27. Cyklické grupy

In: Otakar Borůvka (author): Základy teorie grupoidů a grup. (Czech). Praha: Nakladatelství Československé akademie věd, 1962. pp. 198--202.

Persistent URL: http://dml.cz/dmlcz/401454

27. Cyklické grupy

27.1. Definice

Libovolná grupa $\mathfrak{G}$ se nazývá *cyklická*, když v ní existuje prvek, zvaný *základní*, který se vyznačuje tím, že každý prvek v $\mathfrak{G}$ je jeho mocninou. Když $\mathfrak{G}$ je cyklická grupa a a její základní prvek, pak grupu $\mathfrak{G}$ označujeme zpravidla symbolem (a).

Z prvního vzorce (1) odst. **19.3** plyne, že *každá cyklická grupa je abelovská.*

27.2. Řád cyklické grupy

Uvažujme o libovolné cyklické grupě (a). Jsou-li mocniny a^i, a^j prvku a s každými dvěma různými mocniteli i, j různé, pak má grupa (a) řád 0, neboť obsahuje nekonečně mnoho prvků

$$(1) \qquad \ldots, a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots$$

Protože každý prvek grupy (a) je některou mocninou prvku a, není v grupě (a) jiných prvků než jsou tyto a vychází, že se grupa (a) skládá z prvků (1). Předpokládejme nyní, že mocniny prvku a s některými různými mocniteli i, j jsou rovné, takže $a^i = a^j$, $i \neq j$. Z této rovnosti plyne $a^{-j} \cdot a^i = a^{-j} \cdot a^j$, tj. $a^{i-j} = \underline{1}$. Protože jedno z čísel $i - j, j - i$ je přirozené a mocniny prvku a s těmito mocniteli se rovnají $\underline{1}$, vidíme, že existují přirozená čísla x vyhovující rovnici $a^x = \underline{1}$. Mezi těmito přirozenými čísly je jisté číslo nejmenší; označme je n, takže máme $a^n = \underline{1}$. Uvažujme o těchto prvcích grupy (a):

$$(2) \qquad \underline{1}, a, a^2, \ldots, a^{n-1}.$$

Především snadno zjistíme, že každé dva z nich jsou různé; skutečně, platí-li pro některé z nich rovnost $a^i = a^j$, je jedno z obou čísel $i - j, j - i$ přirozené a menší než n a vyhovuje rovnici $a^x = \underline{1}$; ale to odporuje definici čísla n. Grupa (a) má tedy alespoň n prvků (2) a má tedy řád buď 0 nebo $\geqq n$. Dále snadno ukážeme, že grupa (a) jiných prvků nemá, takže její řád je n. Za tím účelem uvažujme o libovolném prvku a^x grupy (a). Dělíme-li číslo x číslem n, obdržíme jistý podíl q a jistý zbytek r, tedy $x = qn + r$, a máme $0 \leqq r \leqq n - 1$, takže a^r je jedním z prvků (2). Ze vzorců (1) odst. **19.3** plynou rovnosti

$$a^x = a^{qn+r} = a^{qn} \cdot a^r = (a^n)^q \cdot a^r = \underline{1}^q \cdot a^r = \underline{1} \cdot a^r = a^r$$

a odtud vychází, že a^x je prvek a^r. Tím je zjištěno, že se grupa (a) skládá z prvků (2) a má tedy řád n. Dále plyne z naší úvahy, že součin $a^i \,.\, a^j$ libovolného prvku a^i s libovolným prvkem a^j grupy (a) je prvek a^k, kde k značí zbytek dělení čísla $i + j$ číslem n, neboť $a^i \,.\, a^j = a^{i+j}$. Shrneme-li své výsledky o cyklických grupách, dostaneme větu:

Řád n každé cyklické grupy (a) je buď 0 a v tom případě se grupa (a) skládá z prvků (1); nebo $n > 0$ a pak se cyklická grupa (a) skládá z prvků (2). Součin $a^i \,.\, a^j$ libovolného prvku a^i s libovolným prvkem a^j grupy (a) je v prvním případě prvek a^{i+j}, kdežto v druhém případě prvek a^k, kde k je zbytek dělení čísla $i + j$ číslem n. Ve druhém případě je n nejmenší přirozené číslo takové, že $a^n = \underline{1}$.

