Kapitola 6 – Symetrické grupy

6.1. Symetrická grupa množiny

6.1.1. DEFINICE
Nechť M je množina. Permutací množiny M rozumíme každou bijekci množiny M na množinu M. Množinu všech permutací množiny M budeme značit $S(M)$.
Tedy $S(M)=\{\pi : M \to M \mid \pi \text{ je permutace}\}$.

6.1.2. VĚTA
Množina $S(M)$ s operací skládání zobrazení je grupa.
Důkaz: Nechť π, $\rho \in S(M)$. Protože složení bijekcí je bijekce (viz 1.1.8.(c)), je $\pi\rho \in S(M)$.
Nechť π, ρ, $\sigma \in S(M)$. Pak $(\pi\rho)\sigma=\pi(\rho\sigma)$ na základě 1.1.3.(a). Zřejmě $id_M \in S(M)$ a id_M je neutrální prvek vzhledem k operaci skládání zobrazení. Konečně, nechť $\pi \in S(M)$.
Pak π^{-1} je bijekce (viz 1.1.8.(d)), $\pi^{-1} \in S(M)$ a π^{-1} je inverzní prvek k prvku π.

6.1.3. DEFINICE
Grupa $S(M)$ se nazývá symetrická grupa množiny M.
Nechť $n \in \mathbb{N}$. Místo $S(\{1, 2, \ldots, n\})$ píšeme S_n a hovoříme o symetrické grupě n prvků.

6.1.4. VĚTA
Nechť M je množina. Platí:
Grupa $S(M)$ je komutativní právě tehdy, když množina M má nejvýše 2 prvky.
specielně: S_1, S_2 jsou komutativní, S_3, S_4, S_5, S_6, … jsou nekomutativní.
Důkaz:
$\Rightarrow$: Předpokládejme, že M má aspoň tři prvky a, b, c. Definujme $\pi : M \to M$ a $\rho : M \to M$ takto:

$\pi(a)=a$	$\rho(a)=b$
$\pi(b)=c$	$\rho(b)=a$
$\pi(c)=b$	$\rho(c)=c$
$\pi(x)=x$	$\rho(x)=x$ pro $x \in M-\{a, b, c\}$.

Zřejmě π, $\rho \in S(M)$. Dále $(\pi\rho)(a)=\rho(\pi(a))=\rho(a)=b$, $(\rho\pi)(a)=\pi(\rho(a))=\pi(b)=c$.
Vídíme, že $\pi\rho \neq \rho\pi$. Takže grupa $S(M)$ není komutativní.
$\Leftarrow$: Jestliže $M=\emptyset$, pak $S(M)=\{\emptyset\}$. Jestliže M je jednoprvková, pak $S(M)$ je jednoprvková. Jestliže M je dvouprvková, pak $S(M)$ je dvouprvková. Stačí si uvědomit, že každá jednoprvková a dvouprvková grupa je komutativní.

6.1.5. VĚTA
Nechť $n \in \mathbb{N}$. Grupa S_n je konečná a má $n!$ prvků.
Důkaz: přenecháváme čtenáři.

6.1.6. OZNAČENÍ
Nechť $n \in \mathbb{N}$, $\pi \in S_n$. Někdy budeme psát $\pi=\begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix}$.

6.1.7. DEFINICE
Nechť $n \in \mathbb{N}$, i, $j \in \{1, 2, \ldots, n\}$, $i \neq j$. Definujeme permutaci $(i \leftrightarrow j) \in S_n$ takto:
$(i \leftrightarrow j)(i)=j$
$(i \leftrightarrow j)(j)=i$
$(i \leftrightarrow j)(k)=k$ pro každé $k \in \{1, 2, \ldots, n\}-\{i, j\}$
Permutace $(i \leftrightarrow j)$ se nazývá transpozice prvků i a j.

6.1.8. VĚTA

Nechť $n\in\mathbb{N}$, $n\geq 2$, $\pi\in S_n$. Platí:

existují transpozice $\tau_1, \tau_2, \ldots, \tau_k\in S_n$ ($k\in\mathbb{N}$) tak, že $\pi=\tau_1\tau_2\cdots\tau_k$.

