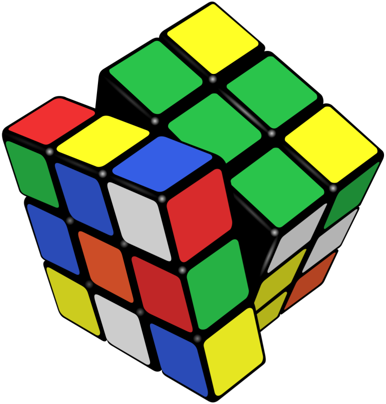
Lineární algebra 1

Martin Balko

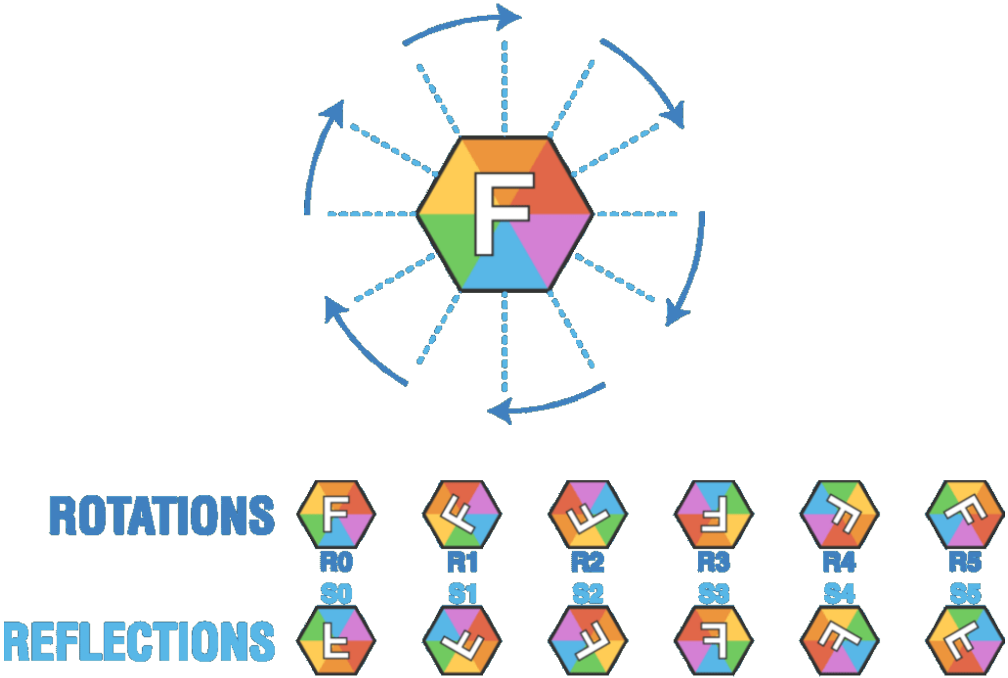
4. přednáška

22. října 2019

Grupy



Zdroj: https://wikipedia.org



Zdroj: https://res.cloudinary.com

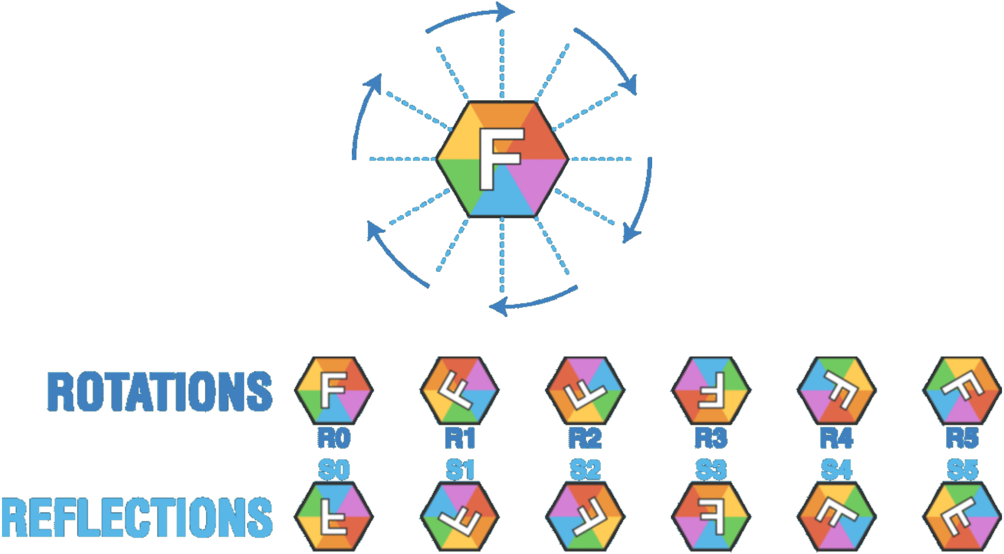
Grupy

- abstraktní algebraické struktury k popisu symetrií.
- Grupa je dvojicí $(G, \circ)$, kde G je množina a $\circ\colon G^2 \to G$ je binární operací na množině splňující:
  1. $\forall\, a, b, c \in G\colon a \circ (b \circ c) = (a \circ b) \circ c,$ (asociativita)
  2. $\exists\, e \in G\ \forall\, a \in G\colon e \circ a = a \circ e = a,$ (neutrální prvek)
  3. $\forall\, a \in G\ \exists\, b \in G\colon a \circ b = b \circ a = e.$ (inverzní prvek)
- Abelovou grupou je grupa, která navíc splňuje:
  4. $\forall\, a \in G\ \forall\, b \in G\colon a \circ b = b \circ a.$ (komutativita)
- Je-li operací $\circ$ sčítání, pak neutrální prvek značíme 0 a inverzní $-a$.
- Je-li operací $\circ$ násobení, pak neutrální prvek značíme 1 a inverzní a^{-1}.

Příklady

- Příklady Abelových grup:
  1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$,
  2. $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$,
