8. Permutace

In: Otakar Borůvka (author): Základy teorie grupoidů a grup. (Czech). Praha: Nakladatelství Československé akademie věd, 1962. pp. 60--68.

Persistent URL: http://dml.cz/dmlcz/401435

8. Permutace

V této kapitole se budeme zabývat prostými zobrazeními konečných množin na sebe. Taková zobrazení mají v algebře a zejména v teorii grup důležitou úlohu.

8.1. Definice

Permutací množiny G rozumíme prosté zobrazení množiny G na sebe (**6.6**).

V tomto odstavci se omezíme na úvahy o permutacích *konečné* množiny.

Nechť tedy G značí libovolnou množinu o konečném počtu n ($\geqq 1$) prvků. Z předpokladu, že množina G je konečná, vyplývá, že každé prosté zobrazení $\mathfrak{p}$ množiny G do sebe je její permutace (**6.10**.2).

Prvky množiny G si myslíme označeny písmeny $a, b, \ldots, m$. Ke každé permutaci $\mathfrak{p}$ množiny G můžeme pak jednoznačně přiřadit symbol tvaru

$$\begin{pmatrix} a & b & \ldots & m \\ a^* & b^* & \ldots & m^* \end{pmatrix},$$

přičemž $a^*, b^*, \ldots, m^*$ jsou písmena, jimiž jsou označeny prvky $\mathfrak{p}a, \mathfrak{p}b, \ldots, \mathfrak{p}m$; pod každým písmenem v prvním řádku stojí tedy v druhém řádku písmeno označující obraz toho prvku v permutaci $\mathfrak{p}$. Protože $\mathfrak{p}G = G$, jsou $a^*, b^*, \ldots, m^*$ opět písmena $a, b, \ldots, m$ napsaná v jistém pořadí. Naopak, každým symbolem toho tvaru, v němž $a^*, b^*, \ldots, m^*$ jsou opět písmena $a, b, \ldots, m$ napsaná v jistém pořadí, je dána jistá permutace množiny G, která každý prvek v prvním řádku zobrazí na prvek stojící pod ním v druhém řádku. Všimněme si, že tutéž permutaci $\mathfrak{p}$ můžeme podobně vyjádřit i jinými symboly, z nichž každý obdržíme, když písmena $a, b, \ldots, m$ napíšeme v prvním řádku v nějakém jiném pořadí a pod každé z nich napíšeme totéž písmeno jako dříve. Zejména je ovšem identické zobrazení množiny G permutací množiny G a nazývá se *identická permutace*; její symbol je $\begin{pmatrix} a & b & \ldots & m \\ a & b & \ldots & m \end{pmatrix}$ nebo kterýkoli z jiných symbolů, jako např. $\begin{pmatrix} b & a & \ldots & m \\ b & a & \ldots & m \end{pmatrix}$, atp.

8.2. Příklady permutací

Uvedeme nejprve několik jednoduchých příkladů permutací množin o $n = 1, 2, 3, 4$ prvcích.

1. $n = 1$. Nechť G značí množinu, která se skládá z jediného bodu a v rovině. V tomto případě existuje ovšem právě jenom jedna permutace množiny G, a to permutace identická $\begin{pmatrix} a \\ a \end{pmatrix}$.

2. $n = 2$. Nechť G značí množinu skládající se z některých dvou bodů v rovině: a, b. Když body a, b otočíme v rovině v jednom anebo v druhém směru okolo středu úsečky o koncových bodech a, b o nějaký úhel α, pak bod a přejde do jistého bodu a' a bod b do b', a máme prosté zobrazení množiny G na množinu $\{a', b'\}$. Když α měří $0°$, $180°$, je množina $\{a', b'\}$ identická s množinou G, a máme tyto permutace množiny G: $\begin{pmatrix} a & b \\ a & b \end{pmatrix}$, $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$.

3. $n = 3$. Nechť G značí množinu tří bodů v rovině: a, b, c, tvořících vrcholy rovnostranného trojúhelníka. Když body a, b, c otočíme v rovině v jednom anebo v druhém směru okolo středu trojúhelníka o vrcholech a, b, c o nějaký úhel α, pak bod a přejde do jistého bodu a', bod b do b' a bod c do c', a máme prosté zobrazení množiny G na množinu $\{a', b', c'\}$. Když α měří $0°$, $120°$, $240°$, pak je množina $\{a', b', c'\}$ identická s množinou G, a máme tyto permutace množiny G: $\begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}$, $\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$, $\begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$. Další permutace množiny G obdržíme, když k bodům a, b, c přiřadíme body souměrně položené vzhledem k některé ose souměrnosti trojúhelníka o vrcholech a, b, c. Tento trojúhelník má celkem tři osy souměrnosti, z nichž každá prochází jedním vrcholem a půlí protější stranu. Přiřadíme-li ke každému bodu a, b, c bod souměrně položený vzhledem k ose souměrnosti, která prochází vrcholem a, obdržíme permutaci $\begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$; podobně obdržíme další permutace $\begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}$, $\begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$. Našli jsme tedy v tomto případě celkem 6 permutací, a to:

$$\begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}, \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}, \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}, \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}, \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}.$$

