GRUPY:

- ABSTRAKTNÍ ALGEBRAICKÉ STRUKTURY PRO POPIS SYMETRIÍ
- **GRUPA** JE DVOJICE $(G, \circ)$, KDE G JE MNOŽINA A $\circ : G \times G \to G$ JE BINÁRNÍ OPERACE NA MNOŽINĚ G SPLŇUJÍCÍ:

1) $\forall a, b, c \in G: \; a \circ (b \circ c) = (a \circ b) \circ c$ (**ASOCIATIVITA**)
2) $\exists e \in G \; \forall a \in G: \; e \circ a = a \circ e = a$ (**NEUTRÁLNÍ PRVEK**)
3) $\forall a \in G \; \exists b \in G: \; a \circ b = b \circ a = e$ (**INVERZNÍ PRVEK**)

- **ABELOVOU GRUPOU** JE GRUPA, KTERÁ NAVÍC SPLŇUJE:

4) $\forall a \in G \; \forall b \in G: \; a \circ b = b \circ a$ (**KOMUTATIVITA**)

- JE-LI OPERACÍ $\circ$ SČÍTÁNÍ, PAK NEUTRÁLNÍ PRVEK ZNAČÍME 0 A INVERZNÍ $-a$
- JE-LI OPERACÍ $\circ$ NÁSOBENÍ, PAK NEUTRÁLNÍ PRVEK ZNAČÍME 1 A INVERZNÍ a^{-1}

- PŘÍKLADY (VÍCE V PREZENTACI):

$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot), (\mathbb{Z}_m = \{0, \dots, m-1\}, \underset{\text{sčítání modulo } m}{+}),$

$(\mathbb{R}^{m \times n}, +), \dots$

TVRZENÍ 5.1 (ZÁKLADNÍ VLASTNOSTI GRUP): PRVKY GRUPY $(G, \circ)$ SPLŇUJÍ NÁSLEDUJÍCÍ VLASTNOSTI:

1) $a \circ c = b \circ c \Rightarrow a = b$ (**KRÁCENÍ**)
2) NEUTRÁLNÍ PRVEK e JE URČEN JEDNOZNAČNĚ
3) PRO KAŽDÉ $a \in G$ JE JEHO INVERZNÍ PRVEK URČEN JEDNOZNAČNĚ
4) ROVNICE $a \circ x = b$ MÁ JEDNO ŘEŠENÍ PRO KAŽDÉ $a, b \in G$
5) $(a^{-1})^{-1} = a$ PRO KAŽDÉ $a \in G$
6) $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$ PRO KAŽDÉ $a, b \in G$

- DŮKAZ (ČÁSTI):

1) $a \circ c = b \circ c \overset{\text{asociativita}}{\Rightarrow} a \circ (c \circ c^{-1}) = b \circ (c \circ c^{-1}) \overset{\text{inverzní prvek}}{\Rightarrow} a \circ e = b \circ e \overset{\text{neutrální prvek}}{\Rightarrow} \underline{\underline{a = b}}$
2) NEUTRÁLNÍ PRVKY $e_1, e_2 \Rightarrow e_1 \overset{\text{neutrální prvek}}{=} e_1 \circ e_2 = e_2 \Rightarrow \underline{\underline{e_1 = e_2}}$
3) INVERZNÍ PRVKY a_1, a_2 K $a \Rightarrow a_1 \circ a \overset{\text{inverzní prvek}}{=} e = a_2 \circ a \overset{\text{krácení}}{\Rightarrow} \underline{\underline{a_1 = a_2}}$
4) VYNÁSOBENÍ ROVNICE $a \circ x = b$ ZLEVA PRVKEM a^{-1} DÁVÁ $x = a^{-1} \circ b$. PO DOSAZENÍ JE ROVNOST SPLNĚNA $\boxtimes$

- **PODGRUPA** grupy $(G,\circ)$ je grupa $(H,\diamond)$ taková, že platí $H \subseteq G$ a pro všechna $a,b \in H$ platí $a \diamond b = a \circ b$
  - nebolí v H platí **uzavřenost** $(a,b \in H \Rightarrow a \diamond b \in H)$, existence neutrálního prvku $(e \in H)$ a inverzního prvku $(a \in H \Rightarrow a^{-1} \in H)$
  - značíme $(H,\diamond) \leq (G,\circ)$

- Příklady:
  - **triviální podgrupy** grupy $(G,\circ)$: $(G,\circ)$ a $(\{e\},\circ)$
  - $(\mathbb{N},+) \not\leq (\mathbb{Z},+) \leq (\mathbb{Q},+) \leq (\mathbb{R},+) \leq (\mathbb{C},+)$

- **PERMUTACE**:
  - zobrazení je **vzájemně jednoznačné** (**bijekce**), je-li prosté a na
  - **permutace** na konečné množině X je vzájemně jednoznačné zobrazení $X \to X$
  - S_n = množina všech permutací na $X = \{1,\dots,n\}$
  - možné zápisy permutací:

    1) **tabulkou** (nahoře vzory, dole obrazy): $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix}$

    2) **grafem** (šipka vede ze vzoru do obrazu):

