

Úvod do theorie grup [2. rozšířené vydání]

16. O cyklických grupách

In: Otakar Borůvka (author): Úvod do theorie grup [2. rozšířené vydání]. (Czech). Praha: Přírodovědecké vydavatelství, 1952. pp. 137--143.

Persistent URL: <http://dml.cz/dmlcz/401422>

Terms of use:

© Přírodovědecké vydavatelství

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://project.dml.cz>

grupu \mathfrak{S}_3 . Použijte této deformace a dokažte pomocí první a třetí věty o isomorfismu grup, že grupa \mathfrak{D} obsahuje invariantní podgrupy řádů 4, 12.

16. O CYKlickÝCH GRUPÁCH.

16.1. Definice.

Libovolná grupa \mathfrak{G} se nazývá cyklická, když v ní existuje prvek, t. zv. 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. 11.3 plyne, že každá cyklická grupa jest abelovská.

16.2. Řád cyklických grup.

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

$$\dots, a^{-2}, a^{-1}, a^0, a^1, a^2, \dots \quad (1)$$

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 $a^{-j} \cdot a^i = a^{-j} \cdot a^j$, t. j. $a^{i-j} = \underline{1}$. Protože jedno z čísel $i - j, j - i$ je přirozené a mocniny prvku a s těmito mocniteli jsou rovny $\underline{1}$, 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) :

$$\underline{1}, a, a^2, \dots, a^{n-1}. \quad (2)$$

Především snadno zjistíme, že každé dva z nich jsou různé; skutečně, platí-li pro některé z nich rovnost $a^i = a^j$, jest jedno z obou čísel $i - j, j - i$ přirozené a menší než n a hová 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 $\geq n$. Dále snadno ukážeme, že grupa (a) jiných prvků nemá, takže její řád jest 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 $0 \leq r \leq n - 1$, takže a^x jest jedním z prvků (2). Ze vzorců (1) odst. 11.3 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 grupa (a) se skládá z prvků (2) a má tedy řád n . Dále plyne z naší úvahy, že součín $a^i \cdot a^j$ 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 $a^i \cdot a^j = a^{i+j}$. Shrňeme-li své výsledky o cyklických grupách, dostaneme větu:

Řád n každé cyklické grupy (a) jest 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). Součín $a^i \cdot a^j$ 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 jest a^{n-i} prvek inverzní vzhledem k prvku a^i .

16.3. Podgrupy cyklických grup.

Uvažujme nyní o nějaké podgrupě \mathfrak{U} v cyklické grupě (a) . Když se podgrupa \mathfrak{U} skládá z jediného prvku $\underline{1}$, pak je cyklická a má základní prvek $\underline{1}$. Předpokládejme nyní, že podgrupa \mathfrak{U} obsahuje kromě prvku $\underline{1}$ některý prvek a^i , kde $i \neq 0$. Protože podgrupa \mathfrak{U} 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{U} existují mocniny prvku a , jejichž mocnitelé jsou přirozená čísla. Mezi těmito mocniteli jest jeden nejmenší; označme jej m , takže máme $a^m \in \mathfrak{U}$ a mocniny prvku a s přirozenými mocniteli menšími než m v podgrupě \mathfrak{U} neexistují. Nechť a^x značí libovolný prvek v \mathfrak{U} . Dělíme-li číslo x číslem m , obdržíme jistý podíl q a jistý zbytek r , takže $x = qm + r$, a máme $0 \leq r \leq m - 1$. Ze vzorců (1) v odst. 11.3 plynou rovnosti $a^x = a^{qm+r} = a^{qm} \cdot a^r$ a odtud vychází, že prvek a^r je součín prvku a^{-qm} s prvkem a^x . Protože a^{-qm} jest inverzní prvek vzhledem k prvku $(a^m)^q$, který jako q -tá mocnina prvku a^m obsaženého v \mathfrak{U} je rovněž v \mathfrak{U} , vidíme, že a^{-qm} je prvek v \mathfrak{U} , a protože

také a^x je prvek v \mathfrak{A} , jest i součin $a^{-am} \cdot a^x$, t. j. prvek a^r , obsažen v podgrupě \mathfrak{A} . Odtud vzhledem k nerovnostem $0 \leq r \leq m - 1$ a k definici čísla m vychází $r = 0$ a máme $a^x = (a^m)^q$. 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) jest abelovská, je v ní každá podgrupa invariantní.