4. $n = 4$. Nechť nyní G značí množinu čtyř bodů v rovině, a, b, c, d, tvořících vrcholy čtverce. Otočíme-li body a, b, c, d v rovině v jednom anebo ve druhém směru okolo středu čtverce o vrcholech a, b, c, d o nějaký úhel α, pak opět obdržíme prosté zobrazení množiny G na množinu jistých bodů v rovině a', b', c', d', a je-li $\alpha = 0°$, $90°$, $180°$, $270°$, obdržíme tyto permutace množiny G:

$$\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ d & a & b & c \end{pmatrix}.$$

Další permutace množiny G opět najdeme, když k bodům a, b, c, d přiřadíme body

souměrně položené vzhledem k některé ose souměrnosti čtverce o vrcholech a, b, c, d. Tento čtverec má celkem čtyři osy souměrnosti, z nichž dvě procházejí vždy dvěma protějšími vrcholy a dvě půlí vždy dvě protější strany. Přiřadíme-li ke každému bodu a, b, c, d bod souměrně položený vzhledem k ose souměrnosti, která prochází vrcholy a, c, obdržíme permutaci $\begin{pmatrix} a & b & c & d \\ a & d & c & b \end{pmatrix}$; podobně obdržíme další permutace $\begin{pmatrix} a & b & c & d \\ c & b & a & d \end{pmatrix}$, $\begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}$, $\begin{pmatrix} a & b & c & d \\ d & c & b & a \end{pmatrix}$. Našli jsme tedy v tomto případě 8 permutací, a to:

$$\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ d & a & b & c \end{pmatrix},$$
$$\begin{pmatrix} a & b & c & d \\ a & d & c & b \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ c & b & a & d \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ d & c & b & a \end{pmatrix}.$$

8.3. Počet permutací

Vraťme se nyní k úvahám o permutacích na libovolné množině G, která má n ($\geqq 1$) prvků $a, b, \ldots, m$.

Kolik je celkem permutací množiny G? Abychom na tuto otázku odpověděli, uvažme, že v libovolné permutaci $\mathfrak{p}$ množiny G se zobrazí prvek a na jistý prvek $\mathfrak{p}a$ množiny G; když $n > 1$, zobrazí se dále prvek b na jistý prvek $\mathfrak{p}b$, různý od $\mathfrak{p}a$, a podobně se zobrazí prvek c na jistý prvek $\mathfrak{p}c$, různý od $\mathfrak{p}a$, $\mathfrak{p}b$, atd., a prvek m se zobrazí na jistý prvek $\mathfrak{p}m$, různý od předcházejících prvků $\mathfrak{p}a$, $\mathfrak{p}b$, $\mathfrak{p}c$, ... Naopak, když k prvku a přiřadíme kterýkoli prvek $a^* \in G$ a dále, v případě $n > 1$, k prvku b kterýkoli prvek $b^* \in G$, různý od a^*, a podobně k prvku c kterýkoli prvek $c^* \in G$, různý od a^*, b^*, atd., a k prvku m prvek $m^* \in G$, různý od předcházejících prvků a^*, b^*, c^*, ..., obdržíme jistou permutaci $\begin{pmatrix} a & b & c & \ldots & m \\ a^* & b^* & c^* & \ldots & m^* \end{pmatrix}$ množiny G. Permutací množiny G je tedy právě tolik, kolik je možností takových přiřazení. Avšak k prvku a můžeme přiřadit některý prvek $a^* \in G$ celkem n způsoby, a to tak, že jednou k němu přiřadíme prvek a, po druhé prvek b, atd., a po n-té prvek m; v případě $n > 1$ můžeme dále přiřadit k prvku b některý prvek $b^* \in G$, různý od a^*, celkem $n - 1$ způsoby a podobně k prvku c některý prvek $c^* \in G$, různý od a^*, b^*, celkem $n - 2$ způsoby, atd., a k prvku m můžeme přiřadit prvek $m^* \in G$, různý od a^*, b^*, c^*, ..., právě jenom jedním způsobem. Vychází tedy celkem $n(n-1)(n-2)\ldots 1$ možností a odpověď na hořejší otázku zní, že *je celkem* $1 \cdot 2 \cdot 3 \ldots n$ *permutací množiny* G. Obvykle se toto číslo označuje symbolem $n!$. Např. každá množina o $n = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ prvcích má celkem $n! = 1, 2, 6, 24, 120, 720, 5040, 40\,320, 362\,880, 3\,628\,800$ permutací. Permutace, které jsme našli v hořejších příkladech 1, 2, 3 bodů v rovině jsou tedy všechny, kdežto v případě 4 bodů v rovině existuje vedle nalezených 8 permutací ještě $2 \cdot 8$ dalších.