  3. grupa matic $(\mathbb{R}^{m \times n}, +)$, kde neutrálním prvkem je nulová matice $m \times n$ a inverzním prvkem k matici A je matice $-A$,
  4. konečná grupa $(\mathbb{Z}_m, +)$, kde $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ a sčítání $+$ se provádí modulo m. Neutrálním prvkem je 0 a inverzním prvkem k a je $-a \bmod m$.
  5. grupa $(\{p(x) \colon p \text{ je polynom}\}, +)$ polynomů se sčítáním.
- Příklady ne nutně Abelových grup:
  1. množina všech zobrazení na množině s operací skládání,
  2. množina regulárních matic řádu n s násobením.
- Příklady negrup:
  1. $(\mathbb{N}, +)$, $(\mathbb{Z}, -)$, $(\mathbb{Z} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, :)$.

Příklad grupy z úvodního obrázku



Zdroj: https://res.cloudinary.com

Grupou symetrií hexagonu je tzv. dihedrální grupa D6 s 12 prvky.

Základní vlastnosti grup

Tvrzení

Prvky grupy $(G, \circ)$ splňují následující vlastnosti:

1. $a \circ c = b \circ c$ implikuje $a = b$, (krácení)
2. neutrální prvek e je určen jednoznačně,
3. pro každé $a \in G$ je jeho inverzní prvek určen jednoznačně,
4. rovnice $a \circ x = b$ má právě jedno řešení pro každé $a, b \in G$,
5. $(a^{-1})^{-1} = a$,
6. $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

- Důkaz (části tvrzení):

