

Definice 1 (Grupa): Množinu G s binární operací $\oplus$ nazveme *grupou*, splňuje-li následující axiomy (pravidla):

- | | |
|--|-------------------------------|
| 1. $\forall a, b \in G : a \oplus b \in G$ | ◀ axiom uzavřenosti |
| 2. $\exists e \in G : \forall a \in G : a \oplus e = e \oplus a = a$ | ◀ existence neutrálního prvku |
| 3. $\forall a \in G : \exists b \in G : a \oplus b = b \oplus a = e$ | ◀ existence inverzního prvku |
| 4. $\forall a, b, c \in G : (a \oplus b) \oplus c = a \oplus (b \oplus c)$ | ◀ asociativita |

Definice 2 (Abelovská grupa): Grupu G nazveme *abelovskou*, splňuje-li navíc podmínku:

- | | |
|---|----------------|
| 5. $\forall a, b \in G : a \oplus b = b \oplus a$ | ◀ komutativita |
|---|----------------|

Důležitou (abelovskou) grupou je konečná grupa $\mathbb{Z}_n$, která je tvořena celými čísly modulo n s operací sčítání modulo n . Například pro $n = 5$ máme $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ a operaci $a + b = (a + b) \bmod 5$.

Úloha 1: Určete, zda následující struktury splňují axiomy grupy a zda jsou Abelovské.

- | | |
|--|---|
| 1. $(\mathbb{Z}, +)$ | 1. $(\mathbb{R}, +)$ |
| 2. $(\mathbb{Z}, \cdot)$ | 2. $(\mathbb{R}, \cdot)$ |
| 3. $(\mathbb{Q}, +)$ | 3. sudé funkce s operací skládání $(f \circ g)(x) = f(g(x))$ |
| 4. $(\mathbb{Q}, \cdot)$ | 4. singulární matice o rozměrech 2×2 s operací sčítání |
| 5. $(\mathbb{Q} \setminus \{0\}, \cdot)$ | |

Úloha 2: V grupě symetrií D_4 (symetrie čtverce) s operací skládání symetrií proveďte následující:

1. Určete všechny prvky grupy.
2. Zjistěte, jestli je grupa abelovská. Pokud ne, sestrojte protipříklad.

Definice 3 (Těleso): Množinu T s binárními operacemi $\oplus$ a $\odot$ nazveme *tělesem*, splňuje-li následující axiomy:

1. $(T, \oplus)$ je abelovská grupa ◀ neutrální prvek 0, inverzní prvek $-a$
2. $(T \setminus \{0\}, \odot)$ je abelovská grupa ◀ neutrální prvek 1, inverzní prvek a^{-1}
3. $\forall a, b, c \in T : a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$ ◀ distributivita

Běžně se setkáme s tělesy reálných, racionálních a komplexních čísel (s obvyklými operacemi). Polynomy také tvoří těleso. Méně často pak s kvaterniony, ty jsou však nekomutativní.

Pokud vezmeme množinu $\mathbb{Z}_n$, automaticky to těleso není. Těleso je to právě tehdy, když n je prvočíslo.

Úloha 3: V tělese $\mathbb{Z}_7$ řešte rovnici

$$3x + 4 = 2$$

Úloha 4: V tělese $\mathbb{Z}_{11}$ řešte soustavu rovnic

$$2x + 3y = 5$$

$$4x - 2y = 7$$

Úloha 5: V tělese $\mathbb{Z}_5$ vypočítejte determinant a najděte inverzi matice

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

Věta 1 (Malá Fermatova): Buď p prvočíslo a $0 \neq a \in \mathbb{Z}_p$. Pak $a^{p-1} = 1$ v tělese $\mathbb{Z}_p$.

Úloha 6: Dokažte malou Fermatovu větu.