15. Cyklické grupy

In: Otakar Borůvka (author): Úvod do teorie grup. (Czech). Praha: Královská česká společnost nauk, 1944. pp. 72--77.

Persistent URL: http://dml.cz/dmlcz/401374

Jak víme z teorie grupoidů (odst. 9.), máme ještě třetí větu o grupoidech a ta se týká zákrytu faktoroidu. Nechť $\mathfrak{A}_1$ značí libovolnou invariantní podgrupu v $\mathfrak{G}$ a $\overline{\mathfrak{A}}_2$ libovolnou invariantní podgrupu v grupě tříd $\mathfrak{G}/\mathfrak{A}_1$. Podle třetí věty o isomorfismu grupoidů jest grupa tříd $(\mathfrak{G}/\mathfrak{A}_1)/\overline{\mathfrak{A}}_2$ isomorfní se zákrytem $\overline{\mathfrak{G}}_2$ grupy tříd $\mathfrak{G}/\mathfrak{A}_1$ vynuceným grupou tříd $(\mathfrak{G}/\mathfrak{A}_1)/\overline{\mathfrak{A}}_2$, t. j. $(\mathfrak{G}/\mathfrak{A}_1)/\overline{\mathfrak{A}}_2 \simeq \overline{\mathfrak{G}}_2$ a sice jest isomorfismus zobrazení, v němž jest ke každému prvku $\overline{\overline{a}} \in (\mathfrak{G}/\mathfrak{A}_1)/\overline{\mathfrak{A}}_2$ přiřazen součet $\bar{a} \in \overline{\mathfrak{G}}_2$ všech prvků $a_1 \in \mathfrak{G}/\mathfrak{A}_1$ ležících v $\overline{\overline{a}}$. Podle odst. 13. jest součet všech prvků grupy tříd $\mathfrak{G}/\mathfrak{A}_1$ ležících v $\overline{\mathfrak{A}}_2$ polem jisté invariantní podgrupy $\mathfrak{A}_2$ v $\mathfrak{G}$ a $\overline{\mathfrak{G}}_2$ jest grupa tříd $\mathfrak{G}/\mathfrak{A}_2$; mimoto máme $\overline{\mathfrak{A}}_2 = \mathfrak{A}_2/\mathfrak{A}_1$. Odtud plyne *třetí věta o isomorfismu grup*:

Je-li $\mathfrak{A}_1$ invariantní podgrupa v $\mathfrak{G}$ a $\overline{\mathfrak{A}}_2$ invariantní podgrupa v $\mathfrak{G}/\mathfrak{A}_1$, pak součet prvků grupy tříd $\mathfrak{G}/\mathfrak{A}_1$ ležících v $\overline{\mathfrak{A}}_2$ jest polem jisté invariantní podgrupy $\mathfrak{A}_2$ v $\mathfrak{G}$ a platí vztah

$$(\mathfrak{G}/\mathfrak{A}_1)/(\mathfrak{A}_2/\mathfrak{A}_1) \simeq \mathfrak{G}/\mathfrak{A}_2,$$

při čemž isomorfismus přiřazuje ke každému prvku $\overline{\overline{a}}$ grupy tříd na levé straně součet všech prvků grupy $\mathfrak{G}/\mathfrak{A}_1$ ležících v $\overline{\overline{a}}$.

Cvičení. 1. Realisujte permutacemi abstraktní grupu 4. řádu, jejíž multiplikační tabulka jest napsána jako první na str. 56.!

2. Když jest dána multiplikační tabulka nějaké konečné grupy $\mathfrak{G}$, pak symboly levých translací na $\mathfrak{G}$ obdržíme, když pokaždé opíšeme vodorovné záhlaví a pod ně napíšeme jeden řádek tabulky. Podobně sestavíme ze svislého záhlaví a jednotlivých sloupců symboly pravých translací na $\mathfrak{G}$.

3. Pravidelný osmistěn má celkem 13 os souměrnosti (3 procházejí vždy dvěma protějšími vrcholy, 6 prochází středy vždy dvou protějších hran a 4 středy vždy dvou protějších stěn). Všechna otočení osmistěnu okolo os souměrnosti, která osmistěn převádějí v sebe, tvoří grupu 24. řádu, t. zv. grupu *oktaedrickou* (při tom se otočení okolo téže osy o úhly lišící se o celé násobky 360^0 považují za stejná); označme pro okamžik tuto grupu $\mathfrak{O}$. Každému otočení, které jest prvkem v $\mathfrak{O}$, odpovídá jistá permutace 3 os souměrnosti procházejících vždy dvěma protějšími vrcholy. Když ke každému prvku v $\mathfrak{O}$ přiřadíme příslušnou permutaci, obdržíme deformaci grupy $\mathfrak{O}$ na symetrickou permutační grupu $\mathfrak{S}_3$. Použijte této deformace a dokažte pomocí první a třetí věty o isomorfismu grup, že grupa $\mathfrak{O}$ obsahuje invariantní podgrupy řádů 4, 12!