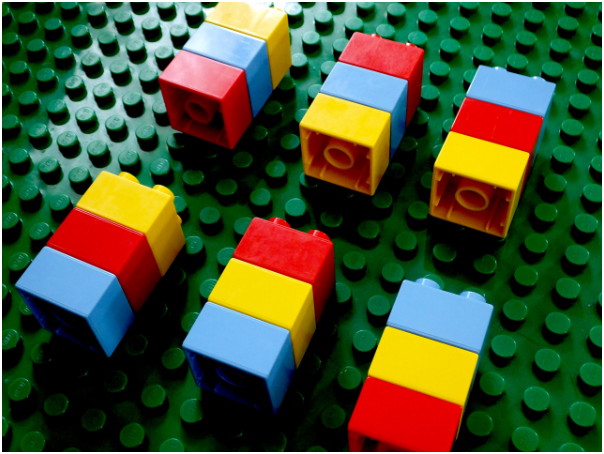
1. $a \circ c = b \circ c \Rightarrow a \circ (c \circ c^{-1}) = b \circ (c \circ c^{-1}) \Rightarrow a \circ e = b \circ e \Rightarrow a = b$.
2. Neutrální prvky e_1 a e_2 $\Rightarrow e_1 = e_1 \circ e_2 = e_2 \Rightarrow e_1 = e_2$.
3. Inverzní prvky a_1 a a_2 k a $\Rightarrow a_1 \circ a = e = a_2 \circ a$ a z krácení $a_1 = a_2$.
4. Vynásobení rovnice $a \circ x = b$ prvkem a^{-1} zleva dává $x = a^{-1} \circ b$. Po dosazení je rovnost splněna. $\square$

Podgrupy

- Podgrupa grupy $(G, \circ)$ je grupa $(H, \diamond)$ taková, že platí $H \subseteq G$ a pro všechna $a, b \in H$ platí $a \circ b = a \diamond b$.
- Neboli v H platí uzavřenost $(a, b \in H \Rightarrow a \circ b \in H)$ a existence neutrálního $(e \in H)$ a inverzního prvku $(a \in H \Rightarrow a^{-1} \in H)$.
- Značíme $(H, \diamond) \leq (G, \circ)$.

- Příklady.
  1. Triviální podgrupy grupy $(G, \circ)$: $(G, \circ)$ a $(\{e\}, \circ)$,
  2. $(\mathbb{N}, +) \not\leq (\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$,

Permutace



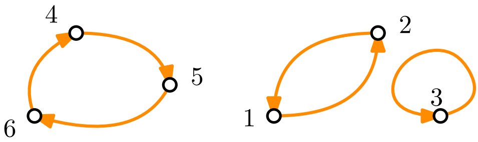
Zdroj: https://playcuriously.wordpress.com

Permutace

- Zobrazení je vzájemně jednoznačné, pokud je prosté a na.
- Permutace na konečné množině X je vzájemně jednoznačné zobrazení $p\colon X \to X$.
- S_n = množina všech permutací na $X = \{1, \ldots, n\}$.

- Možné zápisy permutací:

1. Tabulkou (nahoře vzory, dole obrazy): $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix}$
2. Grafem (šipka vede ze vzoru do obrazu):



3. Rozložením na cykly (v závorce je obrazem prvku jeho následník):

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

Operace s permutacemi

- Identita id je permutace, která zobrazuje každý prvek sám na sebe.
- Transpozice je permutace (i, j), která prohazuje dva prvky. Tedy permutace s jedním cyklem, který má 2 prvky.

1. Inverzní permutace p^{-1} k permutaci p je daná předpisem $p^{-1}(i) = j$, pokud $p(j) = i$.
   - Příklad: $(i, j)^{-1} = (i, j)$, $(i, j, k)^{-1} = (k, j, i)$.
2. Pro $p, q \in S_n$ je složená permutace $p \circ q$ daná předpisem $(p \circ q)(i) = p(q(i))$.
   - Příklad: pro $p = (1, 2)$, $q = (1, 3, 2)$ je $p \circ q = (1, 3)$, $q \circ p = (2, 3)$.
   - Skládání permutací je asociativní, ale ne nutně komutativní.
   - Příklad: $p \circ \mathrm{id} = p = \mathrm{id} \circ p$, $p \circ p^{-1} = \mathrm{id} = p^{-1} \circ p$.

Znaménko permutace

- Pokud se permutace $p \in S_n$ skládá z k cyklů, pak **znaménkem permutace** p je číslo $\mathrm{sgn}(p) = (-1)^{n-k}$.
- Příklad: $\mathrm{sgn}(\mathrm{id}) = 1$, $\mathrm{sgn}((i,j)) = -1$, $\mathrm{sgn}((1,3,4)(2,5)) = -1$.