Důkaz: Indukcí vzhledem k n:

(I) $n=2$

$$S_n=\left\{\begin{pmatrix}1&2\\1&2\end{pmatrix},\begin{pmatrix}1&2\\2&1\end{pmatrix}\right\}$$

$$\begin{pmatrix}1&2\\1&2\end{pmatrix}=(1\leftrightarrow 2)(1\leftrightarrow 2)$$

$$\begin{pmatrix}1&2\\2&1\end{pmatrix}=(1\leftrightarrow 2)$$

(II) $n\geq 3$

Rozlišíme 2 případy:

(1) $\pi(n)=n$

Definujeme $\rho\in S_{n-1}$:

$\rho(1)=\pi(1), \rho(2)=\pi(2), \cdots, \rho(n-1)=\pi(n-1)$. Podle indukčního předpokladu existují transpozice $\sigma_1, \ldots, \sigma_k\in S_{n-1}$ ($k\in\mathbb{N}$) tak, že $\rho=\sigma_1\cdots\sigma_k$.

Definujeme $\tau_1, \ldots, \tau_k\in S_n$ takto:

$\tau_i(1)=\sigma_i(1), \ldots, \tau_i(n-1)=\sigma_i(n-1)$, $\tau_i(n)=n$ pro $i=1, \ldots, k$.

Zřejmě $\tau_1, \ldots, \tau_k\in S_n$ jsou transpozice a $\pi=\tau_1\cdots\tau_k$.

(2) $\pi(n)=i<n$

Položme $\pi'=\pi\cdot(i\leftrightarrow n)$. Pak $\pi'(n)=n$, takže podle již diskutovaného případu (I) existují transpozice $\tau_1, \ldots, \tau_k\in S_n$, ($k\in\mathbb{N}$) tak, že $\pi'=\tau_1\cdots\tau_k$. Pak

$\pi=\pi(i\leftrightarrow n)(i\leftrightarrow n)=\pi'(i\leftrightarrow n)=\tau_1\cdots\tau_k(i\leftrightarrow n)$.

6.2. **Sudé a liché permutace**

6.2.1. DEFINICE

Nechť $n\in\mathbb{N}$, $\pi\in S_n$, $(i, j)\in\{1, 2, \ldots, n\}^2$:

Dvojice (i, j) se nazývá inverze v permutaci π, platí-li:

(I) $i<j$

(II) $\pi(i)>\pi(j)$

π se nazývá sudá permutace, je-li počet všech inverzí v permutaci π sudý.

π se nazává lichá permutace, je-li počet všech inverzí v permutaci π lichý.

Dále definujeme

$$Sg(\pi)=\begin{cases}1 & \text{je-li } \pi \text{ sudá}\\ -1 & \text{je-li } \pi \text{ lichá}\end{cases}$$

6.2.2. TVRZENÍ

Nechť $n\in\mathbb{N}$, $\tau\in S_n$, τ je transpozice. Platí: $Sg(\tau)=-1$.

Důkaz: $\tau=(i\leftrightarrow j)$ pro jistá $i, j\in\{1, \ldots, n\}$, $i\neq j$. Lze předpokládat, že $i<j$.

$$\tau=(i\leftrightarrow j)=\begin{pmatrix}1&\cdots&i&\cdots&j&\cdots&n\\1&\cdots&j&\cdots&i&\cdots&n\end{pmatrix}.$$

Inverze v permutaci τ:

$(i, i+1), (i, i+2), \ldots, (i, i+(j-i-1))$

$(i+1, j), (i+2, j), \ldots, (i+(j-i-1), j)$

(i, j)

Celkový počet inverzí v permutaci τ je $2\cdot(j-i-1)+1$. Číslo $2\cdot(j-i-1)+1$ je liché, takže $Sg(\tau)=-1$.

6.2.3. VĚTA

Necht $n\in\mathbb{N}$, π, $\tau\in S_n$, τ je transpozice. Platí $Sg(\tau\pi)=-Sg(\pi)$.

Důkaz: $\tau=(i\leftrightarrow j)$ pro jistá i, $j\in\{1,\ldots,n\}$, $i\neq j$. Lze předpokládat, že $i<j$. Postupujme indukcí vzhledem k $j-i$:

(α) $j-i=1$

$$\pi=\begin{pmatrix}1 & \ldots & i\ j & \ldots & n\\ \pi(1) & \ldots & \pi(i)\pi(j) & \ldots & \pi(n)\end{pmatrix}$$

$$(i\leftrightarrow j)\pi=\begin{pmatrix}1 & \ldots & i\ j & \ldots & n\\ \pi(1) & \ldots & \pi(j)\pi(i) & \ldots & \pi(n)\end{pmatrix}$$

Je zřejmé, že v permutaci $(i\leftrightarrow j)\pi$ je o jednu inverzi více, než v permutaci π (když $(i,\ j)$ není inverze v π), nebo o jednu inverzi méně než v permutaci π (když $(i,\ j)$ je inverze v π). Každopádně platí, že $Sg(\tau\pi)=-Sg(\pi)$.

