# Cvičenie 1 – grupy, podgrupy

## Grupy

**Definícia 1.** Grupa je dvojica $(G, \circ)$, kde $G$ je množina a $\circ$ je binárna operácia $\circ$ na $G$, pričom

(i) pre všetky $a, b, c \in G$ platí $a \circ (b \circ c) = (a \circ b) \circ c$. (asociatívnosť)

(ii) existuje prvok $e \in G$ tak, že pre všetky $a \in A$ platí $a \circ e = a = e \circ a$. (neutrálny prvok)

(iii) ku každému prvku $a \in G$ existuje prvok $b \in G$ tak, že $a \circ b = b \circ a = e$. (inverzný prvok)

Ak je navyše operácia $\circ$ komutatívna, $G$ sa nazýva *komutatívna* (*abelovská*) *grupa.*

Inverzný prvok k $a$ v grupe $G$ je prvkom $a$ jednoznačne určený, zvyčajne sa označuje $a^{-1}$. V grupe platia *zákony o krátení,* čiže pre každé $a, b, c \in G$ platí:

$$a \circ b = a \circ c \ \Rightarrow \ b = c$$
$$b \circ a = c \circ a \ \Rightarrow \ b = c$$

1. Nech $(G, *)$ je grupa. Dokážte:
   a) $x * y = y * x \Leftrightarrow x * y * x^{-1} * y^{-1} = e$.
   b) Ak $x * x = e$ pre všetky $x \in G$, tak $G$ je komutatívna.

2*. Nech $*$ je asociatívna binárna operácia na množine $G \neq \emptyset$. Nech pre každé $a, b \in G$ majú rovnice $a * x = b$, $y * a = b$ riešenia v $G$. (Inými slovami, pre každé $a, b \in G$ existujú $x \in G$ a $y \in G$ také, že $a * x = b$, $y * a = b$.) Dokážte, že $(G, *)$ je grupa. (Hint: Skúste začať dôkazom existencie ľavého a pravého neutrálneho prvku.)

3. Nech $(G, \cdot)$ je grupa a $P(G)$ je systém všetkých podmnožín $G$. Dokážte, že operácia $\cdot$ na množine $P(G)$ daná predpisom

$$A \cdot B = \{a \cdot b; a, b \in G\}$$

   je asociatívna. Tvorí $P(G) \setminus \{\emptyset\}$ s touto operáciou grupu?

4*. Každá konečná grupa s párnym počtom prvkov obsahuje prvok $x$ taký, že $x = x^{-1}$.

5. Ak $(G, *_G)$ a $(H, *_H)$ sú grupy, tak aj $G \times H$ s operáciou $(a, b) * (a', b') = (a *_G a', b *_H b')$ je grupa.

6. Matice typu $n \times n$, ktorých determinant je rovný 1, s operáciou násobenia matíc tvoria grupu.

7. Nech $G$ je množina všetkých funkcií $f_{a,b} \colon \mathbb{R} \to \mathbb{R}$, ktoré sú tvaru $f_{a,b}(x) = ax + b$ pre nejaké reálne čísla $a, b \in \mathbb{R}$. Tvorí táto množina funkcií s operáciou skladania zobrazení grupu? Je množina $\{f_{a,b}; a, b \in \mathbb{R}, a \neq 0\}$ s operáciou skladania zobrazení grupa? Dostaneme grupu, ak vezmeme len také $a, b \in \mathbb{R}$, že $a = 1$? V tých prípadoch, keď dostaneme grupu, je táto grupa komutatívna?

8. Označme:
   $M_1 = \{f \colon \mathbb{Z} \to \mathbb{Z}; f \text{ je bijekcia}\}$
   $M_2 = \{f \in M_1; f(n) = n \text{ pre všetky celé čísla } n \text{ až na konečný počet}\}$
   $M_3 = \{f \in M_1; f(n) = n \text{ len pre konečný počet } n\}$.
   Ktoré z množín $M_1$, $M_2$, $M_3$ tvoria grupu spolu s operáciou skladania zobrazení?

