

Lineární algebra 1

Přednáška č.7

Tělesa. Vektorové prostory (část 1)

Irena Penev

19.11.20205

- Tato přednáška má dvě části:
 - Tělesa
 - Vektorové prostory (část 1)

1 Tělesa

• Pripomenutí:

Definice

Grupa je uspořádaná dvojice $(G, \circ)$, kde G je množina a $\circ$ je binární operace na G (tj. $\circ : G \times G \rightarrow G$), splňující následující axiomy:

- 1 operace $\circ$ je asociativní, tj. $\forall a, b, c \in G: a \circ (b \circ c) = (a \circ b) \circ c$;
- 2 existuje prvek $e \in G$, který nazýváme *neutrálním prvkem* $(G, \circ)$, t.ž. $\forall a \in G: e \circ a = a \wedge a \circ e = a$;
- 3 $\forall a \in G$ existuje prvek $a' \in G$, který nazýváme *inverzním prvkem* k a , t.ž. $a \circ a' = e \wedge a' \circ a = e$.

Abelova grupa (nebo *abelovská grupa*) je grupa $(G, \circ)$, která splňuje další axiom:

- 4 operace $\circ$ je komutativní, tj. $\forall a, b \in G: a \circ b = b \circ a$.

Neabelovská grupa je grupa, která není abelovská.

• Pripomenutí:

- Každá grupa má **jediný** neutrální prvek.
- Každý prvek ve grupě má **jediný** inverzní prvek.

Definice

Těleso je uspořádaná trojice $(\mathbb{F}, +, \cdot)$, kde $\mathbb{F}$ je množina, zatímco $+$ a $\cdot$ jsou binární operace na množině $\mathbb{F}$ (tj. funkce z $\mathbb{F} \times \mathbb{F}$ do $\mathbb{F}$), které nazýváme *sčítáním* a *násobením* respektive, splňující následující axiomy:

- 1 sčítání a násobení jsou asociativní, tj.
 $\forall a, b, c \in \mathbb{F}: a + (b + c) = (a + b) + c \wedge a \cdot (b \cdot c) = (a \cdot b) \cdot c;$
- 2 sčítání a násobení jsou komutativní, tj.
 $\forall a, b \in \mathbb{F}: a + b = b + a \wedge a \cdot b = b \cdot a;$
- 3 existují **různé** prvky $0_{\mathbb{F}}, 1_{\mathbb{F}} \in \mathbb{F}$ takové, že $\forall a \in \mathbb{F}: a + 0_{\mathbb{F}} = a \wedge a \cdot 1_{\mathbb{F}} = a$; $0_{\mathbb{F}}$ nazýváme *neutrálním prvkem pro sčítání* a $1_{\mathbb{F}}$ nazýváme *neutrálním prvkem pro násobení*;
- 4 $\forall a \in \mathbb{F}$ existuje prvek v $\mathbb{F}$, který značíme $-a$ a nazýváme *opačným prvkem* k a , tj. $a + (-a) = 0_{\mathbb{F}}$;
- 5 $\forall a \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$ existuje prvek v $\mathbb{F}$, který značíme a^{-1} a nazýváme *inverzním prvkem* k a , tj. $a \cdot a^{-1} = 1_{\mathbb{F}}$;
- 6 násobení je distributivní vzhledem k sčítání, tj. $\forall a, b, c \in \mathbb{F}: a \cdot (b + c) = (a \cdot b) + (a \cdot c).$

Příklad

Následující struktury jsou tělesa:

- ① $(\mathbb{Q}, +, \cdot)$; ② $(\mathbb{R}, +, \cdot)$; ③ $(\mathbb{C}, +, \cdot)$.