    3) **rozložením na cykly** (v závorce je obrazem prvku jeho následník):

$$p = (1,2)(3)(4,5,6) = (1,2)(4,5,6)$$

- **identita** **id** je permutace zobrazující každý prvek sám na sebe
- **transpozice** je permutace (i,j), která prohazuje 2 prvky
  - tedy permutace s jedním cyklem, který má 2 prvky

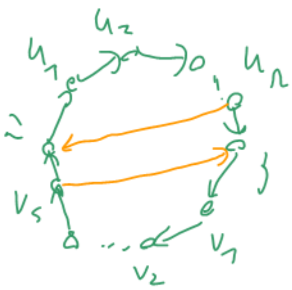
- INVERZNÍ PERMUTACE p^{-1} K PERMUTACI p JE DANÁ PŘEDPISEM
  $p^{-1}(i)=j$, POKUD $p(j)=i$
  - PŘÍKLADY:
    $(i,j)^{-1}=(i,j)$, $(i,j,k)^{-1}=(k,j,i)$
- PRO $p,q\in S_n$ JE SLOŽENÁ PERMUTACE $p\circ q$ DANÁ PŘEDPISEM $(p\circ q)(i)=p(q(i))$
  - PŘÍKLADY:
    $p\circ id=p=id\circ p$, $p\circ p^{-1}=id=p^{-1}\circ p$
    $p=(1,2)$, $q=(1,3,2)$ NA S_3, PAK $p\circ q=(1,3)$ A $q\circ p=(2,3)$

$\Rightarrow$ SKLÁDÁNÍ PERMUTACÍ JE ASOCIATIVNÍ, ALE NE NUTNĚ KOMUTATIVNÍ

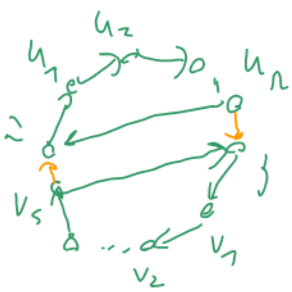
- POKUD SE PERMUTACE $p\in S_n$ SKLÁDÁ Z k CYKLŮ, PAK JEJÍM ZNAMÉNKEM JE ČÍSLO $sgn(p)=(-1)^{n-k}$
- VĚTA 5.2 (O ZNAMÉNKU SLOŽENÍ PERMUTACE S TRANSPOZICÍ):
  BUĎ $p\in S_n$ PERMUTACE A $t=(i,j)\in S_n$ TRANSPOZICE, PAK PLATÍ

$$sgn(p)=-sgn(t\circ p)=-sgn(p\circ t)$$

- DŮKAZ:
  - UKÁŽEME ROVNOST $sgn(p)=-sgn(t\circ p)$, DRUHÁ ANALOGICKY
  - ROZLIŠÍME 2 PŘÍPADY:



1) i A j JSOU VE STEJNÉM CYKLU $(i,u_1,\dots,u_r,j,v_1,\dots,v_s)$:
   PAK $(i,j)\circ(i,u_1,\dots,u_r,j,v_1,\dots,v_s)=(i,u_1,\dots,u_r)(j,v_1,\dots,v_s)$
   A POČET CYKLŮ SE ZVÝŠÍ O 1



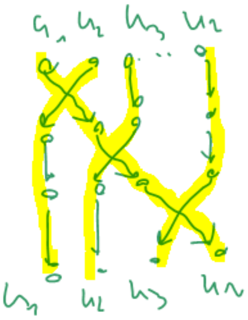
2) i A j JSOU V RŮZNÝCH CYKLECH $(i,u_1,\dots,u_r)$ A $(j,v_1,\dots,v_s)$
   PAK $(i,j)\circ(i,u_1,\dots,u_r)(j,v_1,\dots,v_s)=(i,u_1,\dots,u_r,j,v_1,\dots,v_s)$
   A POČET CYKLŮ SE SNÍŽÍ O 1

$\boxtimes$

- **VĚTA 5.3:**

  KAŽDOU PERMUTACI LZE ROZLOŽIT NA SJEDNOCENÍ TRANSPOZIC

  - **DŮKAZ:**



    - POSTUPNĚ NA TRANSPOZICE ROZLOŽÍME VŠECHNY CYKLY
    - ROZLOŽENÍ CYKLU $(u_1, \dots, u_n) = (u_1, u_2) \circ (u_2, u_3) \circ \dots \circ (u_{n-1}, u_n)$ $\otimes$

    - Z VĚT 5.2 A 5.3 DOSTÁVÁME PAK OKAMŽITĚ NĚKOLIK DŮSLEDKŮ

- **DŮSLEDEK 5.4:**

  PLATÍ $sgn(p) = (-1)^n$, KDE n JE POČET TRANSPOZIC V ROZKLADU p

- **DŮSLEDEK 5.5:**

  PRO $p, q \in S_n$ PLATÍ $sgn(p \circ q) = sgn(p) \cdot sgn(q)$

- **DŮSLEDEK 5.6:**

  PRO $p \in S_n$ PLATÍ $sgn(p) = sgn(p^{-1})$

- MNOŽINA PERMUTACÍ S_n S OPERACÍ SKLÁDÁNÍ TVOŘÍ ZÁKLADNÍ **SYMETRICKOU GRUPU**
  - KAŽDÁ GRUPA JE IZOMORFNÍ NĚJAKÉ PODGRUPĚ SYMETRICKÉ GRUPY