8.4. Vlastnosti permutací

1. *Inverzní permutace.* Uvažujme nyní o vlastnostech permutací podrobněji. Nechť $\mathfrak{p}$ značí libovolnou permutaci množiny G. Protože $\mathfrak{p}$ je prosté zobrazení, existuje inverzní permutace $\mathfrak{p}^{-1}$ vzhledem k $\mathfrak{p}$ množiny G. Snadno si ujasníme, že symbol permutace $\mathfrak{p}^{-1}$ obdržíme, když v symbolu permutace $\mathfrak{p}$ vyměníme oba řádky. Např. permutace inverzní vzhledem k hořejším 8 permutacím čtyř bodů v rovině jsou po pořádku tyto:

$$\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ d & a & b & c \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix},$$

$$\begin{pmatrix} a & b & c & d \\ a & d & c & b \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ c & b & a & d \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ d & c & b & a \end{pmatrix}.$$

2. *Invariantní prvky.* Libovolný prvek $x \in G$ se zobrazí v permutaci $\mathfrak{p}$ na jistý prvek $\mathfrak{p}x$, který je nebo není totožný s prvkem x. Nastane-li první případ, $\mathfrak{p}x = x$, pak pravíme, že *permutace* $\mathfrak{p}$ *nechává prvek* x *beze změny*, neboli *že prvek* x *je v permutaci* $\mathfrak{p}$ *invariantní.* Je zřejmé, že permutace $\mathfrak{p}$ a permutace inverzní $\mathfrak{p}^{-1}$ nechávají beze změny tytéž prvky množiny G. Např. hořejší permutace čtyř bodů v rovině nechávají beze změny tyto prvky: a, b, c, d; žádný; žádný; žádný; a, c; b, d; žádný; žádný.

3. *Cyklické permutace.* Libovolný prvek $x \in G$ a permutace $\mathfrak{p}$ jednoznačně určují řadu prvků v G: x, $\mathfrak{p}x$, $\mathfrak{p}(\mathfrak{p}x)$, $\mathfrak{p}(\mathfrak{p}(\mathfrak{p}x))$, ..., v níž každý, druhým počínajíc, je obrazem v permutaci $\mathfrak{p}$ prvku předcházejícího. Místo x, $\mathfrak{p}x$ píšeme někdy $\mathfrak{p}^0x$, $\mathfrak{p}^1x$ a pro stručnost místo $\mathfrak{p}(\mathfrak{p}x)$, $\mathfrak{p}(\mathfrak{p}(\mathfrak{p}x))$, ... píšeme zpravidla $\mathfrak{p}^2x$, $\mathfrak{p}^3x$, ...

Permutace $\mathfrak{p}$ se nazývá *cyklická*, když existuje prvek $x \in G$ a přirozené číslo k takové, že v řadě prvků x, $\mathfrak{p}x$, $\mathfrak{p}^2x$, $\mathfrak{p}^3x$, ..., $\mathfrak{p}^{k-1}x$ nejsou žádné dva prvky totožné, ale obrazem $\mathfrak{p}^kx$ prvku $\mathfrak{p}^{k-1}x$ je opět prvek x, a když mimoto jsou všechny ostatní prvky množiny G, jsou-li jaké, v permutaci $\mathfrak{p}$ invariantní. Podrobněji pak permutaci $\mathfrak{p}$ popisujeme názvem: *cyklická permutace vzhledem k prvkům* x, $\mathfrak{p}x$, $\mathfrak{p}^2x$, ..., $\mathfrak{p}^{k-1}x$.

Uspořádaná skupina prvků x, $\mathfrak{p}x$, $\mathfrak{p}^2x$, ..., $\mathfrak{p}^{k-1}x$ se nazývá *cyklus permutace* $\mathfrak{p}$, podrobněji: *k-členný cyklus* anebo *k-cyklus*. Když zejména $k = n$, tj. když každý prvek množiny G leží v cyklu permutace $\mathfrak{p}$, pravíme, že $\mathfrak{p}$ je *ryzí cyklická permutace.*

Předpokládejme, že permutace $\mathfrak{p}$ je cyklická vzhledem k prvkům x, $\mathfrak{p}x$, $\mathfrak{p}^2x$, ..., $\mathfrak{p}^{k-1}x$. Pak permutaci $\mathfrak{p}$ vyjadřujeme obvykle jednodušším symbolem, a to tím, že písmena označující prvky x, $\mathfrak{p}x$, $\mathfrak{p}^2x$, ..., $\mathfrak{p}^{k-1}x$ napíšeme v tomto pořadí vedle sebe do závorek. Permutace inverzní $\mathfrak{p}^{-1}$ vzhledem k $\mathfrak{p}$ zobrazí každý prvek řady x, $\mathfrak{p}x$, $\mathfrak{p}^2x$, ..., $\mathfrak{p}^{k-1}x$, kromě prvního, na prvek předcházející, prvek x na prvek $\mathfrak{p}^{k-1}x$ a ostatní prvky množiny G, jsou-li jaké, nechává beze změny; permutace $\mathfrak{p}^{-1}$ je tedy cyklická vzhledem k prvkům $\mathfrak{p}^{k-1}x$, ..., $\mathfrak{p}^2x$, $\mathfrak{p}x$, x. Změníme-li popř. označení prvků množiny G tak, že prvek x označíme a, prvek $\mathfrak{p}x$ písmenem b, prvek $\mathfrak{p}^2x$ písmenem c, atd., prvek $\mathfrak{p}^{k-1}x$ písmenem j, a ostatní prvky množiny G, jsou-li jaké, označíme libovolně dalšími písmeny, vypadá zjednodušený symbol permutace $\mathfrak{p}$ takto: $(a, b,$

$c, \ldots, j$). Je zřejmé, že permutaci $\mathfrak{p}$ můžeme rovněž vyjádřit kterýmkoli dalším symbolem $(b, c, \ldots, j, a)$, $(c, \ldots, j, a, b)$, atd., celkem tedy k způsoby. Symbol inverzní permutace $\mathfrak{p}^{-1}$ je pak např. $(j, \ldots, c, b, a)$.

