Učební texty k přednášce ALGEBRAICKÉ STRUKTURY
Michal Marvan, Matematický ústav
Slezská univerzita v Opavě

12. Cyklické grupy

Buď G grupa, $g \in G$ její prvek a $k \in \mathbf{Z}$ celé číslo. Položme

$$g^k := \begin{cases} \underbrace{g \cdots g}_{k} & \text{pro } k > 0, \\ 1 & \text{pro } k = 0, \\ \underbrace{g^{-1} \cdots g^{-1}}_{-k} & \text{pro } k < 0. \end{cases}$$

Tvrzení. *Buď G grupa, $g \in G$, $k, l \in \mathbf{Z}$. Pak platí*

$$g^k \cdot g^l = g^{k+l},$$
$$(g^k)^l = g^{kl}.$$

Důkaz. Cvičení.

Tvrzení. *Buď G grupa, $g \in G$. Pak $\overline{\{g\}} = \{g^k \mid k \in \mathbf{Z}\}$.*

Důkaz. "$\supseteq$": $\{g^k \mid k \in \mathbf{Z}\}$ je podgrupa v G (plyne z předch. tvrzení) a obsahuje prvek g. Proto obsahuje celou podgrupu $\overline{\{g\}}$.

"$\subseteq$": Každá podgrupa v G obsahující g obsahuje i všechny prvky g^k. Speciálně to platí pro podgrupu $\overline{\{g\}}$.

Definice. Grupa G s jedním generátorem, tj. taková, že $G = \overline{\{g\}}$ pro nějaké $g \in G$, se nazývá *cyklická*.

Tvrzení. *Buď G cyklická grupa.*
(a) *Je-li G nekonečná, pak $G \cong \mathbf{Z}$.*
(b) *Je-li G m-prvková, $m \in \mathbf{N}$, pak $G \cong \mathbf{Z}_m$ (klademe $\mathbf{Z}_1 = \{1\}$).*

Důkaz. Buď G cyklická grupa, g její generátor. Rozeznávejme dva případy:

Případ 1. $g^k \neq g^l$ pro všechna $k \neq l$. Prvky g^k, $k \in \mathbf{Z}$ jsou pak navzájem různé a grupa G je nutně nekonečná. Zaveďme zobrazení

$$f : \mathbf{Z} \to G = \{g^k \mid k \in \mathbf{Z}\},$$
$$f : k \mapsto g^k.$$

Podle předpokladu je toto zobrazení injektivní. Zřejmě je $\operatorname{Im} f = \{g^k \mid k \in \mathbf{Z}\} = G$, a proto je f též surjektivní. Navíc je f homomorfismus. Skutečně, podle předchozího tvrzení máme $g^{k+l} = g^k \cdot g^l$, dále $g^0 = 1$ a $g^{-k} = (g^k)^{-1}$. Tudíž, f je izomorfismus $G \cong \mathbf{Z}$.

Případ 2. Existují čísla $k, l \in \mathbf{Z}$ taková, že $k \neq l$ a $g^k = g^l$. Zobrazení f v tomto případě není injektivní. Připomeňme však, že existuje kongruence κ_f definovaná předpisem $k \mathrel{\kappa_f} l \Leftrightarrow g^k = g^l$, přičemž $G = \operatorname{Im} f \cong G/\kappa_f$.

Bez újmy na obecnosti $k > l$. Položme $n := k - l > 0$; potom $g^n = g^{k-l} = g^k \cdot (g^l)^{-1} = 1$, protože $g^k = g^l$. Označme

$$M = \{n \in \mathbf{Z} \mid g^n = 1\}.$$

V množině M, jak již víme, leží alespoň jedno kladné číslo. Proto existuje i nejmenší kladné číslo ležící v M, označme je m. Můžeme říci, že m je minimální kladný exponent takový, že $g^m = 1$. Ukážeme, že $G \cong \mathbf{Z}_m$.

Nejprve prozkoumejme množinu M. V M zřejmě leží všechny celočíselné násobky čísla m. Vskutku, $g^{q \cdot m} = (g^m)^q = 1^q = 1$ pro libovolné $q \in \mathbf{Z}$.

