Algebra I

Radan Kučera, jarní semestr 2011

Literatura:
J. Rosický: **Algebra**, skriptum PřF MU, 4. vydání, Brno 2002 (nebo později), str. 7–102.

Operace na množině, grupoid

Definice. Nechť G je množina. Libovolné zobrazení $G \times G \to G$ se nazývá (binární) **operace** na množině G.

Označení. Operace budeme značit symbolem $\cdot$ (případně $+$, $\circ$, $\bullet$ apod.), obraz dvojice $[a, b] \in G \times G$ v operaci $\cdot$ symbolem $a \cdot b$.

Definice. Operace $\cdot$ na množině G se nazývá

- **komutativní**, jestliže $\forall a, b \in G: a \cdot b = b \cdot a$;
- **asociativní**, jestliže $\forall a, b, c \in G: a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Definice. Množina G spolu s operací $\cdot$ na G se nazývá **grupoid**, označujeme jej $(G, \cdot)$, nebo jen G, bude-li z kontextu jasné, jakou operaci máme na mysli.

Definice. Grupoid $(G, \cdot)$ se nazývá

- **komutativní**, jestliže $\cdot$ je komutativní operace na G;
- **asociativní** (neboli **pologrupa**), jestliže $\cdot$ je asociativní operace na G.

Neutrální prvek, inverzní prvky, grupa

Definice. Nechť $(G, \cdot)$ je grupoid. Prvek $e \in G$ se nazývá **neutrální prvek** (neboli **jednotkový prvek**) tohoto grupoidu, jestliže $\forall a \in G: e \cdot a = a \cdot e = a$.

Věta. Každý grupoid má nejvýše jeden neutrální prvek. Důkaz.

Definice. Nechť $(G, \cdot)$ grupoid s neutrálním prvkem e a nechť je pevně dáno $a \in G$. Prvek $b \in G$ se nazývá **inverzním prvkem** k prvku a (v grupoidu G), jestliže platí $a \cdot b = b \cdot a = e$.

Věta. V libovolné pologrupě s neutrálním prvkem ke každému prvku existuje nejvýše jeden prvek inverzní.

Definice. Grupoid G se nazývá **grupa**, jestliže

- G je pologrupa (tj. asociativní grupoid),
- G má neutrální prvek,
- ke každému prvku $a \in G$ existuje v G prvek inverzní.

Označení. V grupě $(G, \cdot)$ tedy ke každému prvku $a \in G$ existuje právě jeden prvek inverzní, značíme jej a^{-1}.

Definice. Je-li $(G, \cdot)$ grupa a je-li navíc operace $\cdot$ komutativní, hovoříme o **komutativní grupě**.

Definice. Grupa $(G, \cdot)$ se nazývá **triviální**, má-li množina G jediný prvek, tj. $G = \{e\}$. (Tento jediný prvek e je pak nutně neutrální, neboť musí platit $e \cdot e = e$.)

Příklad. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ jsou komutativní grupy; $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ jsou komutativní grupy, kde $\mathbb{Q}^* = \mathbb{Q} - \{0\}$, $\mathbb{R}^* = \mathbb{R} - \{0\}$, $\mathbb{C}^* = \mathbb{C} - \{0\}$.

Příklad. Nechť R značí kteroukoli z číselných množin $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, pak pro libovolné $m, n \in \mathbb{N}$ definujeme $M_{n,m}(R)$ jako množinu všech matic typu $n \times m$ s prvky z R. Pak $(M_{n,m}(R), +)$ je komutativní grupa (zde $+$ značí sčítání matic).
Naopak $(M_{n,n}(R), \cdot)$, kde $\cdot$ značí násobení matic, je pologrupa s neutrálním prvkem, ale grupa to není. Je-li R kterákoli z číselných množin $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, označme $\mathcal{GL}_n(R)$ množinu všech regulárních matic typu $n \times n$ s prvky z R (tj. matic s nenulovým determinantem). Pak $(\mathcal{GL}_n(R), \cdot)$ je grupa, která není komutativní, je-li $n \geq 2$.

Permutace

Příklad. Nechť X je množina, symbolem X^X značíme množinu všech zobrazení $X \to X$, symbol $\circ$ značí skládání zobrazení. Připomeňme, že pro $f, g \in X^X$ je definováno

$$(f \circ g)(x) = f(g(x)) \qquad \text{pro libovolné } x \in X.$$

Pak $(X^X, \circ)$ je pologrupa s neutrálním prvkem, ale grupa to není.

Definice. **Permutací** na množině X rozumíme libovolnou bijekci $X \to X$. Množinu všech permutací na množině X značíme $\mathcal{S}(X)$. Pokud $X = \{1, 2, \ldots, n\}$, píšeme místo $\mathcal{S}(X)$ stručně jen $\mathcal{S}_n$.

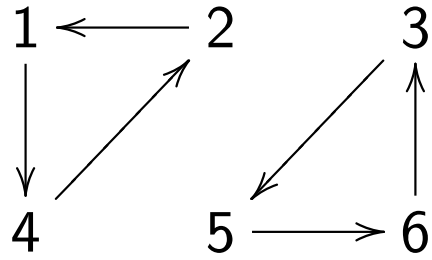
Příklad. $(\mathcal{S}(X), \circ)$ je grupa, která není komutativní, má-li X alespoň tři prvky.

Jak označovat prvky grupy $\mathcal{S}_n$?