Věta o znaménku složení permutace s transpozicí

Buď $p \in S_n$ permutace a $t = (i,j) \in S_n$ transpozice. Pak

$$\mathrm{sgn}(p) = -\mathrm{sgn}(t \circ p) = -\mathrm{sgn}(p \circ t).$$

- Důkaz (rovnosti $\mathrm{sgn}(p) = -\mathrm{sgn}(t \circ p)$, druhá se dokáže analogicky):
- Rozlišíme dva případy.
  1. i a j jsou ve stejném cyklu $(i, u_1, \ldots, u_r, j, v_1, \ldots, v_s)$. Pak $(i,j) \circ (i, u_1, \ldots, u_r, j, v_1, \ldots, v_s) = (i, u_1, \ldots, u_r)(j, v_1, \ldots, v_s)$ a počet cyklů se zvýší o 1.
  2. i a j jsou v různých cyklech $(i, u_1, \ldots, u_r)$ a $(j, v_1, \ldots, v_s)$. Pak $(i,j) \circ (i, u_1, \ldots, u_r)(j, v_1, \ldots, v_s) = (i, u_1, \ldots, u_r, j, v_1, \ldots, v_s)$ a počet cyklů se sníží o 1.

$\square$

Vlastnosti znamének permutací

Věta

Každou permutaci lze rozložit na složení transpozic.

- Důkaz:
- Postupně na transpozice rozložíme všechny cykly.
- Rozložení cyklu $(u_1, \ldots, u_r)$:

$$(u_1, \ldots, u_r) = (u_1, u_2) \circ (u_2, u_3) \circ \cdots \cdots \circ (u_{r-1}, u_r). \qquad \square$$

Důsledek 1

Platí $\operatorname{sgn}(p) = (-1)^r$, kde r je počet transpozic v rozkladu permutace p.

Důsledek 2

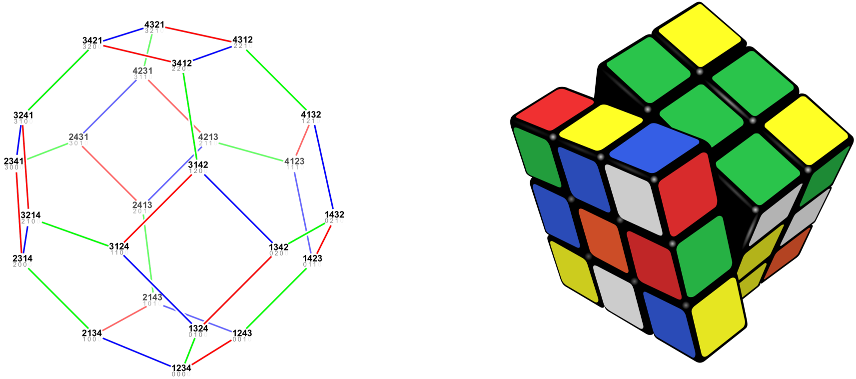
Pro $p, q \in S_n$ platí $\operatorname{sgn}(p \circ q) = \operatorname{sgn}(p) \cdot \operatorname{sgn}(q)$.

Důsledek 3

Pro $p \in S_n$ platí $\operatorname{sgn}(p) = \operatorname{sgn}(p^{-1})$.

Symetrická grupa

- Množina permutací S_n tvoří s operací skládání $\circ$ takzvanou symetrickou grupu $(S_n, \circ)$.



Obrázek: Reprezentace symetrické grupy S_4 a Rubikova kostka.

Zdroj: https://wikimedia.org

- Symetrické grupy popisují symetrie různých objektů.
- Každá grupa je isomorfní nějaké podgrupě symetrické grupy.

