Úvod do teorie grup

Zápisky z přednášky doc. Mgr. Jana Šarocha. Ph.D.

Dominik Doležel

Úvodní informace

- skripta: DRÁPAL, Aleš. *Teorie grup: základní aspekty.* Praha: Karolinum, 2000.
- email: saroch@karlin.mff.cuni.cz

Značení

Množinou přirozených čísel rozumíme množinu $\mathbb{N} = \{1, 2, \dots\}$, pak je $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Zobrazení skládáme zprava doleva, tj. jsou-li $f : A \to B$, $g : B \to C$ dvě zobrazení, pak $g \circ f = gf : A \to C$, tj. pro $a \in A$ je $(g \circ f)(a) = g(f(a))$. Identické zobrazení z A do A značíme id_A nebo $\mathtt{1}_A$.

Kapitola 1

Operátorové grupy

Definice 1. Ať Ω je množina. Množina G spolu s:

(i) binární operací $\cdot : G \times G \to G$ (zapisujeme infixem[1]),

(ii) unární operací $^{-1} : G \to G$ (zapisujeme postfixem[2]),

(iii) nulární operací, tj. konstantou $1 \in G$,

(iv) unárními operacemi $\omega \in \Omega : G \to G$ (zapisované prefixem[3])

se nazývá **Ω-grupou**, pokud:

(i) $\cdot$ je asociativní, tj. $\forall a, b, c \in G : (a \cdot b) \cdot c = a \cdot (b \cdot c)$,

(ii) 1 je **neutrální prvek** vzhledem k operaci $\cdot$, tj. $\forall a \in G : a \cdot 1 = 1 \cdot a = a$,

(iii) $\forall a \in G$ je a^{-1} **inverzní prvek** k a, tj. $a \cdot a^{-1} = a^{-1} \cdot a = 1$,

(iv) $\forall \omega \in \Omega$ je ω **slučitelná s** operací $\cdot$, tj. $\forall a, b \in G : \omega(a \cdot b) = \omega(a) \cdot \omega(b)$.

Poznámka 1.

i. Je-li $\Omega = \emptyset$, pak místo o Ω-grupě hovoříme jen o **grupě**.

ii. Pro všechna $a, b, c \in G$ platí:

$$(a \cdot b = a \cdot c \implies b = c) \wedge (b \cdot a = c \cdot a \implies b = c).$$

Dokážeme aplikací $a^{-1}\cdot$:

$$\begin{aligned} a^{-1} \cdot (a \cdot b) &= a^{-1} \cdot (a \cdot c) \\ (a^{-1} \cdot a) \cdot b &= (a^{-1} \cdot a) \cdot c \\ 1 \cdot b &= 1 \cdot c. \end{aligned}$$

[1] mezi argumenty
[2] za argumentem
[3] před argumentem, tady $\omega(\ )$

iii. Z předchozího plyne $\left(a^{-1}\right)^{-1} = a$, neboť

$$a^{-1} \cdot \left(a^{-1}\right)^{-1} = a^{-1} \cdot a \implies a = \left(a^{-1}\right)^{-1}.$$

iv. Inverzní k $a \in G$ je právě jeden prvek, a sice a^{-1}. Neutrální prvek vzhledem k operaci $\cdot$ je právě jeden, a sice 1. (Sporem předpokládejme, že existuje i $1' \neq 1$, ale zároveň $a \cdot 1 = a \cdot 1' \implies 1 = 1'$, což je spor.)

v. Symbol $\cdot$ se často nepíše.

Definice 2. Ať G je Ω-grupa. **Řádem** Ω-grupy G rozumíme mohutnost množiny G, značíme $|G|$ nebo $\operatorname{ord} G$.

Definice 3. Buďte G, H Ω-grupy, $f : G \to H$ zobrazení. Řekneme, že f je **homomorfismus** Ω-grup G, H, jestliže

(i) $\forall a, b \in G : f(a \cdot b) = f(a) \cdot f(b)$ a

(ii) $\forall a, b \in G, \forall \omega \in \Omega : f(\omega(a)) = \omega(f(a))$.

Lemma 1. *Je-li $f : G \to H$ homomorfismus Ω-grup, pak $f(1) = 1$ a $\forall a \in G : f\left(a^{-1}\right) = (f(a))^{-1}$.*

Důkaz. Platí:

$$1 \cdot f(1) = f(1) = f(1 \cdot 1) = f(1) \cdot f(1) \implies f(1) = 1.$$

Dále

$$f(a^{-1}) \cdot f(a) = f(a^{-1} \cdot a) = f(1) = 1,$$

ale taky

$$f(a) \cdot f(a^{-1}) = f(a \cdot a^{-1}) = f(1) = 1,$$

odkud plyne $f(a^{-1}) = (f(a))^{-1}$, jelikož jediný inverzní prvek k $f(a)$ je pouze $(f(a))^{-1}$. □

Definice 4. Ať $f : G \to H$ je homomorfismus Ω-grup. Pak f je:

(i) **izomorfismus**, jestliže f je bijektivní;

(ii) **endomorfismus** (**grupy G**), jestliže $G = H$;

(iii) **automorfismus**, jestliže je f endomorfismus a izomorfismus.