15. Cyklické grupy.

Libovolná grupa $\mathfrak{G}$ se nazývá *cyklická*, když v ní existuje prvek, t. zv. *základní*, který se vyznačuje tím, že každý prvek v $\mathfrak{G}$ jest jeho mocninou. Když $\mathfrak{G}$ jest cyklická grupa a a její základní prvek, pak grupu

$\mathfrak{G}$ označujeme zpravidla symbolem (a). Z prvního vzorce (1) na str. 52. plyne, že každá cyklická grupa jest abelovská.

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

$$\ldots, a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots; \tag{1}$$

protože každý prvek grupy (a) jest 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 $i - j$, $j - i$ jest přirozené a mocniny prvku a s těmito mocniteli jsou rovny $\underline{1}$, vidíme, že existují přirozená čísla x hovící rovnici $a^x = \underline{1}$. Mezi těmito přirozenými čísly jest jisté číslo nejmenší; označme je n, takže máme $a^n = \underline{1}$. Uvažujme o těchto prvcích grupy (a)

$$\underline{1}, a, a^2, \ldots, a^{n-1}. \tag{2}$$

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 hoví 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 anebo $\geqq n$. 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: $x = qn + r$ a máme $0 \leqq r \leqq n - 1$, takže a^r jest jedním z prvků (2). Ze vzorců (1) na str. 52. 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 jest prvek a^r. Tím jest zjištěno, že grupa (a) se skládá z prvků (2) a má tedy řád n. Dále plyne z naší úvahy, že součin $a^i \cdot a^j$ libovolného prvku a^i s libovolným prvkem a^j grupy (a) jest prvek a^k, kde k značí zbytek dělení čísla $i + j$ číslem n, neboť $a^i \cdot a^j = a^{i+j}$. Shrneme-li naše výsledky o cyklických grupách, vidíme, že *řád n každé cyklické grupy (a) jest buď 0 a v tom případě se grupa (a) skládá z prvků* (1), *anebo $n > 0$ a pak se cyklická grupa (a) skládá z prvků* (2). *Součin $a^i \cdot a^j$ libovolného prvku a^i s libovolným prvkem a^j grupy (a) jest v prvním případě prvek a^{i+j}, kdežto v druhém případě prvek a^k, kde k jest zbytek dělení čísla $i + j$ číslem n. V druhém případě jest n nejmenší přirozené číslo takové, že $a^n = \underline{1}$.* Všimněme si, že v obou případech jest a^{n-i} prvek inversní vzhledem k prvku a^i.

Uvažujme nyní o nějaké podgrupě $\mathfrak{A}$ v cyklické grupě (a)! Když se podgrupa $\mathfrak{A}$ skládá z jediného prvku $\underline{1}$, pak jest 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 inversní prvek a^{-i} a protože jedno z obou čísel i, $-i$ jest přirozené, vidíme, že v podgrupě $\mathfrak{A}$ existují mocniny prvku a, jejichž mocnitelé jsou přirozená čísla. Mezi těmito mocniteli jest jeden nejmenší; označme jej m, takže máme $a^m \in \mathfrak{A}$ 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: $x = qm + r$ a máme $0 \leqq r \leqq m - 1$. Ze vzorců (1) na str. 52. plynou rovnosti $a^x = a^{qm+r} = a^{qm} \cdot a^r$ a odtud vychází, že prvek a^r jest součin prvku a^{-qm} s prvkem a^x. Protože a^{-qm} jest inversní prvek vzhledem k prvku $(a^m)^q$, který jako q-tá mocnina prvku a^m obsaženého v $\mathfrak{A}$ jest rovněž v $\mathfrak{A}$, vidíme, že a^{-qm} jest prvek v $\mathfrak{A}$ a protože také a^x jest prvek v $\mathfrak{A}$, jest i součin $a^{-qm} \cdot a^x$, t. j. prvek a^r, obsažen v podgrupě $\mathfrak{A}$. Odtud vzhledem k nerovnostem $0 \leqq r \leqq m - 1$ a k definici čísla m vychází $r = 0$ a máme $a^x = (a^m)^q$. Tedy jest každý prvek podgrupy $\mathfrak{A}$ jistou mocninou prvku a^m, takže podgrupa $\mathfrak{A}$ jest cyklická a má základní prvek a^m. Touto úvahou jsme došli k výsledku, že *každá podgrupa v cyklické grupě* (a) *jest cyklická*. Protože cyklická grupa (a) jest abelovská, jest v ní každá podgrupa invariantní.

