# Lineární algebra I (pro fyziky)

## Vektorové prostory

Dalibor Šmíd

MFF UK

V prvních 3 přednáškách jsme se setkali s pojmy

- lineární kombinace
- (afinní) podprostor
- lineární zobrazení
- (kanonická) báze

Byly definovány pomocí vektorů z $\mathbb{R}^n$, ale lze je zobecnit na další objekty, které lze mezi sebou sčítat a násobit je skalárem. Takovými objekty mohou být například

- komplexní čísla
- matice typu $m \times n$.
- nekonečné posloupnosti reálných čísel
- polynomy v proměnné $x$
- (spojité) funkce

Vyplatí se tedy naši představu vektoru (a skaláru) abstrahovat pomocí axiomů.

## Definice (Grupa)

Nechť $\circ : G \times G \to G$ je binární operace na množině $G$. Pak *grupou* nazýváme dvojici $(G, \circ)$, která splňuje

1. $\forall a, b, c \in G : (a \circ b) \circ c = a \circ (b \circ c)$ (asociativita)
2. $\exists e \in G : \forall a \in G : a \circ e = e \circ a = a$ (neutrální prvek)
3. $\forall a \in G : \exists a^{-1} \in G : a \circ a^{-1} = a^{-1} \circ a = e$ (inverzní prvky)

Pokud navíc $\forall a, b \in G : a \circ b = b \circ a$, pak je $(G, \circ)$ *komutativní grupa.*

Příklady:

- $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{R}^n, +)$, $(\mathbb{R}^{m \times n}, +)$
- $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\{z \in \mathbb{C} |\ |z| = 1\}, \cdot)$
- $(\{R_\phi : \mathbb{R}^2 \to \mathbb{R}^2 | \phi \in \langle 0, 2\pi)\}, \circ)$, množina všech matic rotací v $\mathbb{R}^2$ s operací maticového součinu
- $(\{\mathrm{Id}, R_{2\pi/3}, R_{-2\pi/3}, Z_{(1,0)^\perp}, Z_{(1,\sqrt{3})^\perp}, Z_{(-1,\sqrt{3})^\perp}\}, \circ)$ neboli množina všech symetrií rovnostranného trojúhelníka

## Definice (Komutativní těleso)

Množina $T$ se nazývá *komutativní těleso*, pokud jsou na ní definovány dvě binární operace $+$ a $\cdot$ , splňující

1. $(T, +)$ je komutativní grupa.
2. Označíme-li neutrální prvek $(T, +)$ symbolem 0, pak $(T \setminus \{0\}, \cdot)$ je komutativní grupa.
3. $\forall a, b, c \in T : a \cdot (b + c) = a \cdot b + a \cdot c$ (distributivita)

Příklady:

1. $\mathbb{Q}$, $\mathbb{R}$ nebo $\mathbb{C}$ s operacemi sčítání a násobení
2. Pokud $p$ je prvočíslo, $\mathbb{Z}_p = \{0, 1, \ldots, p - 1\}$ s operacemi sčítání a násobení modulo $p$

Pokud nepožadujeme $(T \setminus \{0\}, \cdot)$ komutativní a doplníme distributivitu z druhé strany, pak definici splňují např. tzv. kvaterniony, používané pro elegantní popis rotací v $\mathbb{R}^3$.

Prvky $T$ hrají v lineární algebře roli skalárů. My se omezíme na $T = \mathbb{R}$ nebo $\mathbb{C}$ a budeme používat pojem *množina skalárů*.

## Definice (Vektorový prostor)

Nechť $\mathbb{F}$ je množina skalárů. Množinu $V$ nazveme *vektorovým prostorem nad* $\mathbb{F}$, pokud je na ní definována operace *sčítání vektorů*

$$+ : V \times V \to V$$

taková, že $(V, +)$ je komutativní grupa, a operace *násobení skalárem*

$$\cdot : \mathbb{F} \times V \to V,$$

jejíž výsledek pro $r \in \mathbb{F}$ a $v \in V$ označíme $rv$, a tyto operace splňují $\forall u, v \in V$ a $\forall r, s \in \mathbb{F}$

1. $1v = v$
2. $r(sv) = (rs)v$ (asociativita)
3. $(r + s)v = rv + sv$ (distributivita sčítání skalárů)
4. $r(u + v) = ru + rv$ (distributivita sčítání vektorů)

Neutrální prvek ve $(V, +)$ značíme $o$ (*nulový vektor*) a inverzní prvek k $v \in V$ značíme $-v$ (*opačný vektor*).

