4. O permutacích

In: Otakar Borůvka (author): Úvod do teorie grup. (Czech). Praha: Královská česká společnost nauk, 1944. pp. 15--23.

Persistent URL: http://dml.cz/dmlcz/401363

$$\boldsymbol{g}[\beta; c, d]\,\boldsymbol{g}[\alpha; a, b] =$$
$$= \boldsymbol{f}[\alpha - \beta;\ a \,.\, \cos\beta + b \,.\, \sin\beta + c,\ a \,.\, \sin\beta - b \,.\, \cos\beta + d].$$

Poznámka. Zobrazení $\boldsymbol{f}[\alpha; a, b]$ a $\boldsymbol{g}[\alpha; a, b]$ se nazývají *euklidovské pohyby v rovině.*

4. O permutacích.

Permutací množiny G rozumíme prosté zobrazení množiny G na sebe. 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 jest konečná, vyplývá, že každé prosté zobrazení $\boldsymbol{p}$ množiny G do sebe jest její permutace. Neboť pak množina G a její část $\boldsymbol{p}G$, skládající se ze všech obrazů v $\boldsymbol{p}$ jednotlivých prvků množiny G, jsou ekvivalentní množiny a tedy, protože jsou konečné, mají týž počet prvků; odtud plyne $G = \boldsymbol{p}G$ a tato rovnost vyjadřuje, že každý prvek množiny G má v zobrazení $\boldsymbol{p}$ vzor, takže $\boldsymbol{p}$ jest zobrazení množiny G na sebe.

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

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

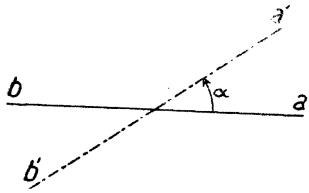
při čemž $a^*, b^*, \ldots, m^*$ jsou písmena, jimiž jsou označeny prvky $\boldsymbol{p}a$, $\boldsymbol{p}b, \ldots, \boldsymbol{p}m$; pod každým písmenem v prvním řádku stojí tedy v druhém řádku písmeno označující obraz toho prvku v permutaci $\boldsymbol{p}$. Protože $\boldsymbol{p}G = G$, jsou $a^*, b^*, \ldots, m^*$ opět písmena $a, b, \ldots, m$ napsaná v jistém pořádku. Naopak, každým symbolem toho tvaru, v němž $a^*, b^*, \ldots, m^*$ jsou opět písmena $a, b, \ldots, m$ napsaná v jistém pořádku, jest 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 $\boldsymbol{p}$ můžeme podobně vyjádřiti i jinými symboly, z nichž každý obdržíme, když písmena $a, b, \ldots, m$ napíšeme v prvním řádku v nějakém jiném pořádku a pod každé z nich napíšeme totéž písmeno jako dříve. Zejména jest ovšem identické zobrazení množiny G permutace množiny G a nazývá se *identická permutace*; její symbol jest $\begin{pmatrix} a & b & \ldots & m \\ a & b & \ldots & m \end{pmatrix}$ anebo kterýkoli z jiných symbolů, jako na př. $\begin{pmatrix} b & a & \ldots & m \\ b & a & \ldots & m \end{pmatrix}$, atp.

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

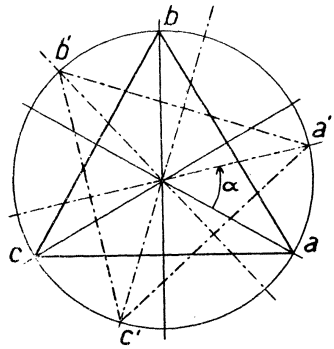
$n = 1$. Nechť G značí množinu, která se skládá z jediného bodu a v rovině. V tomto případě existuje ovšem právě jenom jedna permutace množiny G a sice permutace identická $\begin{pmatrix} a \\ a \end{pmatrix}$.

$n = 2$. 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 (v. obr. 4.), 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 $0°$, $180°$, jest množina $\{a', b'\}$ identická s množinou G a máme tyto permutace množiny G: $\begin{pmatrix} a & b \\ a & b \end{pmatrix}$, $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$.

$n = 3$. Nechť G značí množinu tří bodů v rovině a, b, c, tvořících vrcholy rovnostranného trojúhelníka. Když body a, b, c otočíme v rovině



Obr. 4.