Nejjednodušší cyklické permutace jsou cyklické permutace vzhledem k jedinému prvku; z hořejší definice cyklické permutace plyne, že každá cyklická permutace množiny G vzhledem k jedinému prvku je identická permutace množiny G, takže identickou permutaci množiny G můžeme vyjádřit kterýmkoli symbolem (a), (b), ..., ..., (m).

Každá cyklická permutace množiny G vzhledem ke dvěma prvkům se nazývá *transpozice.*

Např. v hořejších příkladech permutací množiny $n = 1, 2, 3, 4$, bodů v rovině máme tyto cyklické permutace: V případě $n = 1$: (a); v případě $n = 2$: $(a), (a, b)$; v případě $n = 3$: $(a), (a, b), (a, c), (b, c), (a, b, c), (a, c, b)$; v případě $n = 4$: (a), $(a, c), (b, d), (a, b, c, d), (a, d, c, b)$.

4. *Invariantní podmnožiny a rozklady.* Nechť nyní $\mathfrak{p}$ opět značí libovolnou permutaci množiny G. Libovolná neprázdná podmnožina $A \subset G$ se zobrazí v rozšířeném zobrazení $\mathfrak{p}$ na jistou podmnožinu $\mathfrak{p}A \subset G$, která je nebo není částí podmnožiny A. Když nastane první případ $\mathfrak{p}A \subset A$, pak je nutně $\mathfrak{p}A = A$, neboť podle definice částečného zobrazení $\mathfrak{p}_A$ máme $\mathfrak{p}A = \mathfrak{p}_A A$, a protože částečné zobrazení $\mathfrak{p}_A$, jakožto prosté zobrazení konečné množiny A do sebe, je permutací množiny A, máme dále $\mathfrak{p}_A A = A$.

Je-li $\mathfrak{p}A = A$, pravíme, že *permutace* $\mathfrak{p}$ *nechává podmnožinu* A *beze změny*, anebo že *podmnožina* A *je v permutaci* $\mathfrak{p}$ *invariantní.*

Zejména je podmnožina A v permutaci $\mathfrak{p}$ invariantní, když každý její prvek je v $\mathfrak{p}$ invariantní. Je zřejmé, že když permutace $\mathfrak{p}$ nechává podmnožinu A beze změny, pak totéž platí o inverzní permutaci $\mathfrak{p}^{-1}$. Např. hořejší permutace čtyř bodů v rovině nechávají beze změny tyto vlastní podmnožiny v množině bodů a, b, c, d: všechny; žádnou; $\{a, c\}$, $\{b, d\}$; žádnou; $\{a\}$, $\{c\}$, $\{b, d\}$; $\{b\}$, $\{d\}$, $\{a, c\}$; $\{a, b\}$, $\{c, d\}$; $\{a, d\}$, $\{b, c\}$. Všimněme si, že je-li $\mathfrak{p}$ cyklická permutace $(a, b, c, \ldots, j)$, pak každá podmnožina $A \subset G$, která obsahuje prvky $a, b, c, \ldots, j$, je v $\mathfrak{p}$ invariantní a částečná permutace $\mathfrak{p}_A$ je také cyklická a má týž symbol $(a, b, c, \ldots, j)$.

Nechť $\bar{G} = \{\bar{a}, \bar{b}, \ldots, \bar{m}\}$ značí nějaký rozklad množiny G. Když se rozklad $\bar{G}$ vyznačuje tím, že v rozšířeném zobrazení $\mathfrak{p}$ obraz každého prvku v $\bar{G}$ je opět prvkem rozkladu $\bar{G}$, pravíme, že *permutace* $\mathfrak{p}$ *nechává rozklad* $\bar{G}$ *beze změny*, anebo že *rozklad* $\bar{G}$ *je v permutaci* $\mathfrak{p}$ *invariantní.* Snadno si ujasníme, že když permutace $\mathfrak{p}$ nechává rozklad $\bar{G}$ beze změny, pak totéž platí o inverzní permutaci $\mathfrak{p}^{-1}$.