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) jest základní. Pak zejména prvek a jest 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} býti 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 společnou míru 1, jinak řečeno, jejichž mocnitelé jsou s číslem n $(= 0)$ nesoudělní. Uvažujme nyní o případu $n > 0$. Cyklická grupa (a) se skládá z prvků $\underline{1}, a, a^2, \ldots, a^{n-1}$. Značí-li r zbytek dělení čísla vq číslem n, takže $vq = nq' + r$, kde q' jest podíl a $0 \leqq r \leqq n - 1$, máme $a^{vq} = a^r = a$ a odtud plyne $r = 1$, neboť a, a^r jsou z řady $\underline{1}, a, a^2, \ldots, a^{n-1}$, 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 $vq - nq' = 1$ (v. pozn. pod čarou na str. 39.) a odtud plyne pro každé celé číslo i: $i = v(qi) - n(q'i)$ a máme $a^i = (a^v)^{qi}$, takže a^v jest 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, že *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 jest v řadě $1, 2, \ldots, n$ čísel nesoudělných s n.

Důležitým příkladem cyklické grupy řádu 0 jest grupa $\mathfrak{Z}$ a sice jest $\mathfrak{Z} = (1)$. Všechny podgrupy v $\mathfrak{Z}$ se skládají, jak víme, ze všech celých násobků vždy nějakého nezáporného čísla n a jsou tedy, v souhlase s hořejším výsledkem, cyklické grupy (n). Nechť $n \geqq 0$ a uvažujme o grupě tříd $\mathfrak{Z}/(n)$. 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 grupa tříd $\mathfrak{Z}/(n)$ řád n. Snadno ukážeme, že grupa tříd $\mathfrak{Z}/(n)$ jest cyklická a má základní prvek $\bar{a}_1$. Skutečně, podle definice násobení v $\mathfrak{Z}/(n)$ jest 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 jest zejména $\bar{a}_i = \bar{a}_1{}^i$ a tím jest naše tvrzení dokázáno. Současně jest tím zjištěno, že existují cyklické grupy libovolného řádu $n \geqq 0$.

Avšak nejen každá grupa tříd na grupě $\mathfrak{Z}$ jest cyklická, nýbrž i naopak jest každá cyklická grupa isomorfní s jistou grupou tříd 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 celé číslo, jest 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 jest homomorfismus. Vychází tedy především, že cyklická grupa (a) jest homomorfní s grupou $\mathfrak{Z}$. Podle první věty o isomorfismu grup, tvoří množina všech vzorů v $\boldsymbol{d}$ jednotky grupy (a) invariantní podgrupu $\mathfrak{A}$ v $\mathfrak{Z}$ a grupa tříd na $\mathfrak{Z}$ vytvořená invariantní podgrupou $\mathfrak{A}$ jest isomorfní s (a), t. j. $\mathfrak{Z}/\mathfrak{A} \simeq (a)$. Nechť n $(\geqq 0)$ značí řád cyklické grupy (a). Pak také $\mathfrak{Z}/\mathfrak{A}$ má řád n a tedy se podgrupa $\mathfrak{A}$ skládá ze všech celých násobků čísla n. Vychází tedy, že cyklická grupa (a), řádu n, jest isomorfní s grupou tříd na $\mathfrak{Z}$ vytvořenou podgrupou (n) v $\mathfrak{Z}$. Zejména jest tedy každá cyklická grupa řádu 0 isomorfní s grupou $\mathfrak{Z}/(0)$ a tedy také s grupou $\mathfrak{Z}$.

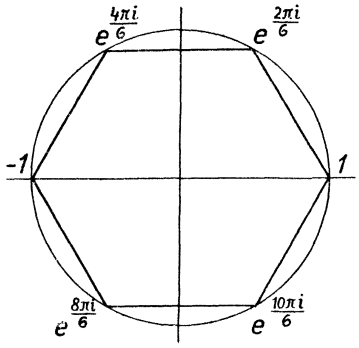
Zřejmě jest každá grupa isomorfní s nějakou cyklickou grupou řádu n $(\geqq 0)$ opět cyklická a má řád n. Naše úvahy obsahují tedy tento výsledek: *Všechny cyklické grupy řádu* $n \geqq 0$ *jsou representovány grupou*

tříd $\mathfrak{Z}/(n)$ *na grupě* $\mathfrak{Z}$ *a to v tom smyslu, že každá cyklická grupa řádu* n *jest isomorfní s* $\mathfrak{Z}/(n)$ *a naopak, každá grupa isomorfní s touto grupou tříd jest cyklická a má řád* n.