9. Doplňte nasledujúcu tabuľku

|   | a | b | c | d |
|---|---|---|---|---|
| a |   |   |   |   |
| b |   |   |   | d |
| c |   |   | d |   |
| d |   |   |   |   |

tak aby ste dostali grupu.

## Podgrupy

Nech $(G, *)$ je grupa a $H \subseteq G$ je ľubovoľná podmnožina $G$. Hovoríme, že $H$ je *podgrupa* grupy $G$, ak $H$ s binárnou operáciou $*$ zúženou na podmnožinu $H$ tvorí grupu.

Ak $H \neq \emptyset$, tak $H$ je podgrupa $\Leftrightarrow$ $(\forall a, b \in H)\ a * b \in H \wedge a^{-1} \in H$ (uzavretosť na operáciu $*$ a inverzné prvky) $\Leftrightarrow$ $(\forall a, b \in H)\ a^{-1}b \in H$.

V prípade, že $H \neq \emptyset$ je <u>konečná</u> podmnožina $G$, tak $H$ je podgrupa $\Leftrightarrow$ $(\forall a, b \in H)$ $a * b \in H$.

Ak $A \subseteq G$, tak najmenšiu podgrupu $G$ obsahujúca $A$ označujeme $[A]$ a voláme ju *podgrupa generovaná množinou A.*

1. Nájdite všetky podgrupy $(\mathbb{Z}_6, \oplus)$.

2. Dokážte: Ak $H$ je podgrupa grupy $(G, \cdot)$ tak $H^2 = H \cdot H \subset H$. (Tu $\cdot$ označuje binárnu operáciu na $P(G)$, ktorú sme definovali v úlohe 3 v časti o grupách.)

3. Ak $A, B, C$ sú podgrupy $G$ a $C \subseteq A \cup B$, tak $C \subseteq A$ alebo $C \subseteq B$.

4. Tvoria pri sčitovaní/násobení matíc grupu štvorcové matice $n \times n$, ktoré sú: symetrické, antisymetrické, diagonálne, regulárne, horné trojuholníkové… (V princípe si môžete vymyslieť čokoľvek zmysluplné, bolo by však dobre pre obe operácie nájsť aspoň po jednom príklade, kedy to nie je grupa a po jednom príklade kedy to grupa je. V oboch prípadoch nám stačí overovať kritérium podgrupy namiesto celej definície grupy.)

5. Nájdite príklad nekonečnej grupy, ktorá obsahuje netriviálnu konečnú podgrupu. (Pod netriviálnou podgrupou rozumieme podgrupu, ktorá má viac ako jeden prvok.)

6. Matice typu $n \times n$, ktoré v každom riadku a každom stĺpci majú práve jednu jednotku a ostatné prvky sú nulové, s operáciou násobenia matíc tvoria grupu.

7. Ukážte, že $H = \{\frac{m}{n}; m, n \text{ sú nepárne}\}$ je podgrupa grupy $(\mathbb{Q} \setminus \{0\}, \cdot)$.

8. Nájdite všetky podgrupy grupy $\mathbb{Z}_2 \times \mathbb{Z}_2$ (súčin dvoch grúp sme definovali na minulom cvičení) a všetky podgrupy grupy $\mathbb{Z}_4$ (v oboch prípadoch operácia $\oplus$). Majú tieto grupy rovnaký počet dvojprvkových podgrúp? (Z toho, čo sa naučíme neskôr – pravdepodobne na najbližšej prednáške – sa na základe tejto úvahy bude dať zdôvodniť, že tieto dve grupy nie sú izomorfné.)

9. Dokážte, alebo vyvráťte: Ak $H_1$ je podgrupa $G_1$ a $H_2$ je podgrupa $G_2$, tak $H_1 \times H_2$ je podgrupa $G_1 \times G_2$.

10. Nech $V$ je vektorový priestor nad poľom $\mathbb{R}$. Je aj každá podgrupa grupy $(V, +)$ podpriestorom priestoru $V$? Ako je to s vektorovými priestormi nad poľom $\mathbb{Z}_p$?

11. Nech $H$ je vlastná podgrupa grupy $G$ (t.j. $H \neq G$). Dokážte, že $[G - H] = G$.