

Lineární prostory nad \mathbb{F}

Odpřednesenou látku naleznete v kapitolách 1.1–1.4
skript *Abstraktní a konkrétní lineární algebra*.

Minulá přednáška

Lineární prostor nad \mathbb{R} jako zobecnění (například) prostoru orientovaných úseček v rovině.

Dnešní přednáška

- 1 Těleso \mathbb{F} jako zobecnění reálných čísel.
- 2 Lineární prostor nad \mathbb{F} jako zobecnění pojmu lineární prostor nad \mathbb{R} .
- 3 **Důležité:** povšmneme si, že důkazy typicky nesouvisí s konkrétními operacemi; souvisí s pouze s **algebraickými vlastnostmi** těchto operací.^a

Od příště budeme pracovat s lineárními prostory nad obecným tělesem.

^aDo jisté míry je tak dnešní přednáška „kopií“ přednášky předchozí. Algebra dovolí od příště takovou marnotratnost nedopustit.

Sčítání a násobení reálných čísel

Množina reálných čísel \mathbb{R} je vybavena dvěma funkcemi

$$+ : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}, \quad \cdot : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$$

pro které platí následující:

1 Vlastnosti sčítání:

- 1 Existuje $0 \in \mathbb{R}$ tak, že pro vš. $a \in \mathbb{R}$ platí: $a + 0 = 0 + a = a$ (existence nuly).
- 2 Pro vš. $a, b, c \in \mathbb{R}$ platí: $(a + b) + c = a + (b + c)$ (asociativita sčítání).
- 3 Pro vš. $a, b \in \mathbb{R}$ platí: $a + b = b + a$ (komutativita sčítání).
- 4 Pro vš. $a \in \mathbb{R}$ existuje právě jedno $b \in \mathbb{R}$ tak, že $a + b = 0$ (existence opačného čísla, značíme $b = -a$).

Sčítání a násobení reálných čísel (pokrač.)

2 Vlastnosti násobení:

- 1 Existuje $1 \in \mathbb{R}$ tak, že pro vš. $a \in \mathbb{R}$ platí: $1 \cdot a = a$ (existence jednotky).
- 2 Pro vš. $a, b, c \in \mathbb{R}$ platí: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (asociativita násobení).
- 3 Pro vš. $a, b \in \mathbb{R}$ platí: $a \cdot b = b \cdot a$ (komutativita násobení).

3 Provázanost sčítání a násobení:

- 1 Pro vš. $a, b, c \in \mathbb{R}$ platí: $a \cdot (b + c) = a \cdot b + a \cdot c$ (levý distributivní zákon).
- 2 Pro vš. $a, b, c \in \mathbb{R}$ platí: $(b + c) \cdot a = b \cdot a + c \cdot a$ (pravý distributivní zákon).

4 Test invertibility: pro vš. $a \in \mathbb{R}$ platí: $a \neq 0$ iff existuje a^{-1} .

Poznámka

Výše uvedené vlastnosti byly podstatné pro zavedení pojmu **lineární prostor nad \mathbb{R}** (viz minulou přednášku).

Příklady: další „standardní“ sčítání a násobení

- 1 Standardní sčítání a násobení racionálních čísel: obě operace na množině \mathbb{Q} **splňují stejné vlastnosti** jako standardní sčítání a násobení na množině \mathbb{R} .
- 2 Standardní sčítání a násobení komplexních čísel: obě operace na množině \mathbb{C} **splňují stejné vlastnosti** jako standardní sčítání a násobení na množině \mathbb{R} .
- 3 Standardní sčítání a násobení celých čísel: obě operace na množině \mathbb{Z} **nesplňují stejné vlastnosti** jako standardní sčítání a násobení na množině \mathbb{R} . **Neplatí test invertibility**: například $2 \neq 0$, ale 2^{-1} v \mathbb{Z} **neexistuje!**^a

^aTest invertibility v \mathbb{R} byl v minulé přednášce podstatný! Množinu \mathbb{Z} tedy jako množinu skalárů nebudeme moci použít.

