j \dots n \end{matrix} \right\}$$

3) ~~Dokažte~~ <sup>Určete</sup> počet prvků třídy sdružení prvků, která je charakterizována rozkladem  $(v) = (1^{v_1} 2^{v_2} \dots n^{v_n})$ .

Řešení

$$\# C_{(v)} = \frac{n!}{1^{v_1} v_1! 2^{v_2} v_2! \dots n^{v_n} v_n!}$$

neboť cykly můžou být permutovány  $\Rightarrow$  faktory  $v_i!$  a též cykly  $\Rightarrow i^{v_i}$

a speciálně pro grupu  $S_n$ .

## Cvičení: Grupa permutací (pokračování)

				T <sub>n</sub>
3) pro S <sub>4</sub> : cykly	(1 <sup>4</sup> )	$\rightarrow \#C_{(1^4)} = \frac{4!}{1^4 4!} = 1$	- jednotkový prvek	E
	(1 <sup>2</sup> 2)	$\#C_{(1^2 2)} = \frac{4!}{1^2 2! 2! 1!} = 6$	(12), (13), (14), (23), (24), (34)	6σ <sub>2</sub>
	(1 <sup>1</sup> 3 <sup>1</sup> )	$\#C_{(13)} = \frac{4!}{3} = 8$	(123), (124), (134), (213), (214), (234) (314), (324)	8C <sub>3</sub>
	(2 <sup>2</sup> )	$\#C_{(2^2)} = \frac{4!}{2^2 2!} = 3$	(12)(34), (13)(24), (14)(23)	3S <sub>4</sub>
	(4 <sup>1</sup> )	$\#C_{(4)} = \frac{4!}{4! 1!} = 6$	(1234), (1243), (1324), (1342) (1423), (1432)	6C <sub>2</sub>

4) ~~Ukážte~~ Ukážte, že grupa S<sub>n</sub> je generována 2 permutacemi ~~(12)~~ (12) a (12...n)

Řešení: stačí vygenerovat transpozice (i i+1)

Protože  $(12...n)^{-1} = (12...n)^{n-1}$ , tj. (12...n) generuje svoji inverzi,  
 můžeme postupně z (12) generovat (23), (34) ... pomocí sdružení  
 např.  $(12...n)(34)(12...n)^{-1} = (45) \dots$

obecně libovolný cyklus na délku cyklu je idemita (zřejmě platí)  
 a tedy  $\underbrace{(ab\dots)}_k^{-1} (ab\dots)^{k-1} = (ab\dots)^k = 1$  - jen posun  
 rozepsáním