## Poznámky

- Z axiomů plyne $0v = 0$, $(-1)v = -v$, $ro = o$ ♣
- $\mathbb{F}^n$ nad $\mathbb{F}$ se nazývá *aritmetický vektorový prostor*
- $\mathbb{F}^{m\times n}$ je vektorový prostor nad $\mathbb{F}$
- Množina $F(M, \mathbb{F})$ všech funkcí z množiny $M$ do $\mathbb{F}$ s operacemi

  $$(f+g)(x) := f(x) + g(x)$$
  $$(rf)(x) := rf(x),$$

  je vektorový prostor. Pro $M = \mathbb{R}$ to dává prostor všech funkcí jedné reálné proměnné, pro $M = \mathbb{N}$ prostor všech nekonečných posloupností, pro $M = \{1, \ldots, n\}$ je to $\mathbb{F}^n$.
- $\mathbb{C}^n$ nad $\mathbb{R}$ je vektorový prostor.

## Definice

Nechť $V$ je vektorový prostor nad $\mathbb{F}$ a $W$ je neprázdná podmnožina $V$ taková, že $\forall v, w \in W$, $\forall r, s \in \mathbb{F}$ platí $rv + sw \in W$. Pak nazýváme $W$ *podprostorem* vektorového prostoru $V$, značíme $W \leq V$.

## Poznámky

- $W$ je podprostor, právě když je uzavřený na součty a násobení libovolným skalárem. ♣
- $0 := \{o\} \leq V$, $V \leq V$ jsou tzv. *triviální podprostory*.
- Podprostor vektorového prostoru je vektorový prostor. ♣
- Pokud $r_1, \ldots, r_n \in \mathbb{F}$, $v_1, \ldots, v_n \in V$, pak se $\sum_{i=1}^{n} r_i v_i$ nazývá *lineární kombinace* vektorů $v_i$ s koeficienty $r_i$. Pro neprázdnou $M \subset V$ značí $\langle M \rangle$ množinu všech lineárních kombinací prvků $M$, neboli její *lineární obal* ($\langle \emptyset \rangle := 0$). Lineární obal libovolné množiny je podprostor. ♣
- Množinu $v + W$, kde $v \in V$ a $W \leq V$, nazýváme *afinní podprostor* ve $V$. Je to podprostor, právě když $v \in W$. ♣

Nechť $W$ je vektorový prostor (který může a nemusí být podprostorem jiného vektorového prostoru). O množině $M \subset W$, pro kterou $\langle M \rangle = W$, říkáme, že prostor $W$ *generuje*, případně, že $M$ je *množinou generátorů* prostoru $W$.

Typicky existuje mnoho různých množin generujících stejný vektorový prostor:

$$\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}, \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \end{pmatrix} \right\}, \mathbb{R}^2, \mathbb{R}^2 \setminus \left\{ \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \end{pmatrix} \right\}$$

jsou všechno množiny generátorů prostoru $\mathbb{R}^2$. Přirozenou otázkou je, jak najít pro daný podprostor množinu generátorů co nejmenší.

## Definice

Lineární kombinace se nazývá *netriviální*, pokud má alespoň jeden koeficient nenulový. Podmožina $M$ vektorového prostoru $V$ nad $\mathbb{F}$ je *lineárně závislá*, pokud existují vektory $v_1, \ldots, v_n \in M$ a jejich netriviální lineární kombinace $\sum_{i=1}^{n} r_i v_i$ rovná nulovému vektoru $o$. V opačném případě je $M$ *lineárně nezávislá*.

## Příklady

- Množina $\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \end{pmatrix} \right\}$ je lineárně závislá, protože lze z vektorů vytvořit lineární kombinaci s koeficienty $-2, -3, 1$, která je netriviální a dává nulový vektor v $\mathbb{R}^2$.
- Množina $\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$ je lineárně nezávislá, protože lineární kombinace $r \begin{pmatrix} 1 \\ 0 \end{pmatrix} + s \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ může být rovna nulovému vektoru pouze pro $r = s = 0$.
- $\emptyset$ je lineárně nezávislá.
- $\{1, i\} \subset \mathbb{C}$ je l. nezávislá v $\mathbb{C}$ nad $\mathbb{R}$, l. závislá v $\mathbb{C}$ nad $\mathbb{C}$.