Příklad: „nestandardní“ sčítání a násobení

- 1 Množina $\mathbb{Z}_2 = \{0, 1\}$ s operacemi:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

- 2 Množina $\mathbb{Z}_3 = \{0, 1, 2\}$ s operacemi:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Operace na množinách \mathbb{Z}_2 a \mathbb{Z}_3 **splňují stejné vlastnosti** jako standardní sčítání a násobení na množině \mathbb{R} .

Slogan pro těleso

Těleso \mathbb{F} je kolekce **jakýchkoli** objektů (těm budeme říkat **prvky tělesa** \mathbb{F}), které mezi sebou můžeme sčítat a násobit. Sčítání a násobení v \mathbb{F} splňují stejné vlastnosti jako standardní sčítání a násobení v \mathbb{R} .

Definice (těleso)

Těleso je množina \mathbb{F} , vybavena dvěma funkcemi

$$+ : \mathbb{F} \times \mathbb{F} \rightarrow \mathbb{F}, \quad \cdot : \mathbb{F} \times \mathbb{F} \rightarrow \mathbb{F}$$

pro které platí následující:

1 Vlastnosti sčítání:

- 1 Existuje $0 \in \mathbb{F}$ tak, že pro vš. $a \in \mathbb{F}$ platí: $a + 0 = 0 + a = a$ (**existence nuly**).
- 2 Pro vš. $a, b, c \in \mathbb{F}$ platí: $(a + b) + c = a + (b + c)$ (**asociativita sčítání**).
- 3 Pro vš. $a, b \in \mathbb{F}$ platí: $a + b = b + a$ (**komutativita sčítání**).
- 4 Pro vš. $a \in \mathbb{F}$ existuje právě jedno $b \in \mathbb{F}$ tak, že $a + b = 0$ (**existence opačného čísla**, značíme $b = -a$).

Definice tělesa (pokrač.)

2 Vlastnosti násobení:

- 1 Existuje $1 \in \mathbb{F}$ tak, že pro vš. $a \in \mathbb{F}$ platí: $1 \cdot a = a$ (existence jednotky).
- 2 Pro vš. $a, b, c \in \mathbb{F}$ platí: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (asociativita násobení).
- 3 Pro vš. $a, b \in \mathbb{F}$ platí: $a \cdot b = b \cdot a$ (komutativita násobení).

3 Provázanost sčítání a násobení:

- 1 Pro vš. $a, b, c \in \mathbb{F}$ platí: $a \cdot (b + c) = a \cdot b + a \cdot c$ (levý distributivní zákon).
- 2 Pro vš. $a, b, c \in \mathbb{F}$ platí: $(b + c) \cdot a = b \cdot a + c \cdot a$ (pravý distributivní zákon).

4 Test invertibility: pro vš. $a \in \mathbb{F}$ platí: $a \neq 0$ iff existuje a^{-1} .

Příklady

- 1 Množiny \mathbb{Q} , \mathbb{R} , \mathbb{C} se standardním sčítáním a násobením **jsou** tělesa.
- 2 Množina \mathbb{Z} se standardním sčítáním a násobením **není** těleso.
- 3 Množiny \mathbb{Z}_2 a \mathbb{Z}_3 **jsou** tělesa (sčítáme a násobíme jako zbytky po dělení 2, resp. 3).

Obecněji: množina $\mathbb{Z}_p = \{0, 1, \dots, p - 1\}$, kde p je **prvočíslo**, je těleso, pokud čísla sčítáme a násobíme jako zbytky po dělení p .

Definice (lineární prostor nad tělesem \mathbb{F})

Lineární prostor nad tělesem \mathbb{F} je množina L spolu se dvěma funkcemi

$$+ : L \times L \rightarrow L, \quad \cdot : \mathbb{F} \times L \rightarrow L$$

pro které platí následující:

1 Vlastnosti sčítání:

- 1 Existuje $\vec{o} \in L$ tak, že pro vš. $\vec{x} \in L$ platí: $\vec{x} + \vec{o} = \vec{o} + \vec{x} = \vec{x}$ (existence nulového vektoru).
- 2 Pro vš. $\vec{x}, \vec{y}, \vec{z} \in L$ platí: $(\vec{x} + \vec{y}) + \vec{z} = \vec{x} + (\vec{y} + \vec{z})$ (asociativita sčítání vektorů).
- 3 Pro vš. $\vec{x}, \vec{y} \in L$ platí: $\vec{x} + \vec{y} = \vec{y} + \vec{x}$ (komutativita sčítání vektorů).
- 4 Pro vš. $\vec{x} \in L$ existuje právě jeden $\vec{y} \in L$ tak, že $\vec{x} + \vec{y} = \vec{o}$ (existence opačného vektoru, značíme $\vec{y} = -\vec{x}$).