Obr. 5.

v jednom anebo v druhém směru okolo středu trojúhelníka o vrcholech a, b, c o nějaký úhel α (v. obr. 5.), 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 jest 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 $\begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$ a 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:

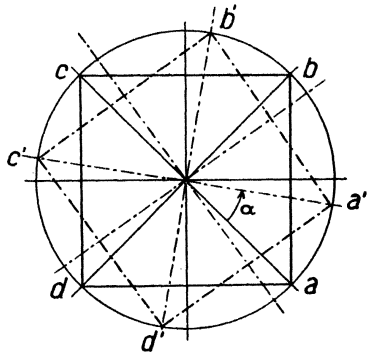
$$\begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}, \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}, \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}, \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}, \begin{pmatrix} a & b & c \\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

$n = 4$. 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 v druhém směru okolo středu čtverce o vrcholech a, b, c, d o nějaký úhel α (v. obr. 6.), pak opět obdržíme prosté zobrazení množiny G na

množinu jistých bodů v rovině a', b', c', d', a měří-li α 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 $\begin{pmatrix} a & b & c & d \\ a & d & c & b \end{pmatrix}$



Obr. 6.

a 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:

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

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

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

Kolik jest celkem permutací množiny G? Abychom na tuto otázku odpověděli, uvažme, že v libovolné permutaci $\boldsymbol{p}$ množiny G zobrazí se prvek a na jistý prvek $\boldsymbol{p}a$ množiny G; když $n > 1$, zobrazí se dále prvek b na jistý prvek $\boldsymbol{p}b$, různý od $\boldsymbol{p}a$, a podobně se zobrazí prvek c na jistý prvek $\boldsymbol{p}c$, různý od $\boldsymbol{p}a$, $\boldsymbol{p}b$, atd., a prvek m se zobrazí na jistý prvek $\boldsymbol{p}m$ různý od předcházejících prvků $\boldsymbol{p}a, \boldsymbol{p}b, \boldsymbol{p}c, \ldots$ 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 $a^*, b^*, c^*, \ldots$, obdržíme jistou permutaci $\begin{pmatrix} a & b & c & \ldots & m \\ a^* & b^* & c^* & \ldots & m^* \end{pmatrix}$ množiny G. Permutací množiny G jest tedy právě tolik, kolik jest možností takových přiřazení. Avšak k prvku a můžeme přiřaditi 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 přiřaditi 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 přiřaditi prvek $m^* \in G$, různý od $a^*, b^*, c^*, \ldots$, právě jenom jedním způsobem. Vychází tedy celkem $n(n-1)(n-2) \ldots 1$ možností a odpověď na hořejší otázku zní, že jest celkem $1 \cdot 2 \cdot 3 \ldots . n$ permutací množiny G. Obvykle se toto číslo označuje symbolem $n!$, jak ostatně víme ze střední školy. Na př. má každá množina o $n = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ prvcích celkem $n! = 1, 2, 6, 24, 120, 720, 5\,040, 40\,320, 362\,880, 3\,628\,800$ 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 permutací.

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

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

Libovolný prvek $x \in G$ zobrazí se v permutaci $\boldsymbol{p}$ na jistý prvek $\boldsymbol{p}x$, který jest totožný, anebo není, s prvkem x; nastane-li první případ $\boldsymbol{p}x = x$, pak pravíme, že permutace $\boldsymbol{p}$ nechává prvek x beze změny, anebo že prvek x jest v permutaci $\boldsymbol{p}$ *invariantní*. Jest zřejmé, že permutace $\boldsymbol{p}$ a permutace inversní $\boldsymbol{p}^{-1}$ nechávají beze změny tytéž prvky množiny G. Na př. hořejší permutace čtyř bodů v rovině nechávají beze změny tyto prvky: a, b, c, d; žádný; žádný; žádný; a, c; b, d; žádný; žádný.