Dokažme, že v M žádné jiné prvky nejsou, tj. že všechny prvky množiny M jsou celočíselným násobkem čísla m. Buď $n \in M$ libovolné. Proveďme dělení se zbytkem

$$n = q \cdot m + r, \quad q, r \in \mathbf{Z}, \quad 0 \leq r < m.$$

Potom $g^r = g^{n-qm} = g^n \cdot g^{-qm} = 1 \cdot 1^{-q} = 1$. Vidíme, že $r \in M$. Přitom však $0 \leq r < m$. Kdyby $r > 0$, pak by bylo kladným číslem ležícím v M, a proto by muselo být $m \leq r$, což není. Tudíž, $r = 0$ a n je násobkem m.

Zaveďme nyní zobrazení

$$G \xrightarrow{f} \mathbf{Z}_m,$$

$$g^k \mapsto [k]_m.$$

Nejprve ukažme, že f je dobře definované zobrazení. Nechť $g^k = g^l$, je nutno ukázat, že potom $[k]_m = [l]_m$. Ovšem $g^{k-l} = 1$, takže $k - l \in M$, a proto je $k - l$ dělitelné číslem m, což ovšem znamená, že $[k]_m = [l]_m$.

Snadno se vidí, že zobrazení f je injektivní. Vskutku, je-li $f(g^k) = f(g^l)$, pak $[m]_s = [n]_s$ pak $m = s \cdot g + n$; $g^m = g^{sq} \cdot g^n = 1 \cdot g^n = g^n$.

Homomorfnost: $f(g^m \cdot g^n) = f(g^{m+n}) = [m + n]_s = [m]_s + [n]_s = f(g^m) + f(g^n)$.

$G, \mathbf{Z}_s$ mají stejný počet prvků, proto h je bijekce, tedy izomorfismus.

Důsledek. *Každá cyklická grupa je komutativní.*

Buď $g \in G$ takový prvek, že $\overline{\{g\}}$ je konečná, řekneme m-prvková. Číslo m se nazývá řád prvku g. Je-li $\overline{\{g\}}$ nekonečná, hovoříme o prvku nekonečného řádu. Počet prvků konečné grupy G se nazývá řád grupy G.

Lagrangeova věta. *Buď G konečná grupa, $g \in G$. Pak řád prvku g dělí řád grupy G.*

Důkaz. Řád podgrupy dělí řád grupy, protože třídy pravého rozkladu podle podgrupy jsou v bijekci, a proto mají stejné počty prvků.

Příklad. Uveďme příklady všech grup o ne více než šesti prvcích.

Počet prvků	
1	$(\{0\}, +)$
2	$(\mathbf{Z}_2, +)$
3	$(\mathbf{Z}_3, +)$
4	$(\mathbf{Z}_4, +)$, $\mathbf{Z}_2 \times \mathbf{Z}_2$ (součin grup)
5	$(\mathbf{Z}_5, +)$
6	$(\mathbf{Z}_6, +)$, Σ_3

Zde Σ_3 značí grupu všech permutací na tříprvkové množině, je to jediná nekomutativní grupa v tabulce.

Příklad. Ukažme, že grupa $\mathbf{Z}_4$ není izomorfní součinu $\mathbf{Z}_2 \times \mathbf{Z}_2$.
Tabulka sčítání v grupě $\mathbf{Z}_2 \times \mathbf{Z}_2$ je

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

Vidíme, že všechny prvky a grupy $\mathbf{Z}_2 \times \mathbf{Z}_2$ splňují $a + a = 0$. Kolik prvků stejné vlastnosti existuje v grupě $\mathbf{Z}_4$? U izomorfních grup by tyto počty byly nutně stejné.

Cvičení. Najděte izomorfismus $\mathbf{Z}_6 \cong \mathbf{Z}_2 \times \mathbf{Z}_3$. Návod: Zbytkové třídě $[a]_6$ přiřaďte dvojici $[a]_2, [a]_3$.

Věta. *Každá p-prvková grupa, kde p je prvočíslo, je cyklická.*

Důkaz. Je to důsledek Lagrangeovy věty. Buď $(G, \cdot, 1, ^{-1})$ grupa. Nechť $r(a)$ označuje řád prvku $a \in G$. Pokud G má jen jeden prvek, tvrzení platí. Jinak existuje prvek $a \neq 1$. Pak podle Lagrangeovy věty $r(a) \mid p$, a tedy $r(a) = 1$ nebo $r(a) = p$. V prvním případě $a \cdot a = a$, a tedy $a = 1$, což jsme vyloučili. Tudíž nastává druhý případ, $r(a) = p$, načež $\overline{\{a\}} = G$, protože $\overline{\{a\}} \subseteq G$ a mají stejně prvků. To znamená, že G je cyklická.