1. Definujte grupu. Důležitou třídou grup jsou komutativní grupy, ty si dokonce vysloužily vlastní jméno a říkáme jim Abelovy (abelovské). Připomeňte i definici komutativity.

2. Je daná operace binární operací (a) na množině $\mathbb{R}$, (b) na množině kladných přirozených čísel $\mathbb{N}^+$?

   (a) sčítání,

   (b) odčítání,

   (c) dělení,

   (d) násobení

3. Najděte příklady binární operace na vhodné množině, která

   (a) je asociativní i komutativní,

   (b) je asociativní, ale není komutativní,

   (c) není ani komutativní, ani asociativní,

   (d) je komutativní, ale není asociativní.

4. Pro kladné celé číslo n a dvě celá čísla a, b řekneme, že a, b jsou kongruentní modulo n psáno $a \equiv b \pmod{n}$, právě když n dělí $a - b$ (tedy $a - b$ je celočíselným násobkem n). Ověřte, jestli následující jsou grupy, případně Abelovy grupy:

   (a) Regulární matice $\mathbb{R}^{12\times 12}$ s operací $\circ$ maticové násobení.

   (b) $(\mathbb{N}, \circ)$, kde $a \circ b = \max\{a, b\}$.

   (c) Binární čísla dlouhá n číslic (2^n) a operace je xor (exkluzivní or, tedy $0 \oplus 0 = 1 \oplus 1 = 0$ a $1 \oplus 0 = 0 \oplus 1 = 1$. Pro více bitová čísla počítáme po jednotlivých složkách, tedy například $1100 \oplus 0111 = 1011$.

   (d) Nosná množina jsou dvojice reálných čísel (píšeme $\mathbb{R}^2$) a binární operace je dána $(a_1, a_2) \circ (b_1, b_2) = (a_1b_1 - a_2b_2, a_1b_2 + a_2b_1)$.

   (e) Otočení čtverce.

   (f) Otočení a symetrie čtverce.

   (g) Otočení pravidelného čtyřstěnu.

   (h) Oblíbené hlavolamy často tvoří grupu (Rubikova kostka, Loydova patnáctka).

   (i) Sčítání celých čísel modulo 6.

   (j) Násobení nenulových čísel modulo 6.

   (k) Násobení nenulových čísel modulo 5.

5. Dokažte, že v každé grupě existuje právě jeden jednotkový prvek.

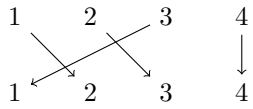
6. Dokažte, že v každé grupě pro každé a existuje právě jeden inverzní prvek.

7. Dokažte, že v každé grupě je možné krátit zprava, tedy z $a \circ c = b \circ c$ plyne $a = b$.

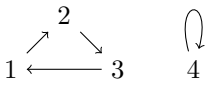
8. Dalším velice důležitým příkladem jsou grupy permutací značené S_n (kterým se říká symetrické grupy). Kde prvky jsou permutace na množině $\{1, \ldots, n\}$ a operace $\circ$ je skládání permutací. Dokažte, že toto je grupa.

   Připomeňme, že permutace je bijekce $\pi\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$. Permutaci můžeme zapsat jako tabulku hodnot, graficky znázornit pomocí šipek které ukazují který prvek se zobrazí na který. Navíc permutaci můžeme zapsat i jako permutační matici, která má v každém řádku i každém sloupci právě jednu jedničku a jinde nuly.

   $$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$



Obrázek 1: Bipartitní znázornění permutace.



Obrázek 2: Znázornění permutace pomocí orientovaného grafu.

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \\ 1 \\ 4 \end{pmatrix}$$

Kolik je různých permutací na n prvkové množině?

Definujme množinu inverzí permutace π jako $I(\pi) = \{(i,j) \mid i < j \text{ a zároveň } \pi(i) > \pi(j)\}$. Znaménko permutace se definuje jako $\operatorname{sgn}(\pi) = (-1)^{|I(\pi)|}$. Znaménko lze definovat i jinými ekvivalentními způsoby.

Jaké je znaménko identity? Transpozice je permutace, která zamění dva prvky. Jaké je znaménko transpozice? Lze každou permutaci dostat jako složení transpozic?

Tvoří permutace znaménka 1 grupu? Co permutace znaménka -1?

Cyklus permutace je orientovaný cyklus v orientovaném grafu $(\{1,\ldots,n\}, \{(i,j) \mid j = \pi(i)\})$ (máme povolené smyčky).

Která permutace má nejvíc cyklů? Existuje permutace, která má pouze jeden cyklus?

Permutaci můžeme zapsat pomocí jejích cyklů tak, že seřadíme její cykly sestupně podle jejich minimálních prvků a zapíšeme je za sebe tak, že začneme vždy minimálním prvkem cyklu. Tedy naše ukázková permutace je zapsaná takto: 4123, což odpovídá cyklům (4)(123). To je ovšem jiná permutace, než permutace 4132, která odpovídá cyklům (4)(132).

9. Pro kladné celé číslo n a dvě celá čísla a, b řekneme, že a, b jsou kongruentní modulo n psáno $a \equiv b \pmod{n}$, právě když n dělí $a - b$ (tedy $a - b$ je celočíselným násobkem n). Ověřte, jestli následující jsou grupy, případně Abelovy grupy:
   (a) Regulární matice $\mathbb{R}^{12\times 12}$ s operací $\circ$ maticové násobení.
   (b) $(\mathbb{N}, \circ)$, kde $a \circ b = \max\{a, b\}$.
   (c) Násobení nenulových čísel modulo 6.
10. Dokažte, že v každé grupě pro každé a existuje právě jeden inverzní prvek.
11. Dokažte, že v každé grupě je možné krátit zprava, tedy z $a \circ c = b \circ c$ plyne $a = b$.