Uvažujme zejména o případu, že každý prvek rozkladu $\bar{G}$ je v permutaci $\mathfrak{p}$ invariantní, takže $\mathfrak{p}\bar{a} = \bar{a}$, $\mathfrak{p}\bar{b} = \bar{b}$, ..., $\mathfrak{p}\bar{m} = \bar{m}$. V tomto případě částečné zobrazení $\mathfrak{p}_{\bar{x}}$, určené permutací $\mathfrak{p}$ každého prvku $\bar{x} \in \bar{G}$ je opět permutací prvku $\bar{x}$. Těmito částečnými permutacemi $\mathfrak{p}_{\bar{a}}, \mathfrak{p}_{\bar{b}}, \ldots, \mathfrak{p}_{\bar{m}}$ je permutace $\mathfrak{p}$ jednoznačně *vytvořena*, a to v tom smyslu, že obraz libovolného prvku $x \in G$ v permutaci $\mathfrak{p}$ je týž jako v částečné permutaci $\mathfrak{p}_{\bar{x}}$ onoho prvku $\bar{x} \in \bar{G}$, v němž prvek x leží. V inverzní permutaci $\mathfrak{p}^{-1}$ je

rovněž každý prvek rozkladu $\bar{G}$ invariantní a permutace $\boldsymbol{p}^{-1}$ je vytvořena inverzními permutacemi $\boldsymbol{p}_{\bar{a}}^{-1}, \boldsymbol{p}_{\bar{b}}^{-1}, \ldots, \boldsymbol{p}_{\bar{m}}^{-1}$. Zvolíme-li naopak na množině G libovolný rozklad $\bar{G} = \{\bar{a}, \bar{b}, \ldots, \bar{m}\}$ a na každém jeho prvku $\bar{x}$ libovolnou permutaci $\boldsymbol{p}_{\bar{x}}$ a definujeme-li na množině G permutaci $\boldsymbol{p}$ tím způsobem, že ke každému prvku $x \in G$ přiřadíme jeho obraz v permutaci $\boldsymbol{p}_{\bar{x}}$ onoho prvku $\bar{x} \in \bar{G}$, v němž prvek x leží, pak každý prvek rozkladu $\bar{G}$ je v permutaci $\boldsymbol{p}$ invariantní a $\boldsymbol{p}_{\bar{a}}, \boldsymbol{p}_{\bar{b}}, \ldots, \boldsymbol{p}_{\bar{m}}$ jsou vytvořující částečné permutace této permutace $\boldsymbol{p}$.

8.5. Vytvoření permutací ryzími cyklickými permutacemi

Nyní ukážeme, že *libovolná permutace $\boldsymbol{p}$ každé množiny G o n ($\geqq 1$) prvcích je vytvořena konečným počtem ryzích cyklických permutací*, jinými slovy, že existuje rozklad $\bar{G} = \{\bar{a}, \bar{b}, \ldots, \bar{m}\}$ množiny G takový, že každý jeho prvek $\bar{a}, \bar{b}, \ldots, \bar{m}$ je v permutaci $\boldsymbol{p}$ invariantní a částečné permutace $\boldsymbol{p}_{\bar{a}}, \boldsymbol{p}_{\bar{b}}, \ldots, \boldsymbol{p}_{\bar{m}}$ jsou ryzí cyklické permutace prvků $\bar{a}, \bar{b}, \ldots, \bar{m}$.

K důkazu použijeme metody úplné indukce.*) Naše tvrzení je správné, když $n = 1$, neboť v tom případě je $\boldsymbol{p}$ identická permutace množiny G a největší rozklad množiny G má onu vlastnost. Zbývá tedy ukázat, že platí-li naše tvrzení o každé množině, která má nejvýše $n - 1$ prvků, kde n značí některé přirozené číslo > 1, pak platí také o každé množině, která má n prvků. Nechť tedy G značí nějakou množinu skládající se z n prvků a $\boldsymbol{p}$ nějakou permutaci množiny G. Nechť dále a značí libovolný prvek v G. Uvažujme o řadě prvků $a, \boldsymbol{p}a, \boldsymbol{p}^2a, \ldots, \boldsymbol{p}^na$ množiny G, z nichž každý následující je obrazem v permutaci $\boldsymbol{p}$ prvku předcházejícího. Těchto prvků je $n + 1$ a odtud plyne, že alespoň jeden prvek se v ní vyskytne alespoň dvakráte. Postupujeme-li tedy v naší řadě od prvního prvku a vždy k prvku následujícímu, přijdeme *po prvé*:

a) k jistému prvku $\boldsymbol{p}^ja$, kde j značí některé číslo $0, \ldots, n - 1$, který se vyznačuje tím, že se mezi prvky $\boldsymbol{p}^{j+1}a, \ldots, \boldsymbol{p}^na$ vyskytne ještě alespoň jednou;

b) k prvku $\boldsymbol{p}^{j+k}a$, kde k je některé číslo $1, \ldots, n - j$, který je totožný s prvkem $\boldsymbol{p}^ja$, takže $\boldsymbol{p}^ja = \boldsymbol{p}^{j+k}a$.