Algebraická tělesa

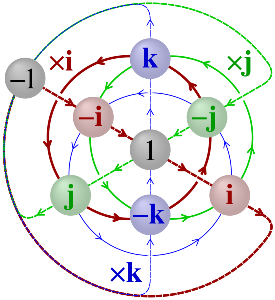
Zdroj: https://galois.com

Tělesa

- Jedná se zobecnění číselných oborů jako například $\mathbb{R}$.
- Těleso je množina $\mathbb{T}$ spolu se dvěma komutativními binárními operacemi $+$ a $\cdot$ splňujícími:
  1. $(\mathbb{T}, +)$ je Abelova grupa (neutrální prvek 0, inverzním k a je $-a$),
  2. $(\mathbb{T} \setminus \{0\}, \cdot)$ je Abelova grupa (neutrální prvek 1, inverzním k a je a^{-1}),
  3. $\forall\, a, b, c \in \mathbb{T}\colon a \cdot (b + c) = a \cdot b + a \cdot c,$ (distributivita).
- Operace $+$ a $\cdot$ nemusí představovat klasické sčítání a násobení.
- Budeme psát ab namísto $a \cdot b$
- Každé těleso má aspoň dva prvky, protože $0 \neq 1$.
- Zavedeme inverzní operace $-$ a $/$ definované jako $a - b = a + (-b)$ a $a/b = ab^{-1}$.
- Podtěleso je podmnožina tělesa, která se stejně definovanými operacemi tvoří těleso.

Příklady

1. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ s klasickými operacemi sčítání a násobení tvoří (nekonečná) tělesa,
2. $\mathbb{Z}$ se sčítáním a násobením těleso netvoří (chybí inverzní prvky pro násobení),
3. $\{0, 1\}$ se sčítáním a násobením modulo 2 je nejmenší možné těleso,
4. kvaterniony (zobecnění komplexních čísel vzniklé přidáním dvou dalších imaginárních jednotek j a k, kde $j^2 = k^2 = -1$ a $ijk = -1$) tvoří nekomutativní těleso.



Zdroj: https://wikipedia.org

Základní vlastnosti těles

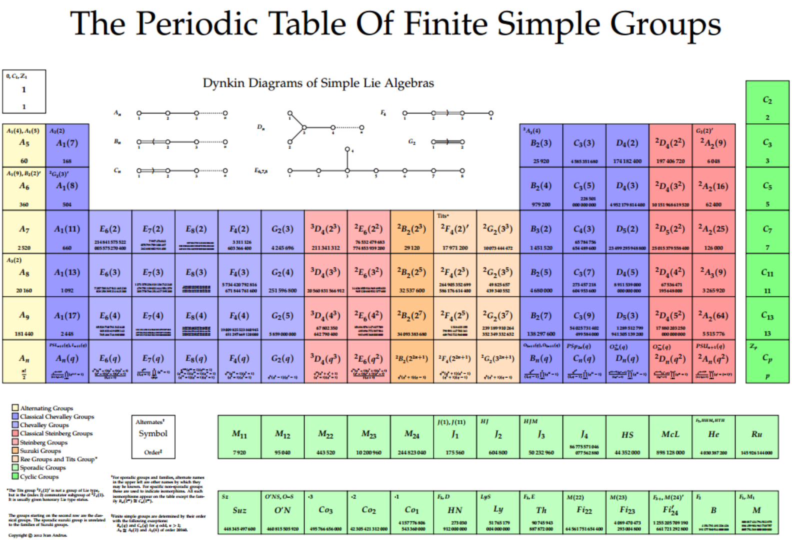
Tvrzení

Prvky tělesa splňují následující vlastnosti:

1. $0a = 0$.
2. $ab = 0$ implikuje $a = 0$ nebo $b = 0$,
3. $-a = (-1)a$.

- Důkaz:

1.
$$\begin{aligned} 0a &= (0+0)a = 0a + 0a \\ (-0a) + 0a &= (-0a) + 0a + 0a \\ 0 &= 0 + 0a \\ 0 &= 0a. \end{aligned}$$
2. Pro $a = 0$ platí. Pro $a \neq 0$ vynásobením obou stran rovnice zleva prvkem a^{-1} máme $a^{-1}ab = a^{-1}0$ a podle 1) tedy $1b = 0$.
3. $0 = 0a = (1-1)a = 1a + (-1)a = a + (-1)a$, tedy $-a = (-1)a$. $\square$



Obrázek: Klasifikace jednoduchých konečných grup (jeden z nejrozsáhlejších projektů dějin matematiky). Všimněme si tzv. Monster grupy.

Zdroj: https://cabinetmagazine.org

Děkuji za pozornost.