Všimněme si, že v obou případech je a^{n-i} prvek inverzní vzhledem k prvku a^i.

27.3. Podgrupy cyklických grup

Uvažujme nyní o nějaké podgrupě $\mathfrak{A}$ v cyklické grupě (a). Když se podgrupa $\mathfrak{A}$ skládá z jediného prvku $\underline{1}$, pak je cyklická a má základní prvek $\underline{1}$. Předpokládejme nyní, že podgrupa $\mathfrak{A}$ obsahuje kromě prvku $\underline{1}$ některý prvek a^i, kde $i \neq 0$. Protože podgrupa $\mathfrak{A}$ obsahuje s prvkem a^i současně inverzní prvek a^{-i} a protože jedno z obou čísel i, $-i$ je přirozené, vidíme, že v podgrupě $\mathfrak{A}$ existují mocniny prvku a, jejichž mocnitelé jsou přirozená čísla. Mezi těmito mocniteli je jeden nejmenší; označme jej m, takže máme $a^m \in \mathfrak{A}$. Mocniny prvku a s přirozenými mocniteli menšími než m v podgrupě $\mathfrak{A}$ neexistují. Nechť a^x značí libovolný prvek v $\mathfrak{A}$. Dělíme-li číslo x číslem m, obdržíme jistý podíl q a jistý zbytek r, takže $x = qm + r$, a máme $0 \leqq r \leqq m - 1$. Ze vzorců (1) v odst. **19.3** plynou rovnosti $a^x = a^{qm+r} = a^{qm} \,.\, a^r$. Odtud vychází, že prvek a^r je součinem prvku a^{-qm} s prvkem a^x. Protože a^{-qm} je inversní prvek vzhledem k prvku $(a^m)^q$, který je jako q-tá mocnina prvku a^m obsaženého v $\mathfrak{A}$ rovněž v $\mathfrak{A}$, vidíme, že a^{-qm} je prvek v $\mathfrak{A}$. Protože také a^x je prvek v $\mathfrak{A}$, je i součin $a^{-qm} \,.\, a^x$, tj. prvek a^r, obsažen v podgrupě $\mathfrak{A}$. Odtud vzhledem k nerovnostem $0 \leqq r \leqq m - 1$ a k definici čísla m vychází $r = 0$. Proto $a^x = (a^m)^q$. Každý prvek podgrupy $\mathfrak{A}$ je tedy jistou mocninou prvku a^m, takže podgrupa $\mathfrak{A}$ je cyklická a má základní prvek a^m. Touto úvahou jsme došli k výsledku, že *každá podgrupa v cyklické grupě (a) je cyklická.*

Protože cyklická grupa (a) je abelovská, *je v ní každá podgrupa invariantní.*

27.4. Základní prvky

Existují v cyklické grupě (a) kromě prvku a ještě další základní prvky? Nechť opět n značí řád grupy (a) a předpokládejme, že některý prvek a^v grupy (a) je základní. Pak zejména prvek a je jistou mocninou prvku a^v, takže máme $a = a^{vq}$, kde q značí

jisté celé číslo. Je-li $n = 0$, pak z této rovnosti plyne $vq = 1$, neboť v tom případě každé dvě mocniny prvku a s různými mocniteli jsou různé a odtud dále plyne $v = q = 1$ anebo $v = q = -1$. Kromě prvku a může tedy jenom prvek a^{-1} být základní a vidíme, že skutečně každý prvek a^i grupy (a) je $-i$-tou mocninou prvku a^{-1}.

V případě $n = 0$ má tedy grupa (a) právě dva základní prvky: a, a^{-1}. Všimněme si, že jsou to jediné dva prvky v (a), jejichž mocnitelé mají s číslem $n\,(= 0)$ největší společný dělitel 1, jinak řečeno, jejichž mocnitelé jsou s číslem $n\,(= 0)$ nesoudělní.