- **Poznámka:** Další nekonečná tělesa existují, ale příklady uvádět nebudeme.
- **Pozor:** $(\mathbb{Z}, +, \cdot)$ **není** těleso, protože prvky $\mathbb{Z} \setminus \{-1, 0, 1\}$ nemají inverzní prvky.
- Za chvíli ověříme, že $(\mathbb{Z}_p, +, \cdot)$ je těleso pro každé **prvočíslo** p .
- **Terminologie/Značení:**
 - Jsou-li operace $+$ a $\cdot$ jasné z kontextu, říkáme pouze “těleso $\mathbb{F}$ ” namísto “těleso $(\mathbb{F}, +, \cdot)$ ”.
 - Pro $a, b \in \mathbb{F}$ obvykle píšeme:
 - ab namísto $a \cdot b$,
 - $a - b$ namísto $a + (-b)$.
 - Jako obvykle, pokud závorky neurčují jinak, provádíme nejprve násobení a teprve potom sčítání. Tedy pro $a, b, c \in \mathbb{F}$ píšeme:
 - $ab + c$ namísto $(a \cdot b) + c$,
 - $a + bc$ namísto $a + (b \cdot c)$.

- **Poznámka:** Nechť $\mathbb{F}$ je těleso.

- Z axiomů 2 a 3 plyne, že každé těleso má **právě jeden** neutrální prvek pro sčítání a **právě jeden** neutrální prvek pro násobení.
- Vskutku, jsou-li 0 a $0'$ neutrální prvky pro sčítání, pak platí

$$\begin{aligned} 0 &= 0 + 0' && \text{protože } 0' \text{ je neutrální prvek pro sčítání} \\ &= 0' + 0 && \text{protože } + \text{ je komutativní (dle axiomu 2)} \\ &= 0' && \text{protože } 0 \text{ je neutrální prvek pro sčítání.} \end{aligned}$$

- Podobně platí pro neutrální prvek pro násobení.
- Je-li $\mathbb{F}$ jasné z kontextu, píšeme prostě 0 a 1 namísto $0_{\mathbb{F}}$ a $1_{\mathbb{F}}$ respektive.

Tvrzení 1

Nechť $\mathbb{F}$ je těleso. Pak platí:

- a) $\forall a \in \mathbb{F}: 0a = a0 = 0;$
- b) $\forall a, b \in \mathbb{F}: ab = 0 \implies (a = 0 \vee b = 0);$
- c) $\forall a \in \mathbb{F}: (-1)a = -a.^a$

^aToto tvrzení si zaslouží vysvětlení. Zde je $-a$ opačný prvek k a . Naproti tomu $(-1)a$ je součin -1 (opačného prvku k neutrálnímu prvku pro násobení) a a . Proto $-a$ není jen zkratka pro $(-1)a$. Oba výrazy jsou si rovny, ale musíme to dokázat!

- Důkaz: za chvíli!
- Nejdříve pár poznámek.

- **Poznámky:** Nechť $(\mathbb{F}, +, \cdot)$ je těleso, a nechť $0_{\mathbb{F}}$ a $1_{\mathbb{F}}$ jsou neutrální prvky pro sčítání a násobení v tomto tělese.

① Dle axiomů 1-4 je $(\mathbb{F}, +)$ Abelova grupa s neutrálním prvkem $0_{\mathbb{F}}$.

- Pro $a \in \mathbb{F}$, opačný prvek k a v tělese $(\mathbb{F}, +, \cdot)$ je právě inverzní prvek k a v grupě $(\mathbb{F}, +)$.
- Jelikož každý prvek v grupě má **jediný** inverzní prvek, plyne, že každý prvek $a \in \mathbb{F}$ má **jediný** opačný prvek $-a$.

② Dle axiomů 1-3 a 5 je $(\mathbb{F} \setminus \{0\}, \cdot)$ Abelova grupa s neutrálním prvkem $1_{\mathbb{F}}$.

- Pro $a \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$, inverzní prvek k a v tělese $\mathbb{F}$ je právě inverzní prvek k a v grupě $(\mathbb{F} \setminus \{0_{\mathbb{F}}\}, \cdot)$, ale s jedním potenciálním problémem...
- Musíme ověřit, že $0_{\mathbb{F}}$ není inverzní prvek k žádnému prvku v $\mathbb{F} \setminus \{0_{\mathbb{F}}\}$!
- Plyne to z toho, že pro každé $a \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$ platí $0_{\mathbb{F}}a = a0_{\mathbb{F}} = 0_{\mathbb{F}} \neq 1_{\mathbb{F}}$, a tedy $0_{\mathbb{F}}$ není inverzní prvek k a .