Libovolný prvek $x \in G$ a permutace $\boldsymbol{p}$ jednoznačně určují řadu prvků v G: $x, \boldsymbol{p}x, \boldsymbol{p}(\boldsymbol{p}x), \boldsymbol{p}(\boldsymbol{p}(\boldsymbol{p}x)), \ldots$, v níž každý, druhým počínajíc, jest obrazem v permutaci $\boldsymbol{p}$ prvku předcházejícího. Místo $x, \boldsymbol{p}x$ píšeme někdy $\boldsymbol{p}^0x, \boldsymbol{p}^1x$ a kvůli stručnosti místo $\boldsymbol{p}(\boldsymbol{p}x), \boldsymbol{p}(\boldsymbol{p}(\boldsymbol{p}x)), \ldots$ píšeme zpravidla $\boldsymbol{p}^2x, \boldsymbol{p}^3x, \ldots$ Permutace $\boldsymbol{p}$ se nazývá *cyklická*, když existuje prvek $x \in G$ a přirozené číslo k takové, že v řadě prvků $x, \boldsymbol{p}x, \boldsymbol{p}^2x, \boldsymbol{p}^3x, \ldots, \boldsymbol{p}^{k-1}x$ nejsou žádné dva prvky totožné, ale obraz $\boldsymbol{p}^kx$ prvku $\boldsymbol{p}^{k-1}x$ jest opět prvek x a když mimo to jsou všechny ostatní prvky množiny G, jsou-li jaké, v permutaci $\boldsymbol{p}$ invariantní. Podrobněji pak permutaci $\boldsymbol{p}$ popisujeme názvem: cyklická vzhledem k prvkům $x, \boldsymbol{p}x, \boldsymbol{p}^2x, \ldots, \boldsymbol{p}^{k-1}x$; uspořádaná skupina prvků $x, \boldsymbol{p}x, \boldsymbol{p}^2x, \ldots, \boldsymbol{p}^{k-1}x$ se nazývá *cyklus* permutace $\boldsymbol{p}$, podrobněji k-členný cyklus anebo k-cyklus. Když zejména $k = n$, t. j. když každý prvek množiny G leží v cyklu permutace $\boldsymbol{p}$, pravíme, že $\boldsymbol{p}$ jest *ryzí* cyklická permutace. Předpokládejme, že permutace $\boldsymbol{p}$ jest cyklická

vzhledem k prvkům $x, \boldsymbol{p}x, \boldsymbol{p}^2x, \ldots, \boldsymbol{p}^{k-1}x$. Pak permutaci $\boldsymbol{p}$ vyjadřujeme obvykle jednodušším symbolem a sice tím, že písmena označující prvky $x, \boldsymbol{p}x, \boldsymbol{p}^2x, \ldots, \boldsymbol{p}^{k-1}x$ napíšeme v tomto pořádku vedle sebe do závorek. Permutace inversní $\boldsymbol{p}^{-1}$ vzhledem k $\boldsymbol{p}$ zobrazí každý prvek řady $x, \boldsymbol{p}x, \boldsymbol{p}^2x, \ldots, \boldsymbol{p}^{k-1}x$, kromě prvního, na prvek předcházející, prvek x na prvek $\boldsymbol{p}^{k-1}x$ a ostatní prvky množiny G, jsou-li jaké, nechává beze změny; permutace $\boldsymbol{p}^{-1}$ jest tedy cyklická vzhledem k prvkům $\boldsymbol{p}^{k-1}x, \ldots, \boldsymbol{p}^2x, \boldsymbol{p}x, x$. Změníme-li eventuálně označení prvků množiny G tak, že prvek x označíme a, prvek $\boldsymbol{p}x$ b, prvek $\boldsymbol{p}^2x$ c, atd., prvek $\boldsymbol{p}^{k-1}x$ j a ostatní prvky množiny G, jsou-li jaké, označíme libovolně zbývajícími písmeny, vypadá zjednodušený symbol permutace $\boldsymbol{p}$ takto: $(a, b, c, \ldots, j)$. Jest zřejmé, že permutaci $\boldsymbol{p}$ můžeme rovněž vyjádřiti kterýmkoli dalším symbolem $(b, c, \ldots, j, a)$, $(c, \ldots, j, a, b)$, atd., celkem tedy k způsoby. Symbol inversní permutace $\boldsymbol{p}^{-1}$ jest pak na př. $(j, \ldots, c, b, a)$. 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 jest identická permutace množiny G, takže identickou permutaci množiny G můžeme vyjádřiti kterýmkoli symbolem (a), (b), $\ldots$, (m). Každá cyklická permutace množiny G vzhledem ku dvěma prvkům se nazývá *transposice*. Na př. 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).