Uvažujme nyní o případu $n > 0$. Cyklická grupa (a) se skládá z prvků $1, a, a^2, \ldots, a^{n-1}$. Značí-li r zbytek dělení čísla vq číslem n, takže $vq = nq' + r$, kde q' je podíl a $0 \leqq r \leqq n - 1$, máme $a^{vq} = a^r = a$. Odtud plyne $r = 1$, neboť a, a^r jsou z řady $1, a, a^2, \ldots, a^{n-1}$, v níž každé dva prvky s různými mocniteli jsou různé. Máme tedy rovnost $vq - nq' = 1$ a odtud plyne, že čísla v, n jsou nesoudělná, Značí-li naopak v libovolné celé číslo nesoudělné s n, pak existují celá čísla q, q' taková, že $vq - nq' = 1$, a odtud plyne pro každé celé číslo i vztah $i = v(qi) - n(q'i)$. Proto máme $a^i = (a^v)^{qi}$, takže a^v je základním prvkem grupy (a). V případě $n > 0$ jsou tedy základními prvky grupy (a) právě ony mocniny prvku a, jejichž mocnitelé jsou s číslem n nesoudělní. Viděli jsme, že týž výsledek platí i v případě $n = 0$, takže naše výsledky můžeme shrnout větou:

Základními prvky libovolné cyklické grupy (a) řádu $n \geqq 0$ jsou právě jenom mocniny prvku a, jejichž mocnitelé jsou s číslem n nesoudělní.

V případě $n = 0$ má tedy cyklická grupa (a) právě dva základní prvky, kdežto v případě $n > 0$ jich má tolik, kolik je v řadě $1, 2, \ldots, n$ čísel nesoudělných s n.

27.5. Určení všech cyklických grup

1. Důležitým příkladem cyklické grupy řádu 0 je grupa $\mathfrak{Z}$. Zřejmě je $\mathfrak{Z} = (1)$. Všechny podgrupy v $\mathfrak{Z}$ se skládají, jak víme, ze všech celých násobků vždy nějakého nezáporného čísla n a jsou tedy, podle hořejšího výsledku, cyklickými grupami (n). Nechť $n \geqq 0$ a uvažujme o faktorové grupě $\mathfrak{Z}/(n)$. Připomeňme si, že když $n = 0$, pak se $\mathfrak{Z}/(n)$ skládá z množin $\bar{a}_i = \{i\}$, kde $i = \ldots, -2, -1, 0, 1, 2, \ldots$, a když $n > 0$, pak se skládá z prvků $\bar{a}_0, \ldots, \bar{a}_{n-1}$, kde $\bar{a}_i$ značí množinu všech prvků v $\mathfrak{Z}$ lišících se od čísla i jenom o nějaký celý násobek čísla n; v obou případech má faktorová grupa $\mathfrak{Z}/(n)$ řád n. Snadno ukážeme, že faktorová grupa $\mathfrak{Z}/(n)$ je cyklická a má základní prvek $\bar{a}_1$. Skutečně, podle definice násobení v $\mathfrak{Z}/(n)$ je libovolná i-tá mocnina libovolného prvku $\bar{a}_j \in \mathfrak{Z}/(n)$ onen prvek v $\mathfrak{Z}/(n)$, který obsahuje číslo ij a tedy je zejména $\bar{a}_i = a_1^i$. Tím je naše tvrzení dokázáno. Současně je tím zjištěno, že existují cyklické grupy libovolného řádu $n \geqq 0$.

Avšak nejen každá faktorová grupa na grupě $\mathfrak{Z}$ je cyklická, nýbrž i naopak každá cyklická grupa je izomorfní s jistou faktorovou grupou na grupě $\mathfrak{Z}$. Skutečně,