Definice (lineární prostor nad tělesem \mathbb{F}), pokrač.

2 Vlastnosti násobení skalárem:

- 1 Pro vš. $\vec{x} \in L$ platí: $1 \cdot \vec{x} = \vec{x}$ (násobení jednotkovým skalárem).
- 2 Pro vš. $a, b \in \mathbb{F}$ a vš. $\vec{x} \in L$ platí: $a \cdot (b \cdot \vec{x}) = (a \cdot b) \cdot \vec{x}$ (asociativita násobení skalárem).

3 Distributivní zákony:

- 1 Pro vš. $a, b \in \mathbb{F}$ a vš. $\vec{x} \in L$ platí: $(a + b) \cdot \vec{x} = a \cdot \vec{x} + b \cdot \vec{x}$ (distributivita součtu skalárů).
- 2 Pro vš. $a \in \mathbb{F}$ a vš. $\vec{x}, \vec{y} \in L$ platí: $a \cdot (\vec{x} + \vec{y}) = a \cdot \vec{x} + a \cdot \vec{y}$ (distributivita součtu vektorů).

Poznámka

Axiomy tří typů: chování operace $+$, chování operace \cdot a vzájemný vztah obou operací.

Definice je formálně stejná jako pro lineární prostor nad \mathbb{R} . Jediná změna: těleso \mathbb{R} je nahrazeno obecným tělesem \mathbb{F} .

Příklady lineárních prostorů nad obecným tělesem \mathbb{F}

- ① Prostory \mathbb{F}^n nad \mathbb{F} , $n \geq 1$. Vektory jsou uspořádané n -tice prvků \mathbb{F} , psané do sloupce. Skaláry jsou prvky tělesa \mathbb{F} .

Například: v $(\mathbb{Z}_7)^2$ je vektor $\begin{pmatrix} 2 \\ 0 \end{pmatrix}$, v \mathbb{Q}^3 je vektor $\begin{pmatrix} 2.14 \\ -21.7 \\ 12 \end{pmatrix}$,

v \mathbb{C}^2 je vektor $\begin{pmatrix} 2 - 4i \\ \sqrt{3}i \end{pmatrix}$, atd.

- ② Prostory $\mathbb{F}[x]$ polynomů v neurčité x s koeficienty z tělesa \mathbb{F} . Skaláry jsou prvky tělesa \mathbb{F} , vektory jsou jednotlivé polynomy. Sčítání a násobení je definováno analogicky jako v $\mathbb{R}[x]$.
Například: v $\mathbb{Z}_3[x]$ platí:

$$(2x + 2) + (x + 2) = 1$$

$$(2x + 2) \cdot (x + 2) = 2x^2 + 1$$

Jednoduché důsledky definice

Ať L je lineární prostor. Potom:

- 1 Nulový vektor je jednoznačně určen.
- 2 Pro vš. $\vec{x} \in L$ platí: $0 \cdot \vec{x} = \vec{o}$.
- 3 Opačný vektor k $\vec{x} \in L$ je vektor $(-1) \cdot \vec{x}$.
- 4 Pro vš. $a \in \mathbb{R}$ platí: $a \cdot \vec{o} = \vec{o}$.

Důkaz.

- 1 Ať existují \vec{o}_1, \vec{o}_2 tak, že pro vš. $\vec{x} \in L$ platí:
 $\vec{x} + \vec{o}_1 = \vec{o}_1 + \vec{x} = \vec{x}$ a $\vec{x} + \vec{o}_2 = \vec{o}_2 + \vec{x} = \vec{x}$. Pak
 $\vec{o}_1 = \vec{o}_1 + \vec{o}_2 = \vec{o}_2$.
- 2 Pro vš. $\vec{x} \in L$ platí:
 $\vec{x} = 1 \cdot \vec{x} = (1 + 0) \cdot \vec{x} = 1 \cdot \vec{x} + 0 \cdot \vec{x} = \vec{x} + 0 \cdot \vec{x}$. Tudíž $0 \cdot \vec{x}$
musí být nulový vektor.