Nechť nyní $\boldsymbol{p}$ opět značí libovolnou permutaci množiny G. Libovolná neprázdná podmnožina $A \subset G$ zobrazí se v permutaci $\boldsymbol{p}$ na jistou podmnožinu $\boldsymbol{p}A \subset G$, která jest anebo není částí podmnožiny A. Když nastane první případ $\boldsymbol{p}A \subset A$, pak jest nutně $\boldsymbol{p}A = A$, neboť podle definice částečného zobrazení $\boldsymbol{p}_A$ máme $\boldsymbol{p}A = \boldsymbol{p}_A A$, a protože částečné zobrazení $\boldsymbol{p}_A$, jakožto prosté zobrazení konečné množiny A do sebe, jest permutací množiny A, máme dále $\boldsymbol{p}_A A = A$. V tomto případě $\boldsymbol{p}A = A$ pravíme, že permutace $\boldsymbol{p}$ nechává podmnožinu A beze změny, anebo, že podmnožina A jest v permutaci $\boldsymbol{p}$ *invariantní*. Zejména jest podmnožina A v permutaci $\boldsymbol{p}$ invariantní, když každý její prvek jest v $\boldsymbol{p}$ invariantní. Jest zřejmé, že když permutace $\boldsymbol{p}$ nechává podmnožinu A beze změny, pak totéž platí o inversní permutaci $\boldsymbol{p}^{-1}$. Na př. 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 $\boldsymbol{p}$ cyklická permutace $(a, b, c, \ldots, j)$, pak každá podmnožina $A \subset G$, která obsahuje prvky $a, b, c, \ldots, j$, jest v $\boldsymbol{p}$ invariantní a částečná permutace $\boldsymbol{p}_A$ jest také cyklická a má týž symbol $(a, b, c, \ldots, j)$.

Nechť $\overline{G} = \{\overline{a}, \overline{b}, \ldots, \overline{m}\}$ značí nějaký rozklad množiny G. Když rozklad $\overline{G}$ se vyznačuje tím, že obraz v permutaci $\boldsymbol{p}$ každého jeho prvku jest opět prvkem rozkladu $\overline{G}$, pravíme, že permutace $\boldsymbol{p}$ nechává rozklad G beze změny, anebo, že rozklad $\overline{G}$ jest v permutaci $\boldsymbol{p}$ *invariantní*. Snadno si ujasníme, že když permutace $\boldsymbol{p}$ nechává rozklad $\overline{G}$ beze změny, pak totéž platí o inversní permutaci $\boldsymbol{p}^{-1}$. Uvažujme zejména o případu, že každý prvek rozkladu $\overline{G}$ jest v permutaci $\boldsymbol{p}$ invariantní, takže $\boldsymbol{p}\overline{a} = \overline{a}$, $\boldsymbol{p}\overline{b} = \overline{b}$, ..., $\boldsymbol{p}\overline{m} = \overline{m}$. V tomto případě jest částečné zobrazení určené permutací $\boldsymbol{p}$, $\boldsymbol{p}_{\overline{x}}$, každého prvku $\overline{x} \in \overline{G}$, permutací prvku $\overline{x}$. Těmito částečnými permutacemi $\boldsymbol{p}_{\overline{a}}, \boldsymbol{p}_{\overline{b}}, \ldots, \boldsymbol{p}_{\overline{m}}$ jest permutace $\boldsymbol{p}$ jednoznačně *vytvořena* a sice v tom smyslu, že obraz libovolného prvku $x \in G$ v permutaci $\boldsymbol{p}$ jest týž jako v částečné permutaci $\boldsymbol{p}_{\overline{x}}$ onoho prvku $\overline{x} \in \overline{G}$, v němž prvek x leží. V inversní permutaci $\boldsymbol{p}^{-1}$ jest rovněž každý prvek rozkladu $\overline{G}$ invariantní a permutace $\boldsymbol{p}^{-1}$ jest vytvořena inversními permutacemi $\boldsymbol{p}_{\overline{a}}^{-1}$, $\boldsymbol{p}_{\overline{b}}^{-1}$ ..., $\boldsymbol{p}_{\overline{m}}^{-1}$. Zvolíme-li naopak na množině G libovolný rozklad $\overline{G} = \{\overline{a}, \overline{b}, \ldots, \overline{m}\}$ a na každém jeho prvku $\overline{x}$ libovolnou permutaci $\boldsymbol{p}_{\overline{x}}$ a definujeme-li na množině G permutaci $\boldsymbol{p}$ tím způsobem, že ke každému prvku $x \in G$ přiřadíme jeho obraz v permutaci $\boldsymbol{p}_{\overline{x}}$ onoho prvku $\overline{x} \in \overline{G}$, v němž prvek x leží, pak jest každý prvek rozkladu $\overline{G}$ v permutaci $\boldsymbol{p}$ invariantní a $\boldsymbol{p}_{\overline{a}}$, $\boldsymbol{p}_{\overline{b}}$, ..., $\boldsymbol{p}_{\overline{m}}$ jsou vytvořující částečné permutace této permutace $\boldsymbol{p}$.