uvažujme o libovolné cyklické grupě (a). Pak ke každému prvku $x \in (a)$ existuje alespoň jedno celé číslo ξ takové, že $a^{\xi} = x$ a ovšem naopak, je-li ξ libovolné číslo celé, je a^{ξ} prvkem v (a). Přiřadíme-li tedy ke každému prvku $\xi \in \mathfrak{Z}$ prvek $a^{\xi} \in (a)$, obdržíme jisté zobrazení $\boldsymbol{d}$ grupy $\mathfrak{Z}$ na grupu (a). Když ξ, η jsou libovolné prvky v $\mathfrak{Z}$ a $\boldsymbol{d}\xi = x$, $\boldsymbol{d}\eta = y$, máme $x = a^{\xi}$, $y = a^{\eta}$ a tedy $xy = a^{\xi}a^{\eta} = a^{\xi+\eta}$, takže $\boldsymbol{d}(\xi + \eta) = xy = \boldsymbol{d}\xi\boldsymbol{d}\eta$. Odtud plyne, že zobrazení $\boldsymbol{d}$ zachovává násobení v obou grupách $\mathfrak{Z}$, (a), a tedy je homomorfizmus. Vychází tedy především, že cyklická grupa (a) je homomorfní s grupou $\mathfrak{Z}$. Podle první věty o izomorfismu grup (**26.3.**1) tvoří množina všech vzorů v $\boldsymbol{d}$ jednotky grupy (a) invariantní podgrupu $\mathfrak{A}$ v $\mathfrak{Z}$ a faktorová grupa na $\mathfrak{Z}$, vytvořená invariantní podgrupou $\mathfrak{A}$, je izomorfní s (a), tj. $\mathfrak{Z}/\mathfrak{A} \cong (a)$. Nechť n $(\geqq 0)$ značí řád cyklické grupy (a). Pak také $\mathfrak{Z}/\mathfrak{A}$ má řád n a podgrupa $\mathfrak{A}$ se tedy skládá ze všech celých násobků čísla n. Vychází tedy, že cyklická grupa (a), řádu n, je izomorfní s faktorovou grupou na $\mathfrak{Z}$ vytvořenou podgrupou (n) v $\mathfrak{Z}$. Zejména je tudíž každá cyklická grupa řádu 0 izomorfní s grupou $\mathfrak{Z}/(0)$ a tedy také s grupou $\mathfrak{Z}$.

Zřejmě je každá grupa, která je izomorfní s nějakou cyklickou grupou řádu n $(\geqq 0)$, opět cyklická a má řád n. Naše úvahy obsahují tedy tento výsledek:

Všechny cyklické grupy řádu $n \geqq 0$ jsou representovány faktorovou grupou $\mathfrak{Z}/(n)$ na grupě $\mathfrak{Z}$, a to v tom smyslu, že každá cyklická grupa řádu n je izomorfní se $\mathfrak{Z}/(n)$ a naopak, každá grupa izomorfní s touto faktorovou grupou je cyklická a má řád n.

2. Příklad. Jako příklad cyklické grupy řádu $n > 0$ uveďme grupu skládající se z kořenů rovnice $x^n = 1$, přičemž násobení je násobení v aritmetickém smyslu. Kořeny této rovnice jsou:

$$\varepsilon_0 = 1,\ \varepsilon_1 = e^{2\pi i/n},\ \varepsilon_2 = e^{4\pi i/n},\ \ldots,\ \varepsilon_{n-1} = e^{2(n-1)\pi i/n}$$

a tvoří tedy cyklickou grupu $(e^{2\pi i/n})$. Body, jejichž souřadnice jsou reálné a imaginární části těchto kořenů, jsou vrcholy pravidelného n-úhelníka. Např. pro $n = 6$ máme vrcholy pravidelného 6-úhelníka. Základní prvky této grupy řádu 6 jsou $e^{2\pi i/6}$, $e^{10\pi i/6}$.

27.6. Fermatova věta pro grupy

Pojem cyklické grupy má důležitý význam i pro grupy, které nejsou nutně cyklické. Uvažujme o libovolné grupě $\mathfrak{G}$. Nechť a značí libovolný prvek v $\mathfrak{G}$. Jednotlivé mocniny prvku a tvoří cyklickou podgrupu (a) v $\mathfrak{G}$.

Řádem prvku a rozumíme řád cyklické podgrupy (a). Řád n prvku a je tedy buď 0 nebo nejmenší přirozené číslo x, pro něž $a^x = \underline{1}$; vždycky tedy platí $a^n = \underline{1}$.