Tvrzení

*Nechť $V$ je vektorový prostor nad $\mathbb{F}$. Pak platí:*

1. *$M \subset V$ mající alespoň dva prvky je lineárně závislá, právě když existuje $v \in M$, který lze vyjádřit jako lineární kombinaci ostatních prvků $M$.*
2. *Nechť $M$ generuje $V$. Pak $M$ je lineárně závislá, právě když existuje vlastní podmnožina $N \subset M$, která generuje $V$.*

Důkaz.

Nechť existuje netriviální lineární kombinace $\sum_{i=1}^{n} r_i v_i = o$, kde $v_i$ jsou z $M$. Bez újmy na obecnosti předpokládejme, že $r_1 \neq 0$. Pak $v_1 = \sum_{i=2}^{n} \frac{-r_i}{r_1} v_i$. Naopak, pokud lze nějaký $v_1 \in M$ zapsat jako $\sum_{i=2}^{n} s_i v_i$, stačí položit $s_1 = -1$ a $\sum_{i=1}^{n} s_i v_i = o$. Tím je dokázán první bod. Pro druhý bod vyberme v $M$ vektor $v$, který je dle bodu 1 lineární kombinací ostatních. Pak lze vzít $N = M \setminus \{v\}$. Naopak, pokud $N \subset M$ obě generují $V$ a $v \in M \setminus N$, pak lze $v$ zapsat jako lineární kombinaci prvků $N$ a tedy podle bodu 1 je $M$ lineárně závislá. $\square$

**Definice**

Nechť $V$ je vektorový prostor nad $\mathbb{F}$. Množina $M$, která generuje $V$ a zároveň je lineárně nezávislá, se nazývá *báze vektorového prostoru $V$*.

Základním příkladem báze je kanonická báze $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ v $\mathbb{F}^n$. Je hned vidět, že je lineárně nezávislá a generuje $\mathbb{F}^n$.

Podle předchozího tvrzení je báze minimální množina generátorů, tedy taková, jejíž žádná vlastní podmnožina už stejný prostor negeneruje.

**Tvrzení**

*Nechť $V$ je vektorový prostor nad $\mathbb{F}$. Množina $M$ je bází $V$, právě když lze každý vektor z $V$ vyjádřit jako lineární kombinací prvků $M$ právě jedním způsobem.*

Jádro důkazu: pokud by $v \in V$ měl dvojí vyjádření $\sum_{i=1}^{n} r_i v_i$, $\sum_{i=1}^{n} s_i v_i$, pak by rozdíl těchto vyjádření byl netriviální lineární kombinací rovnou nulovému vektoru.

Předpokládejme, že $M = \{v_1, \ldots, v_n\}$ je báze vektorového prostoru $V$ nad $\mathbb{F}$. Každému vektoru $v \in V$ lze podle předchozího tvrzení přiřadit jednoznačně $n$-tici $(r_1, \ldots, r_n)$ prvků $\mathbb{F}$. Když tedy určíme nějaké pořadí prvků $M$, přiřazujeme vlastně vektoru $v$ z $V$ vektor $\mathbf{r}$ z $\mathbb{F}^n$. Tomuto vektoru se říká *vektor souřadnic vektoru $v$ vzhledem k bázi $M$* nebo též *reprezentace vektoru $v$ vzhledem k bázi $M$*. Pokud například

$$M = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

je báze $\mathbb{R}^{2\times 2}$, pak je matice $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ reprezentována vzhledem k $M$ vektorem $(1, 2, 3, 4)^T$. Počítání v rozličných vektorových prostorech můžeme takto převést na výpočty s vektory aritmetickými. Ale jak tyto výpočty ovlivňuje to, jakou bázi ve $V$ si zvolíme? Budou mít vždy příslušné aritmetické vektory stejný počet složek? A dá se vždy najít báze s konečně mnoha prvky? Odpovědi se pokusíme nalézt v příští přednášce.