Nyní ukážeme, že *libovolná permutace $\boldsymbol{p}$ každé množiny G o n ($\geqq 1$) prvcích jest vytvořena konečným počtem ryzích cyklických permutací*, jinými slovy, že existuje rozklad $\overline{G} = \{\overline{a}, \overline{b}, \ldots, \overline{m}\}$ množiny G takový, že každý jeho prvek $\overline{a}, \overline{b}, \ldots, \overline{m}$ jest v permutaci $\boldsymbol{p}$ invariantní a částečné permutace $\boldsymbol{p}_{\overline{a}}, \boldsymbol{p}_{\overline{b}}, \ldots, \boldsymbol{p}_{\overline{m}}$ jsou ryzí cyklické permutace prvků $\overline{a}, \overline{b}, \ldots \overline{m}$. K důkazu použijeme metody úplné indukce.*) Naše tvrzení jest správné když $n = 1$, neboť v tom případě jest $\boldsymbol{p}$ identická permutace množiny G a největší rozklad množiny G má onu vlastnost. Zbývá tedy ukázati, 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

*) Metoda úplné indukce zakládá se na této větě: *Když ke každému přirozenému číslu n jest přiřazen nějaký výrok $\boldsymbol{g}n$ a tyto výroky jsou toho druhu, že 1. výrok $\boldsymbol{g}1$ jest správný, 2. pro každé $n > 1$, pro které jsou správné výroky $\boldsymbol{g}1, \ldots, \boldsymbol{g}(n-1)$, jest 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 n, jest nejmenší. Podle předpokladu 1. jest $n > 1$; podle definice čísla n jsou výroky $\boldsymbol{g}1, \ldots, \boldsymbol{g}(n-1)$ správné, kdežto výrok $\boldsymbol{g}n$ jest nesprávný, ale to odporuje předpokladu 2. Podobná věta platí v případě, že jde o výroky přiřazené k celým číslům, která jsou větší anebo rovna nějakému celému číslu k.