Důkaz (pokrač.)

- ③ Platí: $\vec{x} + (-1) \cdot \vec{x} = 1 \cdot \vec{x} + (-1) \cdot \vec{x} = (1 - 1) \cdot \vec{x} = 0 \cdot \vec{x} = \vec{o}$.
- ④ Platí: $a \cdot \vec{o} = a \cdot (0 \cdot \vec{o}) = (a \cdot 0) \cdot \vec{o} = 0 \cdot \vec{o} = \vec{o}$.

Velmi důležitý důsledek definice

Ať L je lineární prostor, $a \in \mathbb{F}$, $\vec{x} \in L$. Pak $a \cdot \vec{x} = \vec{o}$ právě tehdy, když $a = 0$ nebo $\vec{x} = \vec{o}$.

Důkaz.

Díky předchozímu stačí dokázat pouze implikaci zleva doprava.

Ať $a \cdot \vec{x} = \vec{o}$ a $a \neq 0$. Potom existuje a^{-1} . Tudíž
 $\vec{o} = a^{-1} \cdot \vec{o} = a^{-1} \cdot (a \cdot \vec{x}) = (a^{-1} \cdot a) \cdot \vec{x} = 1 \cdot \vec{x} = \vec{x}$.

Povšimněme si:

Důkazy jsou stejné, jako v minulé přednášce!

Jaký nejobecnější výpočet lze v lineárním prostoru vykonat?

- 1 Například můžeme sečíst čtyři vektory: $\vec{x} + \vec{y} + \vec{z} + \vec{w}$.
Díky asociativitě sčítání **nemusíme psát závorky**.
- 2 Například můžeme násobek vektoru opět vynásobit: $b \cdot (a \cdot \vec{x})$.
Díky axiomům **jde opět o násobek** $(b \cdot a) \cdot \vec{x}$.
- 3 Obecněji, **můžeme sčítat konečně mnoho násobků vektorů**.
To znamená: je-li dán **konečný seznam** vektorů $(\vec{x}_1, \dots, \vec{x}_n)$ a **konečný seznam** skalárů^a (a_1, \dots, a_n) , lze utvořit **lineární kombinaci**

$$a_1 \cdot \vec{x}_1 + a_2 \cdot \vec{x}_2 + a_3 \cdot \vec{x}_3 + \dots + a_n \cdot \vec{x}_n$$

značenou i $\sum_{i=1}^n a_i \cdot \vec{x}_i$ nebo $\sum_{i \in \{1, \dots, n\}} a_i \cdot \vec{x}_i$

^aTěmto skalárům říkáme **koeficienty** lineární kombinace.

Definice

Seznam (také: **skupina**) **vektorů** je buď prázdná posloupnost $()$ nebo konečná posloupnost $(\vec{x}_1, \dots, \vec{x}_n)$.

Pozor: je rozdíl mezi seznamem a množinou

$$(\vec{x}_1, \vec{x}_2, \vec{x}_3) \neq (\vec{x}_3, \vec{x}_2, \vec{x}_1) \text{ vs. } \{\vec{x}_1, \vec{x}_2, \vec{x}_3\} = \{\vec{x}_3, \vec{x}_2, \vec{x}_1\}$$

$$(\vec{x}_1, \vec{x}_1, \vec{x}_2) \neq (\vec{x}_1, \vec{x}_2) \text{ vs. } \{\vec{x}_1, \vec{x}_1, \vec{x}_2\} = \{\vec{x}_1, \vec{x}_2\}$$

Definice (lineární kombinace konečného seznamu vektorů)

Pro seznam vektorů tvaru

- 1 $()$ definujeme \vec{o} jako jeho (jedinou možnou) **lineární kombinaci** (s prázdným seznamem koeficientů).