Cvičení 1. *Ať $f : G \to H$ je homomorfismus Ω-grup. Ukažte, že f je izomorfismus právě tehdy, když existuje homomorfismus $g : H \to G$ tak, že $f \circ g = \mathrm{id}_G$ a $g \circ f = \mathrm{id}_H$.*

Lemma 2. *(i) Ať $f : G \to H$, $g : H \to K$ jsou homomorfismy Ω-grup. Pak $g \circ f$ je homomorfismus.*

(ii) Je-li $f : G \to H$ homomorfismus, pak $f^{-1} : H \to G$ je opět homomorfismus.

Důkaz. (i) Snadné.

(ii) f^{-1} je jistě bijekce, ověříme jen, že f^{-1} je homomorfismus. Počítejme

$$f\left(f^{-1}(a)\cdot f^{-1}(b)\right) = f\left(f^{-1}(a)\right)\cdot f\left(f^{-1}(b)\right) = a\cdot b.$$

Na tuto rovnost aplikujeme f^{-1}:

$$f^{-1}(a)\cdot f^{-1}(b) = f^{-1}(a\cdot b).$$

Ať $\omega\in\Omega$, $a\in H$ jsou libovolná. Pak

$$f\left(\omega\left(f^{-1}(a)\right)\right) = \omega\left(f\left(f^{-1}(a)\right)\right) = \omega(a).$$

Opět aplikujeme f^{-1}:

$$\omega\left(f^{-1}(a)\right) = f^{-1}\left(\omega(a)\right),$$

což jsme chtěli dokázat. □

Definice 5. Pokud je v Ω-grupě G operace $\cdot$ komutativní, tj.

$$\forall a,b\in G : a\cdot b = b\cdot a,$$

potom nazýváme G **komutativní** (též **abelovskou**) Ω-grupou.

Příklad 1. 1. $\Omega=\emptyset$:

- $(\mathbb{Z},+,-,0)$ je abelovská grupa
- X je množina, $S(X)=\{\sigma : X\to X, \sigma \text{ bijekce}\}$
  s operacemi $\circ$ (skládání zobrazení), $^{-1}$ (inverzní zobrazení), $\mathtt{1}$ (identické zobrazení)
  $S(x)$ je abelovská právě tehdy, když $|X|<3$. Je-li $X=\{1,2,\dots,n\}, n\in\mathbb{N}$, pak $S(X):=S_n$[4].
- R je okruh, pak $(R,+,-,0)$ je abelovská grupa,
  $(R^*,\cdot,^{-1},\mathtt{1})$, kde $R^*=\{r\in R, \exists s\in R, r\cdot s=s\cdot r=\mathtt{1}\}$ je grupa invertibilních prvků
- $n\in\mathbb{N}, T$ je těleso, $M_n(T)$ je okruh matic $n\times n$ nad tělesem T
  $(M_n(T))^*=\{A\in M_n(T), \det(A)\neq 0\}:=GL_n(T)$[5]
- Ať $G=(V,E)$ je neorientovaný graf. Pak $Aut(G)=\{f:V\to V, f \text{ automorfismus grafu } G\}$.
  Speciálně pro graf C_n, $n\in\mathbb{N}\setminus\{1,2\}$ platí $Aut(C_n):=D_{2n}=D_n\leq S_n$.

2. $\Omega\neq\emptyset$:
   T je (komutativní) těleso, V je vektorový prostor nad T. Pak $(V,+,-,0)$ je abelovská grupa, $\Omega=\{\cdot t : V\to V, t\in T\}$. V je Ω-grupa.
   Obecněji: R je okruh, M je (pravý) modul nad R. Například je-li $M=N_{2\times 3}(T)$, pak

[4] symetrická grupa na n prvcích
[5] zobecněná lineární grupa

$\left(M, +, -, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}\right)$ je abelovská grupa. Je-li $R = M_3(T)$, M je pravý R modul, pak M je Ω-grupa.

Definice 6. Ať G je Ω-grupa, $A \subseteq G$. Pak A nazveme **Ω-podgrupou** Ω-grupy G, píšeme $A \leq G$, pokud:

(i) $1 \in A$,

(ii) $\forall a, b \in A : a \cdot b \in A$ a $a^{-1} \in A$,

(iii) $\forall a \in A : \forall \omega \in \Omega : \omega(a) \in A$.

Důsledek 1. Ať G je Ω-grupa. Množina $Aut(G)$ všech automorfismů Ω-grupy G tvoří spolu s operacemi $\circ, ^{-1}, \mathrm{id}_G$ grupu. Platí $Aut(G) \leq S(G)$.

Důsledek 2. Ať G je Ω-grupa, $\omega \in \Omega$. Pak $\omega : G \to G$ je endomorfismus grupy G (tj. $\emptyset$-grupy G). Mj. platí, že $\omega(1) = 1$, $\omega\left(a^{-1}\right) = (\omega(a))^{-1} \forall a \in G$.

Důkaz. Plyne ihned z 1. □

Poznámka 2. Často je přímo $\Omega \subseteq End(G) = \{f : G \to G, f \text{ je endomorfismus grupy } G\}$.

Lemma 3. *Ať G je grupa, $g \in G$ libovolné. Označme $\alpha_G : G \to G$ takové, že $\forall a \in G : \alpha_G(a) = gag^{-1}$. Pak je $\alpha_g \in Aut(G)$ a nazývá se vnitřní automorfismus určený prvkem g.*