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

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

a tvoří tedy cyklickou grupu $(e^{\frac{2\pi i}{n}})$. Body, jejichž souřadnice jsou reální a imaginární části těchto kořenů, jsou vrcholy pravidelného n-úhelníka. Na př. pro $n = 6$ máme vrcholy pravidelného 6-úhelníka (v. obr. 11.). Základní prvky této grupy řádu 6 jsou $e^{\frac{2\pi i}{6}}, e^{\frac{10\pi i}{6}}$.



Obr. 11.

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 jest 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* $a \in \mathfrak{G}$ *jest dělitelem řádu* N *grupy* $\mathfrak{G}$, t. j. že platí rovnost $N = nd$, kde d značí vhodné celé číslo. Toto tvrzení jest důsledkem toho (str. 60.), že řád každé podgrupy v $\mathfrak{G}$ jest dělitelem řádu grupy $\mathfrak{G}$. 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 *jest* N*-tá mocnina libovolného prvku jednotka grupy.*

Naše úvahy ukončíme poznámkou o vytvoření na př. levých translací nějaké konečné grupy ryzími cyklickými permutacemi. Nechť $\mathfrak{G}$ značí libovolnou konečnou grupu a a libovolný prvek v $\mathfrak{G}$. Jak jsme vyložili v odst. 14., jest levá translace ${}_at$ grupy $\mathfrak{G}$ permutací grupy $\mathfrak{G}$ a jest tedy vytvořena (v. odst. 4.) konečným počtem ryzích cyklických permutací, t. j. existuje rozklad $\overline{G} = \{\overline{a}, \ldots, \overline{m}\}$ grupy $\mathfrak{G}$ takový, že každý jeho prvek $\overline{a}, \ldots, \overline{m}$ jest v ${}_at$ invariantní a částečné permutace ${}_at_{\overline{a}}, \ldots, {}_at_{\overline{m}}$ jsou ryzí cyklické permutace prvků $\overline{a}, \ldots, \overline{m}$. Libovolný prvek $\overline{x}$ rozkladu

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

$\overline{G}$ se skládá z prvků cyklu x, ${}_a\boldsymbol{t}x$, $({}_a\boldsymbol{t})^2x$, ..., $({}_a\boldsymbol{t})^{k-1}x$, při čemž x značí libovolný prvek v $\bar{x}$ a k nejmenší přirozené číslo takové, že $({}_a\boldsymbol{t})^k x = x$. Podle definice levé translace ${}_a\boldsymbol{t}$ máme ${}_a\boldsymbol{t}x = ax$, $({}_a\boldsymbol{t})^2x = a^2x$, ..., $({}_a\boldsymbol{t})^{k-1}x = a^{k-1}x$ a z rovností $({}_a\boldsymbol{t})^k x = a^k x = x$ plyne $a^k = \underline{1}$. Odtud vidíme, že náš cyklus jest x, ax, a^2x, ..., $a^{k-1}x$ a dále, že množina $\underline{1}, a, a^2, \ldots, a^{k-1}$ jest pole cyklické podgrupy (a) v $\mathfrak{G}$. Prvek $\bar{x}$ jest tedy pravá třída prvku x vzhledem k cyklické podgrupě (a) a odtud plyne dále, že $\overline{G}$ jest pravý rozklad grupy $\mathfrak{G}$ vytvořený cyklickou podgrupou (a). O ryzích cyklických permutacích, které vytvořují libovolnou levou translaci ${}_a\boldsymbol{t}$ v nějaké konečné grupě $\mathfrak{G}$, platí tedy věta, že *jejich cykly se skládají z těchže prvků jako pravé třídy vzhledem k cyklické podgrupě* (a) *v grupě* $\mathfrak{G}$.

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

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 $\mathfrak{G}$, jest dělitelem čísla n.

4. Každá grupa, jejíž řád jest prvočíslo, jest cyklická.

5. Řád každého prvku $\bar{a}$ libovolné grupy tříd na nějaké konečné grupě $\mathfrak{G}$ jest dělitelem řádu každého prvku v $\mathfrak{G}$ obsaženého v $\bar{a}$. Když řád prvku $\bar{a}$ jest mocninou nějakého prvočísla p, pak v $\bar{a}$ existuje prvek a, jehož řád jest rovněž mocninou prvočísla p.