- 2 $(\vec{x}_1, \dots, \vec{x}_n)$ je vektor $\sum_{i=1}^n a_i \cdot \vec{x}_i$ jeho **lineární kombinace** (se seznamem koeficientů (a_1, \dots, a_n)).

Příklad (geometrický význam lineární kombinace)

Pro seznam (\mathbf{a}_1) v \mathbb{R}^2



a seznam (2.5) reálných čísel je



lineární kombinace.

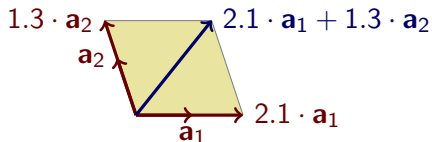
Všechny možné lineární kombinace vektoru \mathbf{a}_1 vytvářejí v \mathbb{R}^2 přímku procházející počátkem (se směrem \mathbf{a}_1).

Příklad (geometrický význam lineární kombinace)

Pro seznam $(\mathbf{a}_1, \mathbf{a}_2)$ v \mathbb{R}^3



a seznam $(2.1, 1.3)$ reálných čísel je



Všechny možné lineární kombinace seznamu $(\mathbf{a}_1, \mathbf{a}_2)$ vytvářejí v \mathbb{R}^3 rovinu procházející počátkem (se směrem $(\mathbf{a}_1, \mathbf{a}_2)$).

Význam lineárních kombinací (zatím jen slogan)

Ať L je lineární prostor nad \mathbb{F} .

Lineární kombinace seznamu $(\vec{x}_1, \dots, \vec{x}_n)$ v L vytvářejí „rovný kus“ prostoru L .

Tento „rovný kus“ prostoru L prochází počátkem \vec{o} a má „směr“ $(\vec{x}_1, \dots, \vec{x}_n)$.

Příští přednáška: těmto „rovným kusům“ v L budeme říkat **lineární podprostory** L .

Příklad (lineární kombinace a soustavy rovnic)

Existují koeficienty $x, y \in \mathbb{Z}_7$ tak, že v $(\mathbb{Z}_7)^2$ platí rovnost

$$x \cdot \begin{pmatrix} 2 \\ 3 \end{pmatrix} + y \cdot \begin{pmatrix} 6 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 6 \end{pmatrix} \quad ?$$

Dva pohledy na tento problém:

- 1 Hledáme prvky $x, y \in \mathbb{Z}_7$ tak, že platí

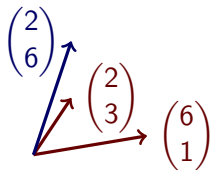
$$2x + 6y = 2$$

$$3x + 1y = 6$$

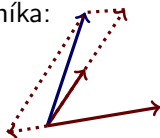
To znamená: koeficienty lineární kombinace jsou řešením jisté soustavy lineárních rovnic nad \mathbb{Z}_7 .

Příklad (lineární kombinace a soustavy rovnic, pokrač.)

- 2 Pro zadané vektory



hledáme „natažení“ červených vektorů tak, aby modrý vektor byl úhlopříčkou čtyřúhelníka:



Pozor: výše uvedený obrázek je „slogan“! Pracujeme totiž v $(\mathbb{Z}_7)^2$.

Zobecnění předchozího (zatím jen slogan)

Hledáme-li pro pevný seznam $(\mathbf{a}_1, \dots, \mathbf{a}_s)$ a pevný vektor \mathbf{b} v \mathbb{F}^r reálné koeficienty x_1, \dots, x_s tak, aby platila rovnost

$$x_1 \cdot \mathbf{a}_1 + \dots + x_s \cdot \mathbf{a}_s = \mathbf{b}$$

pak lze na tuto úlohu pohlížet dvěma způsoby:

- 1 Řešíme **soustavu r lineárních rovnic o s neznámých**.
- 2 Hledáme „natažení“ vektorů $\mathbf{a}_1, \dots, \mathbf{a}_s$ pomocí skalárů x_1, \dots, x_s tak, aby vektor \mathbf{b} **tvořil úhlopříčku rovnoběžnostěnu**.

Příští přednášky: druhý pohled na tuto úlohu nám dovolí vybudovat elegantní metodu řešení (Gaussovu eliminaci).