Dále snadno zjistíme, že *řád n každého prvku $a \in \mathfrak{G}$ je dělitelem řádu N grupy $\mathfrak{G}$*, tj. že platí rovnost $N = nd$, kde d značí jisté celé číslo. Toto tvrzení je zřejmé, je-li $N = 0$. V případě $N > 0$ plyne z věty, že řád každé podgrupy v $\mathfrak{G}$ je děli-

telem řádu grupy $\mathfrak{G}$. Z rovnosti $N = nd$ plyne: $a^N = a^{nd} = (a^n)^d = \underline{1}^d = \underline{1}$. Odtud vychází tzv. *Fermatova věta pro grupy*:

V každé grupě libovolného řádu N je N-tá mocnina libovolného prvku jednotka grupy.

27.7. Vytvoření translací na konečných grupách ryzími cyklickými permutacemi

Své úvahy ukončíme poznámkou *o vytvoření např. levých translací nějaké konečné grupy ryzími cyklickými permutacemi.*

Nechť $\mathfrak{G}$ značí libovolnou konečnou grupu a nechť a je libovolný prvek v $\mathfrak{G}$. Jak jsme vyložili v odst. **26.2.**1, je levá translace ${}_a\mathbf{t}$ grupy $\mathfrak{G}$ permutací grupy $\mathfrak{G}$ a je tedy vytvořena konečným počtem ryzích cyklických permutací, tj. existuje rozklad $\bar{G} = \{\bar{a}, \ldots, \bar{m}\}$ grupy $\mathfrak{G}$ takový, že každý jeho prvek $\bar{a}, \ldots, \bar{m}$ je v ${}_a\mathbf{t}$ invariantní a částečné permutace ${}_a\mathbf{t}_{\bar{a}}, \ldots, {}_a\mathbf{t}_{\bar{m}}$ jsou ryzí cyklické permutace prvků $\bar{a}, \ldots, \bar{m}$. Libovolný prvek $\bar{x}$ rozkladu $\bar{G}$ se skládá z prvků cyklu: $x, {}_a\mathbf{t}x, ({}_a\mathbf{t})^2x, \ldots, ({}_a\mathbf{t})^{k-1}x$, přičemž x značí libovolný prvek v $\bar{x}$ a k nejmenší přirozené číslo takové, že $({}_a\mathbf{t})^k x = x$. Podle definice levé translace ${}_a\mathbf{t}$ máme ${}_a\mathbf{t}x = ax$, $({}_a\mathbf{t})^2x = a^2x$, $\ldots$, $({}_a\mathbf{t})^{k-1}x = a^{k-1}x$ a z rovností $({}_a\mathbf{t})^k x = a^k x = x$ plyne $a^k = \underline{1}$. Odtud vidíme, že náš cyklus je $x, ax, a^2x, \ldots, a^{k-1}x$, a dále, že množina $\{\underline{1}, a, a^2, \ldots, a^{k-1}\}$ je polem cyklické podgrupy (a) v $\mathfrak{G}$. Prvek $\bar{x}$ je tedy pravá třída prvku x vzhledem k cyklické podgrupě (a). Odtud dále plyne, že $\bar{G}$ je pravý rozklad grupy $\mathfrak{G}$ vytvořený cyklickou podgrupou (a).

O ryzích cyklických permutacích, které vytvořují libovolnou levou translaci ${}_a\mathbf{t}$ v nějaké konečné grupě $\mathfrak{G}$, platí tedy věta, že *se jejich cykly skládají z týchž prvků jako pravé třídy vzhledem k cyklické podgrupě (a) v grupě $\mathfrak{G}$.*

27.8. Cvičení

1. Prvek $a \neq 1$ v libovolné grupě $\mathfrak{G}$ má řád 2, když a jen když je sám k sobě inverzní.
2. V každé konečné grupě sudého řádu existují prvky řádu 2.
3. Má-li prvek a libovolné grupy $\mathfrak{G}$ řád n, pak řád každého prvku cyklické podgrupy (a) v $\mathfrak{G}$ je dělitelem čísla n.
4. Každá grupa, jejíž řád je prvočíslo, je cyklická.
5. Řád každého prvku $\bar{a}$ libovolné faktorové grupy na nějaké konečné grupě $\mathfrak{G}$ je dělitelem řádu každého prvku v $\mathfrak{G}$ obsaženého v $\bar{a}$. Když je řád prvku $\bar{a}$ mocninou nějakého prvočísla p, pak v $\bar{a}$ existuje prvek a, jehož řád je rovněž mocninou prvočísla p.