Není-li $\boldsymbol{p}^ja$ hned první prvek a, tj. jestliže $j > 0$, pak se oba prvky $\boldsymbol{p}^{j-1}a, \boldsymbol{p}^{j+k-1}a$ zobrazí v permutaci $\boldsymbol{p}$ na týž prvek $\boldsymbol{p}^ja$ a tedy platí rovnost $\boldsymbol{p}^{j-1}a = \boldsymbol{p}^{j+k-1}a$, neboť $\boldsymbol{p}$

*) Metoda úplné indukce se zakládá na této větě: *Když ke každému přirozenému číslu n je přiřazen nějaký výrok $\boldsymbol{g}n$ a tyto výroky jsou toho druhu, že: 1. výrok $\boldsymbol{g}1$ je správný, 2. pro každé $n > 1$, pro které jsou správné výroky $\boldsymbol{g}1, \ldots, \boldsymbol{g}(n-1)$, je správný i výrok $\boldsymbol{g}n$, pak všechny výroky jsou správné.* Skutečně, v opačném případě jsou nesprávné výroky přiřazeny k jistým přirozeným číslům a jedno z nich, označme je m, je nejmenší. Podle předpokladu 1 je $m > 1$; podle definice čísla m jsou výroky $\boldsymbol{g}1, \ldots, \boldsymbol{g}(m-1)$ správné, kdežto výrok $\boldsymbol{g}m$ je nesprávný, ale to odporuje předpokladu 2.

Podobná věta platí v případě, že jde o výroky přiřazené celým číslům, která jsou větší nebo rovná nějakému celému číslu k.

je zobrazení prosté; ale to není možné, protože prvek $\mathfrak{p}^j a$ se vyznačuje vlastností, že v naší řadě $a, \mathfrak{p}a, \mathfrak{p}^2 a, \ldots, \mathfrak{p}^n a$ není před ním prvku vyskytujícího se pak ještě jednou, kdežto z hořejší rovnosti vyplývá, že takovým prvkem je $\mathfrak{p}^{j-1} a$. Tím je zjištěno, že $j = 0$. Podle definice čísla k máme $\mathfrak{p}^k a = a$, ale žádný prvek $\mathfrak{p}a, \ldots, \mathfrak{p}^{k-1} a$ není prvek a. Jsou-li některé dva z prvků $a, \mathfrak{p}a, \ldots, \mathfrak{p}^{k-1} a$ stejné, tj. platí-li pro některá celá čísla r, s, vyhovující nerovnostem $0 \leqq r < s \leqq k - 1$, rovnost $\mathfrak{p}^r a = \mathfrak{p}^s a$, pak odtud plyne $\mathfrak{p}^{k-s}(\mathfrak{p}^r a) = \mathfrak{p}^{k-s}(\mathfrak{p}^s a)$, tj. $\mathfrak{p}^{k-s+r} a = \mathfrak{p}^k a = a$; tato rovnost ale odporuje tomu, že žádný z prvků $\mathfrak{p}a, \ldots, \mathfrak{p}^{k-1} a$ není prvek a, neboť $1 \leqq k - s + r \leqq k - 1$, a tedy prvek $\mathfrak{p}^{k-s+r} a$ je jedním z nich. Tím je zjištěno, že žádné dva prvky $a, \mathfrak{p}a, \ldots, \ldots, \mathfrak{p}^{k-1} a$ nejsou stejné.

Nechť $\bar{a}$ značí množinu prvků $a, \mathfrak{p}a, \ldots, \mathfrak{p}^{k-1} a$. Vidíme, že podmnožina $\bar{a} \subset G$ je v permutaci $\mathfrak{p}$ invariantní a že částečná permutace $\mathfrak{p}_{\bar{a}}$ je ryzí cyklická permutace této množiny. Jestliže $k = n$, tj. platí-li $\bar{a} = G$, pak $\mathfrak{p}_{\bar{a}} = \mathfrak{p}$ a největší rozklad množiny G má vlastnost, o kterou jde. Uvažujme tedy o případu $k < n$. V tomto případě jsou v množině G kromě prvků $a, \mathfrak{p}a, \ldots, \mathfrak{p}^{k-1} a$ ještě další prvky, jejichž počet je nejvýše $n - 1$: množinu těchto prvků označme H. V částečném zobrazení $\mathfrak{p}_H$ je obraz každého prvku $x \in H$, opět prvek v H, neboť v opačném případě platí rovnost $\mathfrak{p}x = \mathfrak{p}^l a$, kde l značí některé číslo $0, \ldots, k - 1$, a odtud plyne $x = \mathfrak{p}^{l-1} a$, je-li $l > 0$, a $x = \mathfrak{p}^{k-1} a$, je-li $l = 0$; ale to v obou případech odporuje předpokladu $x \in H$. Permutace $\mathfrak{p}_H$ je tedy zobrazení množiny H do sebe, a protože je prosté a množina H má jenom konečný počet prvků, je $\mathfrak{p}_H$ permutace množiny H. Platí-li naše tvrzení o každé množině, která má nejvýše $n - 1$ prvků, pak existuje rozklad $\bar{H} = \{\bar{b}, \ldots, \bar{m}\}$ množiny H takový, že každý jeho prvek je v permutaci $\mathfrak{p}_H$ invariantní a částečné permutace prvků $\bar{b}, \ldots, \bar{m}$, určené permutací $\mathfrak{p}_H$, jsou ryzí cyklické permutace. Protože permutace $\mathfrak{p}_H$ zobrazuje každý prvek množiny H na týž prvek jako permutace $\mathfrak{p}$, jsou částečná zobrazení $\mathfrak{p}_{\bar{b}}, \ldots, \mathfrak{p}_{\bar{m}}$ prvků $\bar{b}, \ldots, \bar{m}$, určená permutací $\mathfrak{p}$, právě tyto ryzí cyklické permutace. Systém množin $\bar{G} = \{\bar{a}, \bar{b}, \ldots, \bar{m}\}$ je zřejmě rozklad množiny G a vidíme, že každý jeho prvek $\bar{a}, \bar{b}, \ldots, \bar{m}$ je v permutaci $\mathfrak{p}$ invariantní a že částečné permutace $\mathfrak{p}_{\bar{a}}, \mathfrak{p}_{\bar{b}}, \ldots, \mathfrak{p}_{\bar{m}}$ jsou ryzí cyklické permutace prvků $\bar{a}, \bar{b}, \ldots, \bar{m}$. Tím je důkaz naší věty proveden.