každý následující jest obrazem v permutaci $\boldsymbol{p}$ prvku předcházejícího. Těchto prvků jest $n + 1$ 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 *poprve* 1. k jistému prvku $\boldsymbol{p}^j a$, kde j značí některé číslo $0, \ldots, n-1$, který se vyznačuje tím, že se mezi prvky $\boldsymbol{p}^{j+1}a, \ldots, \boldsymbol{p}^n a$ vyskytne ještě alespoň jednou 2. k prvku $\boldsymbol{p}^{j+k}a$, kde k jest některé číslo $1, \ldots, n-j$, který jest totožný s prvkem $\boldsymbol{p}^j a$, takže $\boldsymbol{p}^j a = \boldsymbol{p}^{j+k}a$. Není-li $\boldsymbol{p}^j a$ hned první prvek a, t. j. 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 $\boldsymbol{p}^j a$ a tedy platí rovnost $\boldsymbol{p}^{j-1}a = \boldsymbol{p}^{j+k-1}a$, neboť $\boldsymbol{p}$ jest zobrazení prosté; ale to není možné, protože prvek $\boldsymbol{p}^j a$ se vyznačuje vlastností, že v naší řadě $a, \boldsymbol{p}a, \boldsymbol{p}^2a, \ldots, \boldsymbol{p}^n a$ není před ním prvku vyskytujícího se pak ještě jednou, kdežto z hořejší rovnosti vyplývá, že jest takový prvek $\boldsymbol{p}^{j-1}a$. Tím jest zjištěno, že $j = 0$. Podle definice čísla k máme $\boldsymbol{p}^k a = a$, ale žádný prvek $\boldsymbol{p}a, \ldots, \boldsymbol{p}^{k-1}a$ není prvek a. Jsou-li některé dva prvky $a, \boldsymbol{p}a, \ldots, \boldsymbol{p}^{k-1}a$ stejné, t. j. platí-li pro některá celá čísla $0 \leqq r < s \leqq k-1$ rovnost $\boldsymbol{p}^r a = \boldsymbol{p}^s a$, pak odtud plyne $\boldsymbol{p}^{k-s}(\boldsymbol{p}^r a) = \boldsymbol{p}^{k-s}(\boldsymbol{p}^s a)$, t. j. $\boldsymbol{p}^{k-s+r}a = \boldsymbol{p}^k a = a$; tato rovnost ale odporuje tomu, že žádný z prvků $\boldsymbol{p}a, \ldots, \boldsymbol{p}^{k-1}a$ není prvek a, neboť $1 \leqq k - s + r \leqq k-1$ a tedy prvek $\boldsymbol{p}^{k-s+r}a$ jest jedním z nich. Tím jest zjištěno, že žádné dva prvky $a, \boldsymbol{p}a, \ldots, \boldsymbol{p}^{k-1}a$ nejsou stejné. Nechť $\bar{a}$ značí množinu prvků $a, \boldsymbol{p}a, \ldots, \boldsymbol{p}^{k-1}a$. Vidíme, že podmnožina $\bar{a} \subset G$ jest v permutaci $\boldsymbol{p}$ invariantní a že částečná permutace $\boldsymbol{p}_{\bar{a}}$ jest ryzí cyklická permutace této množiny. Jestliže $k = n$, t. j. platí-li $\bar{a} = G$, pak $\boldsymbol{p}_{\bar{a}} = \boldsymbol{p}$ 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 $a, \boldsymbol{p}a, \ldots, \boldsymbol{p}^{k-1}a$ ještě další prvky, jejichž počet jest nejvýše $n-1$; množinu těchto prvků označme H. V částečném zobrazení $\boldsymbol{p}_H$ jest obraz každého prvku $x \in H$ opět prvek v H, neboť v opačném případě platí rovnost $\boldsymbol{p}x = \boldsymbol{p}^l a$, kde l značí některé číslo $0, \ldots, k-1$ a odtud plyne $x = \boldsymbol{p}^{l-1}a$, je-li $l > 0$ a $x = \boldsymbol{p}^{k-1}a$, je-li $l = 0$, ale to v obou případech odporuje předpokladu $x \in H$. $\boldsymbol{p}_H$ jest tedy zobrazení množiny H do sebe a protože jest prosté a množina H má jenom konečný počet prvků, jest $\boldsymbol{p}_H$ permutace množiny H. Platí-li naše tvrzení o každé množině, která má nejvýše $n-1$ prvků, pak existuje rozklad $\overline{H} = \{\bar{b}, \ldots, \overline{m}\}$ množiny H takový, že každý jeho prvek jest v pertumaci $\boldsymbol{p}_H$ invariantní a částečné permutace prvků $\bar{b}, \ldots, \overline{m}$ určené permutací $\boldsymbol{p}_H$ jsou ryzí cyklické permutace. Protože permutace $\boldsymbol{p}_H$ zobrazuje každý prvek množiny H na týž prvek jako permutace $\boldsymbol{p}$, jsou částečná zobrazení $\boldsymbol{p}_{\bar{b}}, \ldots, \boldsymbol{p}_{\overline{m}}$ prvků $\bar{b}, \ldots, \overline{m}$ určená permutací $\boldsymbol{p}$ právě tyto ryzí cyklické permutace. Systém množin $\overline{G} = \{\bar{a}, \bar{b}, \ldots, \overline{m}\}$ jest zřejmě rozklad množiny G a vidíme, že každý jeho prvek $\bar{a}, \bar{b}, \ldots, \overline{m}$ jest v permutaci $\boldsymbol{p}$ invariantní a částečné permutace $\boldsymbol{p}_{\bar{a}}, \boldsymbol{p}_{\bar{b}}, \ldots, \boldsymbol{p}_{\overline{m}}$ jsou

ryzí cyklické permutace prvků $\bar{a}, \bar{b}, \ldots, \overline{m}$. Tím jest důkaz naší věty proveden.