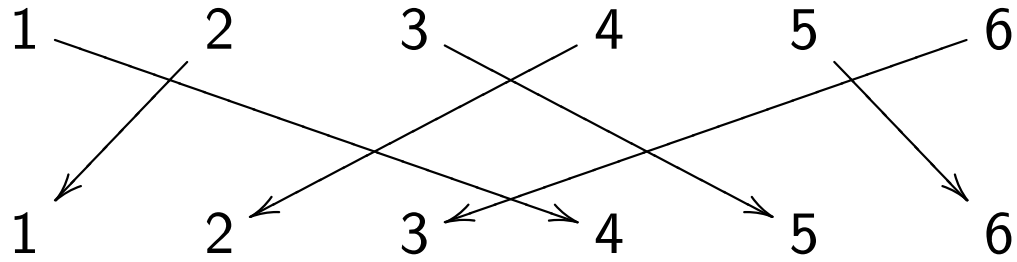
dvouřádkovou maticí

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 6 & 3 \end{pmatrix}$$

orientovaným grafem



anebo schématem



Definice. Nechť $i_1, \ldots, i_k$ jsou různé prvky množiny $\{1, 2, \ldots, n\}$, přičemž $k \geq 2$. Permutaci z $\mathcal{S}_n$ takovou, že

$$i_1 \mapsto i_2, \quad i_2 \mapsto i_3, \quad i_3 \mapsto i_4, \quad \ldots, \quad i_{k-1} \mapsto i_k, \quad i_k \mapsto i_1,$$

přičemž pro všechny prvky $a \in \{1, 2, \ldots, n\}$, $a \notin \{i_1, \ldots, i_k\}$ platí $a \mapsto a$, nazýváme **cyklem délky** k a značíme $(i_1, \ldots, i_k)$. Cykly délky 2 se nazývají **transpozice**.

Definice. Cykly $(i_1, \ldots, i_k), (j_1, \ldots, j_r) \in \mathcal{S}_n$ se nazývají **nezávislé**, jsou-li množiny $\{i_1, \ldots, i_k\}$ a $\{j_1, \ldots, j_r\}$ disjunktní (tj. mají-li prázdný průnik).

Věta. *Každou neidentickou permutaci $f \in \mathcal{S}_n$ lze napsat jako složení několika nezávislých cyklů, a to jednoznačně až na jejich pořadí.*

Věta. *Nechť $n > 1$, pak každou permutaci $f \in \mathcal{S}_n$ lze napsat jako složení několika transpozic.* Důkaz.

Definice. Nechť $f \in \mathcal{S}_n$. Řekneme, že uspořádaná dvojice $[i, j]$ je **inverze** permutace f, jestliže $1 \leq i < j \leq n$ a platí $f(i) > f(j)$. Permutace f se nazývá **sudá** nebo **lichá** podle toho, má-li sudý nebo lichý počet inverzí. Paritu $p(f)$ permutace f definujeme:

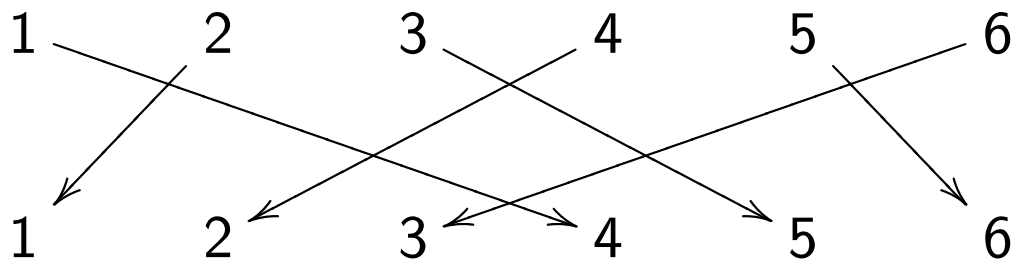
$$p(f) = \begin{cases} 1 & \text{je-li } f \text{ sudá,} \\ -1 & \text{je-li } f \text{ lichá.} \end{cases}$$

Jak zjistit paritu permutace $f \in \mathcal{S}_n$?

Je-li f dána dvouřádkovou maticí, spočítáme, kolikrát ve spodním řádku „je menší číslo předběhnuto větším“:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 6 & 3 \end{pmatrix}$$

$4 > 1,\ \ 4 > 2,\ \ 4 > 3,\ \ 5 > 2,\ \ 5 > 3,\ \ 6 > 3$:
šest inverzí – sudá permutace.
Je-li f dána schématem



spočítáme, kolikrát se protínají šipky:
šest průsečíků - šest inverzí - sudá permutace.

A co parita permutace $f \in \mathcal{S}_n$ zapsané jako složení cyklů?

Věta. *Pro libovolné $f, g \in \mathcal{S}_n$ platí*

$$p(f \circ g) = p(f) \cdot p(g).$$

Jinými slovy: složením libovolných dvou permutací stejné parity dostaneme sudou permutaci, kdežto složením libovolných dvou permutací různé parity dostaneme lichou permutaci. Důkaz.

Důsledek. *Složení sudého počtu transpozic je sudá permutace, složení lichého počtu transpozic je lichá permutace.* Důkaz. Pokračování.

Důsledek. *Cyklus liché délky je sudá permutace a cyklus sudé délky je lichá permutace.*

Důsledek. *Neidentická permutace je sudá, právě když ve svém rozkladu na složení nezávislých cyklů má sudý počet cyklů sudé délky. Je tedy lichá, právě když v tomto rozkladu má lichý počet cyklů sudé délky.* Příklady. Ještě jeden.