(β) $j-i\geq 2$

$\tau\pi=(i\leftrightarrow j)\pi=(i\leftrightarrow j-1)(j-1\leftrightarrow j)(i\leftrightarrow j-1)\pi$. Podle indukčního předpokladu

$$\begin{aligned}Sg(\tau\pi)&=Sg((i\leftrightarrow j-1)(j-1\leftrightarrow j)(i\leftrightarrow j-1)\pi)\\&=-Sg((j-1\leftrightarrow j)(i\leftrightarrow j-1)\pi)\\&=Sg((i\leftrightarrow j-1)\pi)\\&=-Sg(\pi).\end{aligned}$$

6.2.4. VĚTA

Nechť $n\in\mathbb{N}$, π, $\rho\in S_n$. Platí: $Sg(\pi\rho)=Sg(\pi)\cdot Sg(\rho)$.

Důkaz: Pokud $n=1$, je tvrzení zřejmé, neboť $\pi=\rho=id$.

Nechť $n\geq 2$. Podle 6.1.8. existují transpozice $\tau_1,\ldots,\tau_k\in S_n$, $k\in\mathbb{N}$ tak, že $\pi=\tau_1\tau_2\cdots\tau_k$. Aplikací věty 6.2.3. snadno dostaneme

$Sg(\pi\rho)=Sg(\tau_1\tau_2\cdots\tau_k\rho)=-Sg(\tau_2\cdots\tau_k\rho)=\cdots(-1)^k\cdot Sg(\rho)$.

Ovšem $Sg(\pi)=Sg(\tau_1\tau_2\cdots\tau_k id)=-Sg(\tau_2\cdots\tau_k id)=\cdots=(-1)^k\cdot Sg(id)=(-1)^k\cdot 1=(-1)^k$, takže $Sg(\pi\rho)=Sg(\pi)\cdot Sg(\rho)$.

6.3. **Alternující grupa**

6.3.1. OZNAČENÍ

Nechť $n\in\mathbb{N}$. Klademe $A_n=\{\tau\in S_n|Sg(\pi)=1\}$.

6.3.2. TVRZENÍ

Nechť $n\in\mathbb{N}$. Platí: A_n je podgrupa grupy S_n.

Důkaz:

(a) Chceme: $id\in A_n$. To však platí, neboť $Sg(id)=1$.

(b) Nechť π, $\rho\in A_n$. Chceme: $\pi\rho\in A_n$. Tedy chceme: $Sg(\pi\rho)=1$. Podle 6.2.4. máme $Sg(\pi\rho)=Sg(\pi)\cdot Sg(\rho)=1\cdot 1=1$.

(c) Nechť $\pi\in A_n$. Chceme: $\pi^{-1}\in A_n$. Tedy chceme: $Sg(\pi^{-1})=1$. Víme, že $\pi\pi^{-1}=id$, tedy $Sg(\pi)\cdot Sg(\pi^{-1})=Sg(id)=1$, což dává $Sg(\pi^{-1})=1$, protože $Sg(\pi)=1$.

Grupa A_n se nazývá alternující grupa n prvků.

6.3.3. TVRZENÍ

Nechť $n\in\mathbb{N}$, $n\geq 2$. Platí: $card(A_n)=\frac{1}{2}card(S_n)$ (tedy $card(A_n)=\frac{n!}{2}$).

Důkaz: Označme $L_n=\{\pi\in S_n|Sg(\pi)=-1\}$. Je $S_n=A_n\cup L_n$, $A_n\cap L_n=\emptyset$, takže $card\ S_n=card(A_n)+card(L_n)$. Stačí tedy sestrojit bijekci $\varphi: A_n\to L_n$. Pro $\pi\in A_n$

definujeme $\varphi(\pi)=(1\leftrightarrow 2)\cdot\pi$. Podle 6.2.4. a 6.2.2. je
$Sg(\varphi(\pi))=Sg((1\leftrightarrow 2)\pi)=Sg((1\leftrightarrow 2))\cdot Sg(\pi)=-1\cdot 1=-1$.
Vidíme, že $\varphi(\pi)\in L_n$. Tudíž φ je korektně definované zobrazení množiny A_n do množiny L_n . Zbývá ukázat, že φ je bijekce. Zdůvodnění přenecháváme čtenáři.