8.6. Způsob k určení ryzích cyklických permutací vytvořujících danou permutaci

Když je dána nějaká permutace $\mathfrak{p}$ množiny G o $n \geqq 1$ prvcích, obdržíme ryzí cyklické permutace, které ji vytvořují takto: Vyjdeme od libovolného prvku $a \in G$ a určíme nejprve cyklus $a, \mathfrak{p}a, \ldots, \mathfrak{p}^{k-1} a$; pak, jeli $k < n$, zvolíme libovolný prvek $b \in G$, který není v tomto cyklu, a určíme další cyklus $b, \mathfrak{p}b, \ldots, \mathfrak{p}^{l-1} b$; dále, je-li $k + l < n$, zvolíme libovolný prvek $c \in G$, který není v žádném předcházejícím cyklu, určíme cyklus začínající prvkem c, a tímto způsobem pokračujeme. Permutaci $\mathfrak{p}$

vyjadřujeme pak tím, že v nějakém pořadí napíšeme vedle sebe zjednodušené symboly jednotlivých ryzích cyklických permutací, které ji vytvořují. Z takového vyjádření obdržíme pak vyjádření inverzní permutace $\boldsymbol{p}^{-1}$ tím způsobem, že v každém cyklu obrátíme pořadí jednotlivých písmen. Např. hořejší permutace množiny $n = 1, 2, 3, 4$ bodů v rovině jsou vytvořeny ryzími cyklickými permutacemi takto: V případě $n = 1$: (a); v případě $n = 2$: $(a)(b)$, (a, b); v případě $n = 3$: $(a)(b)(c)$, (a, b, c), (a, c, b), $(a)(b, c)$, $(a, c)(b)$, $(a, b)(c)$; v případě $n = 4$: $(a)(b)(c)(d)$, (a, b, c, d), $(a, c)(b, d)$, (a, d, c, b), $(a)(c)(b, d)$, $(a, c)(b)(d)$, $(a, b)(c, d)$, $(a, d)(b, c)$. Inverzní permutace vzhledem k těmto jsou vyjádřeny takto: V případě $n = 1$: (a); v případě $n = 2$: $(a)(b)$, (a, b); v případě $n = 3$: $(a)(b)(c)$, (c, b, a), (b, c, a), $(a)(b, c)$, $(a, c)(b)$, $(a, b)(c)$; v případě $n = 4$: $(a)(b)(c)(d)$, (d, c, b, a), $(a, c)(b, d)$, (b, c, d, a), $(a)(c)(b, d)$, $(a, c)(b)(d)$, $(a, b)(c, d)$, $(a, d)(b, c)$.

8.7. Skládání permutací

1. *Pojem skládání permutací.* Permutace množiny G můžeme ovšem skládat podle pravidla o skládání zobrazení. Nechť $\boldsymbol{p}$, $\boldsymbol{q}$ značí libovolné permutace množiny G. Zobrazení složené $\boldsymbol{qp}$ z permutací $\boldsymbol{p}$, $\boldsymbol{q}$ je opět permutace množiny G. Symbol permutace $\boldsymbol{qp}$ obdržíme, když pod každé písmeno x, označující některý prvek množiny G, napíšeme písmeno prvku $\boldsymbol{q}(\boldsymbol{p}x)$. Máme-li permutace $\boldsymbol{p}$, $\boldsymbol{q}$ vyjádřeny obvyklými dvouřádkovými symboly, vyhledáme písmeno prvku $\boldsymbol{q}(\boldsymbol{p}x)$ takto: Vyhledáme nejprve písmeno prvku $\boldsymbol{p}x$ stojící v symbolu permutace $\boldsymbol{p}$ pod písmenem x a pak písmeno prvku $\boldsymbol{q}(\boldsymbol{p}x)$, které stojí v symbolu permutace $\boldsymbol{q}$ pod písmenem prvku $\boldsymbol{p}x$. Když např. $n = 3$ a permutace $\boldsymbol{p}$, $\boldsymbol{q}$ jsou dány symboly $\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$, $\begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$, pak symbol permutace $\boldsymbol{qp}$ je $\begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}$. Podobně postupujeme, když máme permutace $\boldsymbol{p}$, $\boldsymbol{q}$ vyjádřeny ryzími cyklickými permutacemi, které je vytvořují. Např. když opět $n = 3$ a permutace $\boldsymbol{p}$, $\boldsymbol{q}$ jsou dány symboly (a, b, c), $(a)(b, c)$, je permutace $\boldsymbol{qp}$ vyjádřena symbolem $(a, c)(b)$.