16.4. Základní prvky.

Existují v cyklické grupě (a) kromě prvku a ještě další základní prvky? Necht' opět n značí řád grupy (a) a předpokládejme, že některý prvek a^r grupy (a) je základní. Pak zejména prvek a jest jistou mocninou prvku a^r , takže máme $a = a^{rq}$, kde q značí jisté celé číslo. Je-li $n = 0$, pak z této rovnosti plyne $rq = 1$, neboť v tom případě každé dvě mocniny prvku a s různými mocniteli jsou různé a odtud dále plyne $r = q = 1$ anebo $r = q = -1$. Kromě prvku a může tedy jenom prvek a^{-1} být základní a vidíme, že skutečně každý prvek a^i grupy (a) jest $-i$ -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 případě $n > 0$. Cyklická grupa (a) se skládá z prvků $1, a, a^2, \dots, a^{n-1}$. Značí-li r zbytek dělení čísla rq číslem n , takže $rq = nq' + r$, kde q' je podíl a $0 \leq r \leq n - 1$, máme $a^{rq} = a^r = a$ a odtud plyne $r = 1$, neboť a, a^r jsou z řady $1, a, a^2, \dots, a^{n-1}$, v níž každé dva prvky s různými mocniteli jsou různé. Máme tedy rovnost $rq - nq' = 1$ a odtud plyne, že čísla r, n jsou nesoudělná. Značí-li naopak v libovolné celé číslo nesoudělné s n , pak existují celá čísla q, q' taková, že $rq - nq' = 1$ (viz pozn. pod čarou na str. 77), a odtud plyne pro každé celé číslo i vztah $i = r(qi) - n(q'i)$, a máme $a^i = (a^r)^{qi}$, takže a^r 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 shrnouti větou:

Základními prvky libovolné cyklické grupy (a) řádu $n \geq 0$ 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, tolik je v řadě 1, 2, ..., n čísel nesoudělných s n .

16.5. Určení všech cyklických grup.

16.5.1. 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, cyklické grupy (n). Nechť $n \geq 0$ 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 $i = \dots, -2, -1, 0, 1, 2, \dots$, a když $n > 0$, pak se skládá z prvků $\bar{a}_0, \dots, \bar{a}_{n-1}$, 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 $\bar{a}_i = \bar{a}_1^i$. Tím je naše tvrzení dokázáno. Současně je tím zjištěno, že existují cyklické grupy libovolného řádu $n \geq 0$.

Avšak nejen každá faktorová grupa na grupě \mathfrak{Z} je cyklická, nýbrž i naopak každá cyklická grupa je isomorfní 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, jest a^ξ prvkem v (a). Přiřadíme-li tedy ke každému prvku $\xi \in \mathfrak{Z}$ prvek $a^\xi \in (a)$, obdržíme jisté zobrazení \mathbf{d} grupy \mathfrak{Z} na grupu (a). Když ξ, η jsou libovolné prvky v \mathfrak{Z} a $\mathbf{d}\xi = x, \mathbf{d}\eta = y$, máme $x = a^\xi, y = a^\eta$ a tedy $xy = a^\xi a^\eta = a^{\xi+\eta}$, takže $\mathbf{d}(\xi + \eta) = xy = \mathbf{d}\xi \mathbf{d}\eta$. Odtud plyne, že zobrazení \mathbf{d} zachovává násobení v obou grupách $\mathfrak{Z}, (a)$, a tedy je homomorfismus. Vychází tedy především, že cyklická grupa (a) je homomorfní s grupou \mathfrak{Z} . Podle první věty o isomorfismu grup tvoří množina všech vzorů v \mathbf{d} jednotky grupy (a) invariantní podgrupu \mathfrak{A} v \mathfrak{Z} a faktorová grupa na \mathfrak{Z} , vytvořená invariantní podgrupou \mathfrak{A} , jest isomorfní s (a), t. j. $\mathfrak{Z}/\mathfrak{A} \simeq (a)$.

Nechť $n (\geq 0)$ 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 , jest isomorfní s faktorovou grupou na \mathfrak{Z} vytvořenou podgrupou (n) v \mathfrak{Z} . Zejména je tudíž každá cyklická grupa řádu 0 isomorfní s grupou $\mathfrak{Z}/(0)$ a tedy také s grupou \mathfrak{Z} .

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

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

16.5.2 Příklad.

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

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

a tvoří tedy cyklickou grupu $(e^{\frac{2\pi i}{n}})$. Body, jejichž souřadnice jsou reálné a imaginární části těchto kořenů, jsou vrcholy pravidelného n -úhelníka. Na př. pro $n = 6$ máme vrcholy pravidelného 6-úhelníka (viz obr. 13).