Když jest dána nějaká permutace $\boldsymbol{p}$ množiny G o $n \geqq 1$ prvcích, obdržíme ryzí cyklické permutace, které ji vytvořují, takto: Vycházejíce od libovolného prvku $a \in G$ určíme nejprve cyklus $a, \boldsymbol{p}a, \ldots, \boldsymbol{p}^{k-1}a$; pak, je-li $k < n$, zvolíme libovolný prvek $b \in G$, který není v tomto cyklu a určíme další cyklus $b, \boldsymbol{p}b, \ldots, \boldsymbol{p}^{l-1}b$; 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 $\boldsymbol{p}$ vyjadřujeme pak tím, že v nějakém pořádku napíšeme vedle sebe zjednodušené symboly jednotlivých ryzích cyklických permutací, které ji vytvořují. Z takového vyjádření obdržíme pak vyjádření inversní permutace $\boldsymbol{p}^{-1}$ tím způsobem, že v každém cyklu obrátíme pořádek jednotlivých písmen. Na př. 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), $(a)(c)(b, d)$, $(a, c)(b)(d)$, $(a, b)(c, d)$, $(a, d)(b, c)$. Inversní 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), $(a)(c)(b, d)$, $(a, c)(b)(d)$, $(a, b)(c, d)$, $(a, d)(b, c)$.

Permutace množiny G můžeme ovšem skládati podle pravidla o skládání zobrazení. Nechť $\boldsymbol{p}, \boldsymbol{q}$ značí libovolné permutace množiny G. Zobrazení složené $\boldsymbol{qp}$ z permutací $\boldsymbol{p}, \boldsymbol{q}$ jest 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 na př. $n = 3$ 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 $\boldsymbol{qp}$ jest $\begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}$. Podobně postupujeme, když máme permutace $\boldsymbol{p}, \boldsymbol{q}$ vyjádřeny ryzími cyklickými permutacemi, které je vytvořují. Na př. když opět $n = 3$ a permutace $\boldsymbol{p}, \boldsymbol{q}$ jsou dány symboly (a, b, c), $(a)(b, c)$, jest permutace $\boldsymbol{qp}$ vyjádřena symbolem $(a, c)(b)$. Při této příležitosti si všimněme, že výsledek složení dvou permutací množiny G může záviseti na pořádku, v jakém je složíme, t. j. permutace $\boldsymbol{qp}$ složená z permutací $\boldsymbol{p}, \boldsymbol{q}$ může býti různá od permutace $\boldsymbol{pq}$ složené z permutací $\boldsymbol{q}, \boldsymbol{p}$. Tak na

př. v hořejším příkladě jest $qp \neq pq$, neboť permutace qp jest cyklická permutace (a, c), kdežto permutace pq jest (a, b). Jsou-li permutace p, q ve vzájemném vztahu daném tím, že výsledek jejich složení nezávisí na pořádku, t. j. platí-li $qp = pq$, pak se nazývají *zaměnitelné* anebo *komutativní*. Na př. jest identická permutace množiny G zaměnitelná s každou jinou permutací množiny G.

Pro každé permutace p, q, r množiny G platí ovšem asociativní zákon

$$r(qp) = (rq)p,$$

a permutace množiny G vyskytující se na obou stranách této rovnosti označujeme stručněji symbolem rqp. Pomocí asociativního zákona snadno ukážeme, že *permutace inversní vzhledem ke složené permutaci* qp *jest permutace* $p^{-1}q^{-1}$, t. j. že platí rovnost $(qp)^{-1} = p^{-1}q^{-1}$. Skutečně, nechť x značí libovolný prvek množiny G. Podle významu permutace $p^{-1}q^{-1}$ a podle asociativního zákona platí rovnosti $(p^{-1}q^{-1})(qpx) = p^{-1}(q^{-1}(qpx)) = p^{-1}((q^{-1}q)px)$ a dále máme $p^{-1}((q^{-1}q)px) = p^{-1}(e(px)) = p^{-1}((ep)x) = p^{-1}(px) = (p^{-1}p)x = ex = x$, při čemž e značí identickou permutaci množiny G. Vychází tedy, že permutace $p^{-1}q^{-1}$ zobrazuje prvek qpx na prvek x a tím jest platnost našeho tvrzení dokázána.

Cvičení. 1. Vymyslete příklad prostého zobrazení nekonečné množiny (na př. 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 postupovati při sepisování symbolů všech permutací libovolné množiny o n (≥ 1) prvcích, abyste na některou nezapomněli!

4. Pravidelný n-úhelník ($n \geq 3$) 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 $p \in M_n$, $q \in M_n$, pak také $qp \in M_n$ 2. $e \in M_n$ 3. když $p \in M_n$, pak také $p^{-1} \in M_n$.

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