

Proseminář z lineární algebry

přednáška 4

Grupy a tělesa

Grupa

grupa $(G, \circ)$, G neprázdné množina, $\circ : G \times G \mapsto G$ binární operace

- ▶ asociativita $\forall a, b, c \in G : a \circ (b \circ c) = (a \circ b) \circ c$
- ▶ neutrální prvek $\exists e \in G \forall a \in G : e \circ a = a \circ e = a$
- ▶ inverzní prvek $\forall a \in G \exists b \in G : a \circ b = b \circ a = e$

Abelova (komutativní) grupa

- ▶ komutativita $\forall a, b \in G : a \circ b = b \circ a$

Příklady grup

- ▶ $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ aditivní grupy
- ▶ $(\mathbb{Z}_n, +)$ konečná grupa s prvky $\{0, 1, \dots, n-1\}$ a operací sčítání modulo n
- ▶ $(\mathbb{R}^{m \times n}, +)$ matice stejného typu se sčítáním
- ▶ $(\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot), (\mathbb{C} \setminus \{0\}, \cdot)$ multiplikativní grupy
- ▶ regulární matice řádu n s násobením
- ▶ permutace množiny X s operací skládání zobrazení

poslední dva příklady nejsou komutativní

Vlastnosti grup

některé základní vlastnosti a vztahy v grupách

- ▶ $a \circ c = b \circ c$ implikuje $a = b$
- ▶ neutrální prvek e je určen jednoznačně
- ▶ $\forall a \in G$ je jeho inverzní prvek a^{-1} určen jednoznačně
- ▶ $\forall a, b \in G$ má rovnice $a \circ x = b$ právě jedno řešení
- ▶ $\forall a \in G : (a^{-1})^{-1} = a$
- ▶ $\forall a, b \in G : (a \circ b)^{-1} = a^{-1} \circ b^{-1}$

$(H, \circ)$ je podgrupou grupy $(G, \circ)$, pokud $H \subseteq G$ a $(H, \circ)$ je grupa

Permutace

symetrická grupa $(S_n, \circ)$

zápisy permutací

- ▶ tabulka se vzory a obrazy

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix}$$

- ▶ diagram
- ▶ rozklad na cykly

$$p = (1, 2)(3)(4, 5, 6)$$

Znaménko permutace

Každou permutaci lze zapsat jako složení transpozic.

znaménko permutace $p \in S_n$

- ▶ $\text{sgn}(p) = (-1)^t$, kde t je počet transpozic v zápise p

alternativně

- ▶ $\text{sgn}(p) = (-1)^{n-k}$, kde k je počet cyklů
- ▶ $\text{sgn}(p) = (-1)^v$, kde v je počet tzv. inverzí (dvojic $i < j$ pro které $p(i) > p(j)$)

vlastnosti

- ▶ $\forall p, q \in S_n : \text{sgn}(p \circ q) = \text{sgn}(p)\text{sgn}(q)$
- ▶ $\forall p \in S_n : \text{sgn}(p^{-1}) = \text{sgn}(p)$

Tělesa

(algebraické) těleso $(\mathbb{T}, +, \cdot)$

- ▶ $(\mathbb{T}, +)$ Abelova grupa, neutr. prvek 0, inverzní k a značíme $-a$
- ▶ $(\mathbb{T} \setminus \{0\}, \cdot)$ Abelova grupa, neutr. prvek 1, inverzní a^{-1}
- ▶ distributivita $\forall a, b, c \in \mathbb{T} : a(b + c) = ab + ac$

běžně používaná tělesa $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

kvaterniony – nekomutativní těleso

- ▶ $\forall a \in \mathbb{T} : 0a = 0$
- ▶ $\forall a \in \mathbb{T} : -a = (-1)a$
- ▶ $\forall a, b \in \mathbb{T} : ab = 0 \Rightarrow (a = 0 \vee b = 0)$

Konečná tělesa

- ▶ $\mathbb{Z}_n$ s operacemi modulo n tvoří těleso právě tehdy, když n je prvočíslo.
- ▶ Konečné těleso s právě n prvky existuje právě tehdy, když n je mocninou prvočísla.
- ▶ **Pozor:** existuje těleso se 4 prvky, ale není to $\mathbb{Z}_4$.
- ▶ Charakteristika tělesa $\mathbb{T}$ je nejmenší přirozené n takové, že součet n kopií prvku 1 je roven 0, případně je to 0, pokud takové n neexistuje.
- ▶ Charakteristika tělesa je vždy buď prvočíslo nebo nula.
- ▶ **Malá Fermatova věta.** Buď p prvočíslo a $0 \neq a \in \mathbb{Z}_p$, pak v $\mathbb{Z}_p$ platí $a^{p-1} = 1$.