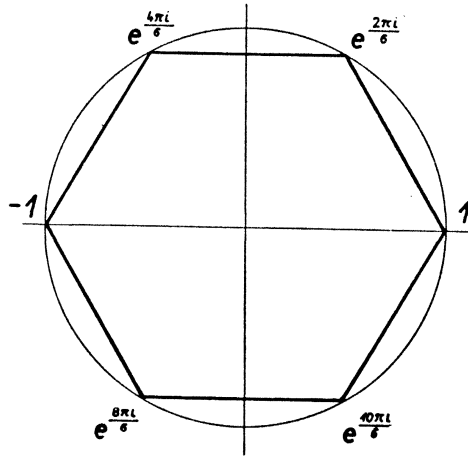
Základní prvky této grupy řádu 6 jsou $e^{\frac{2\pi i}{6}}$, $e^{\frac{10\pi i}{6}}$.

16.6. 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 $a^n = \underline{1}$.

*) Je-li x libovolné reálné číslo, pak e^{ix} , kde $i = \sqrt{-1}$, je definováno vzorcem $e^{ix} = \cos x + i \sin x$.



Obr. 13.

Dále snadno zjistíme, že řád n každého prvku $a \in \mathcal{G}$ je dělitelem řádu N grupy \mathcal{G} , t. j. 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 $\nu \in \mathcal{G}$ je dělitelem řádu grupy \mathcal{G} . Z rovnosti $N = nd$ plyne: $a^N = a^{nd} = (a^n)^d = \underline{1}^d = \underline{1}$ a odtud vychází t. zv. *Fermatova věta pro grupy*:

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

16.7. Vytvoření levých translací ryzími cyklickými permutacemi.

Své úvahy ukončíme poznámkou o vytvoření na př. levých translací nějaké konečné grupy ryzími cyklickými permutacemi.

Nechť \mathcal{G} značí libovolnou konečnou grupu a necht a je libovolný prvek $\nu \in \mathcal{G}$. Jak jsme vyložili v odst. 15.2.1, je levá translace $a^{\mathfrak{t}}$ grupy \mathcal{G} permutací grupy \mathcal{G} a je tedy vytvořena (viz odst. 4.4.5) konečným počtem ryzích cyklických permutací, t. j. existuje rozklad $\bar{G} = \{\bar{a}, \dots, \bar{m}\}$ grupy \mathcal{G} takový, že každý jeho prvek \bar{a}, \dots, \bar{m} je $\nu^{\mathfrak{t}}$ invariantní a částečné permutace $a^{\mathfrak{t}}\bar{a}, \dots, a^{\mathfrak{t}}\bar{m}$ jsou ryzí cyklické permutace prvků \bar{a}, \dots, \bar{m} . Libovolný prvek \bar{x} rozkladu \bar{G} se skládá z prvků cyklu: $x, a^{\mathfrak{t}}x, (a^{\mathfrak{t}})^2x, \dots,$

$(a^t)^{k-1}x$, při čemž x značí libovolný prvek v \bar{x} a k nejmenší přirozené číslo takové, že $(a^t)^kx = x$. Podle definice levé translace a^t máme $a^tx = ax$, $(a^t)^2x = a^2x$, ..., $(a^t)^{k-1}x = a^{k-1}x$ a z rovností $(a^t)^kx = a^kx = x$ plyne $a^k = \underline{1}$. Odtud vidíme, že náš cyklus je $x, ax, a^2x, \dots, a^{k-1}x$, a dále, že množina $\underline{1}, a, a^2, \dots, a^{k-1}$ 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 vytvářejí libovolnou levou translaci a^t v nějaké konečné grupě \mathfrak{G} , platí tedy věta, že *jejich cykly se skládají z těchto prvků jako pravé třídy vzhledem k cyklické podgrupě (a) v grupě \mathfrak{G} .*

16.8. Cvičení.

16.8.1. Prvek $a \neq \underline{1}$ v libovolné grupě \mathfrak{G} má řád 2, když a jen když je sám k sobě inverzní.

✓ 16.8.2. V každé konečné grupě sudého řádu existují prvky řádu 2.

16.8.3. Má-li prvek a libovolné grupy \mathfrak{G} řád n , pak řád každého prvku cyklické podgrupy (a) v \mathfrak{G} , je dělitelem čísla n .

16.8.4. Každá grupa, jejíž řád je prvočíslo, je cyklická.

16.8.5. 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 řád prvku \bar{a} je mocninou nějakého prvočísla p , pak v \bar{a} existuje prvek a , jehož řád je rovněž mocninou prvočísla p .