2. *Permutace vzájemně zaměnitelné.* Všimněme si, že výsledek složení dvou permutací množiny G může záviset na pořadí, v jakém je složíme, tj. permutace $\boldsymbol{qp}$ složená z permutací $\boldsymbol{p}$, $\boldsymbol{q}$ může být různá od permutace $\boldsymbol{pq}$ složené z permutací $\boldsymbol{q}$, $\boldsymbol{p}$. Tak např. v hořejším příkladě je $\boldsymbol{qp} \neq \boldsymbol{pq}$, neboť permutace $\boldsymbol{qp}$ je permutace (a, c), kdežto permutace $\boldsymbol{pq}$ je (a, b). Jsou-li permutace $\boldsymbol{p}$, $\boldsymbol{q}$ ve vzájemném vztahu daném tím, že výsledek jejich složení nezávisí na pořadí, tj. platí-li $\boldsymbol{qp} = \boldsymbol{pq}$, pak se nazývají *vzájemně zaměnitelné* neboli *vzájemně komutativní.* Např. identická permutace množiny G je zaměnitelná s každou jinou permutací množiny G.

3. *Asociativní zákon o skládání permutací.* Pro každé permutace $\boldsymbol{p}$, $\boldsymbol{q}$, $\boldsymbol{r}$ množiny G platí ovšem *asociativní zákon*

$$\boldsymbol{r}(\boldsymbol{qp}) = (\boldsymbol{rq})\boldsymbol{p},$$

a permutaci množiny G vyskytující se na obou stranách této rovnosti označujeme stručněji symbolem $\boldsymbol{rqp}$.

4. *Permutace inverzní vzhledem k složené permutaci.* Pomocí asociativního zákona snadno ukážeme, že *permutace inverzní vzhledem ke složené permutaci* $\boldsymbol{qp}$ *je permutace* $\boldsymbol{p}^{-1}\boldsymbol{q}^{-1}$, tj. že platí rovnost

$$(\boldsymbol{qp})^{-1} = \boldsymbol{p}^{-1}\boldsymbol{q}^{-1}.$$

Skutečně, nechť x značí libovolný prvek množiny G. Podle významu permutace $\boldsymbol{p}^{-1}\boldsymbol{q}^{-1}$ a podle asociativního zákona platí $(\boldsymbol{p}^{-1}\boldsymbol{q}^{-1})(\boldsymbol{qp}x) = \boldsymbol{p}^{-1}(\boldsymbol{q}^{-1}(\boldsymbol{qp}x)) = \boldsymbol{p}^{-1}((\boldsymbol{q}^{-1}\boldsymbol{q})\boldsymbol{p}x)$ a dále máme $\boldsymbol{p}^{-1}((\boldsymbol{q}^{-1}\boldsymbol{q})\boldsymbol{p}x) = \boldsymbol{p}^{-1}(\mathbf{e}(\boldsymbol{p}x)) = \boldsymbol{p}^{-1}((\mathbf{e}\boldsymbol{p})x) = \boldsymbol{p}^{-1}(\boldsymbol{p}x) = (\boldsymbol{p}^{-1}\boldsymbol{p})x = \mathbf{e}x = x$, přičemž $\mathbf{e}$ značí identickou permutaci množiny G. Vychází tedy, že permutace $\boldsymbol{p}^{-1}\boldsymbol{q}^{-1}$ zobrazuje prvek $\boldsymbol{qp}x$ na prvek x, a tím je platnost našeho tvrzení dokázána.

8.8. Cvičení

1. Vymyslete příklad prostého zobrazení nekonečné množiny (např. množiny všech přirozených čísel) do sebe, které není permutací.

2. Napište symboly všech permutací množiny skládající se ze čtyř prvků a jednotlivé permutace vyjádřete ryzími cyklickými permutacemi.

3. Uveďte nějaké pravidlo, podle něhož budete postupovat při sepisování symbolů všech permutací libovolné množiny o n ($\geqq 1$) prvcích, abyste na některou nezapomněli.

4. Pravidelný n-úhelník ($n \geqq 3$) v rovině má celkem n os souměrnosti. Otočení vrcholů okolo středu n-úhelníka o úhly měřící $0°$, $\left(\frac{360}{n}\right)°$, $\left(2 \cdot \frac{360}{n}\right)°$, ..., $\left(\overline{n-1} \cdot \frac{360}{n}\right)°$ a přiřazení k vrcholům vrcholů souměrně položených vzhledem k jednotlivým osám souměrnosti určuje celkem $2n$ permutací množiny vrcholů; označme pro okamžik množinu těchto permutací M_n. Dokažte, že množina M_n má tyto vlastnosti: 1. Když $\boldsymbol{p} \in M_n$, $\boldsymbol{q} \in M_n$, pak také $\boldsymbol{qp} \in M_n$; 2. $\mathbf{e} \in M_n$; 3. když $\boldsymbol{p} \in M_n$, pak také $\boldsymbol{p}^{-1} \in M_n$.

5. Každé dvě cyklické permutace každé množiny o n ($\geqq 1$) prvcích, jejichž cykly nemají společných prvků, jsou zaměnitelné.