③ Dle axiomů 2 a 6, pro každé $a, b, c \in \mathbb{F}$ platí:

- $a(b + c) \stackrel{\text{ax. 6.}}{=} ab + ac$;
- $(b + c)a \stackrel{\text{ax. 2.}}{=} a(b + c) \stackrel{\text{ax. 6.}}{=} ab + ac \stackrel{\text{ax. 2.}}{=} ba + ca$.

Tvrzení 1

Nechť $\mathbb{F}$ je těleso. Pak platí:

- (a) $\forall a \in \mathbb{F}: 0a = a0 = 0$;
- (b) $\forall a, b \in \mathbb{F}: ab = 0 \implies (a = 0 \vee b = 0)$;
- (c) $\forall a \in \mathbb{F}: (-1)a = -a$.^a

^aToto tvrzení si zaslouží vysvětlení. Zde je $-a$ opačný prvek k a . Naproti tomu $(-1)a$ je součin -1 (opačného prvku k neutrálnímu prvku pro násobení) a a . Proto $-a$ není jen zkratka pro $(-1)a$. Oba výrazy jsou si rovny, ale musíme to dokázat!

Důkaz. (a) Nechť $a \in \mathbb{F}$. Jelikož je násobení v tělese $\mathbb{F}$ komutativní, platí $0a = a0$. Tedy stačí dokázat, že $a0 = 0$.

Všimněme si, že

$$a0 \stackrel{\text{ax. 3}}{=} a(0 + 0) \stackrel{\text{ax. 6}}{=} a0 + a0.$$

Tím je ukázáno, že platí $a0 = a0 + a0$, a tedy (viz příští slajd):

Důkaz (pokračování). Připomenutí: $a0 = a0 + a0$.

0	$=$	$-(a0) + a0$	protože je $-(a0)$ opačný prvek k $a0$
	$=$	$-(a0) + (a0 + a0)$	protože $a0 = a0 + a0$ (dokázáno výše)
	$=$	$(-(a0) + a0) + a0$	protože je $+$ asociativní
	$=$	$0 + a0$	protože je $-(a0)$ opačný prvek k $a0$
	$=$	$a0$	protože je 0 neutrální prvek pro sčítání tělesa $\mathbb{F}$.

Tedy $a0 = 0$. Tím je ukázáno (a).

Tvrzení 1

Nechť $\mathbb{F}$ je těleso. Pak platí:

- a) $\forall a \in \mathbb{F}: 0a = a0 = 0;$
- b) $\forall a, b \in \mathbb{F}: ab = 0 \implies (a = 0 \vee b = 0);$
- c) $\forall a \in \mathbb{F}: (-1)a = -a.$ ^a

^aToto tvrzení si zaslouží vysvětlení. Zde je $-a$ opačný prvek k a . Naproti tomu $(-1)a$ je součin -1 (opačného prvku k neutrálnímu prvku pro násobení) a a . Proto $-a$ není jen zkratka pro $(-1)a$. Oba výrazy jsou si rovny, ale musíme to dokázat!

Důkaz (pokračování). (b) Nechť $a, b \in \mathbb{F}$ jsou takové, že $ab = 0$. Je třeba ukázat, že $a = 0$ nebo $b = 0$. Můžeme předpokládat, že $b \neq 0$, protože jinak máme hotovo. Nyní má b inverzní prvek b^{-1} , a tedy platí:

$$a = a \cdot 1 = a(\underbrace{bb^{-1}}_{=1}) \stackrel{\text{ax. 1}}{=} (\underbrace{ab}_{=0})b^{-1} = 0b^{-1} \stackrel{(a)}{=} 0.$$

Tím jsme dokázali (b).

Důkaz (pokračování). (c). Nechť $a \in \mathbb{F}$. Je třeba ukázat, že $(-1)a = -a$. Nejprve si všimněme, že

$$0 \stackrel{(a)}{=} 0a = (1-1)a = 1a + (-1)a = a + (-1)a,$$

a tedy

$$-a = -a + 0$$

protože 0 je neutrální prvek pro sčítání v tělese $\mathbb{F}$

$$= -a + (a + (-1)a)$$

protože $0 = a + (-1)a$
(dokázáno výše)

$$= (-a + a) + (-1)a$$

protože je + asociativní

$$= 0 + (-1)a$$

protože je $-a$ opačný prvek k a

$$= (-1)a$$

protože 0 je neutrální prvek pro sčítání v tělese $\mathbb{F}$

Tím je ukázáno (c). $\square$

Tvrzení 1

Nechť $\mathbb{F}$ je těleso. Pak platí:

- Ⓐ $\forall a \in \mathbb{F}: 0a = a0 = 0;$
- Ⓑ $\forall a, b \in \mathbb{F}: ab = 0 \implies (a = 0 \vee b = 0);$
- Ⓒ $\forall a \in \mathbb{F}: (-1)a = -a.^a$

^aToto tvrzení si zaslouží vysvětlení. Zde je $-a$ opačný prvek k a . Naproti tomu $(-1)a$ je součin -1 (opačného prvku k neutrálnímu prvku pro násobení) a a . Proto $-a$ není jen zkratka pro $(-1)a$. Oba výrazy jsou si rovny, ale musíme to dokázat!

- Nyní uvažujme **konečná** tělesa.
- Jak uvidíme, $\mathbb{Z}_p$ je těleso pro každé prvočíslo p .
 - Na druhou stranu, pokud $n \in \mathbb{N}$ **není** prvočíslo, pak $(\mathbb{Z}_n, +, \cdot)$ **není** těleso.
- Připomeňme si Malou Fermatovu větu.

Malá Fermatova věta

Pro každé prvočíslo $p \in \mathbb{N}$ a každé $a \in \mathbb{Z}_p \setminus \{0\}$, platí $a^{p-1} = 1$.

Věta 2

$(\mathbb{Z}_p, +, \cdot)$ je těleso pro každé prvočíslo p .

Důkaz. Je zřejmé, že $(\mathbb{Z}_p, +, \cdot)$ splňuje axiomy 1-4 a 5. Zbývá dokázat, že $(\mathbb{Z}_p, +, \cdot)$ splňuje axiom 5. Nechť $a \in \mathbb{Z}_p \setminus \{0\}$. Dle Malé Fermatovy věty platí $a \cdot a^{p-2} = a^{p-1} = 1$, a tedy je a^{p-2} inverzní prvek k a . $\square$

Malá Fermatova věta

Pro každé prvočíslo $p \in \mathbb{N}$ a každé $a \in \mathbb{Z}_p \setminus \{0\}$, platí $a^{p-1} = 1$.

- **Poznámka:** Pokud $n \in \mathbb{N}$ **není** prvočíslo, pak $(\mathbb{Z}_n, +, \cdot)$ **není** těleso.
- Vskutku:
 - ① Pro $n = 1$ má $\mathbb{Z}_n = \mathbb{Z}_1$ pouze jeden prvek, zatímco každé těleso má alespoň dva různé prvky (a to 0 a 1).
 - ② Předpokládejme nyní, že $n \in \mathbb{N}$ je složené číslo, a tedy $n = pq$ pro nějaká celá čísla $p, q \geq 2$.
 - Pak platí $[p]_n[q]_n = [pq]_n = [n]_n = 0$.
 - Kdyby $(\mathbb{Z}_n, +, \cdot)$ bylo těleso, pak by z Tvzení 1(b) plynulo, že $[p]_n = 0$ nebo $[q]_n = 0$, a tedy $p \equiv 0 \pmod{n}$ nebo $q \equiv 0 \pmod{n}$, tj. $n \mid p$ nebo $n \mid q$, což je spor.

Věta 3

Nechť $n \geq 2$ je celé číslo. Pak existuje těleso o velikosti n právě tehdy, když je n mocninou prvočísla.^a Dále, je-li n mocninou prvočísla, pak až na „isomorfismus“ (tj. až na přejmenování operací a prvků tělesa) existuje právě jedno těleso o velikosti n , a to se značí $\mathbb{F}_n$.^b

^a„ n je mocninou prvočísla“ znamená, že existuje prvočíslu p a kladné celé číslo m takové, že $n = p^m$.

^bTechnicky jde o těleso $(\mathbb{F}_n, +, \cdot)$, ale obvykle píšeme prostě $\mathbb{F}_n$.

Důkaz. Vynechán.

- **Poznámka:** Pro prvočíslu p platí $\mathbb{F}_p = \mathbb{Z}_p$.
 - Na druhou stranu, pro $n = p^m$, kde p je prvočíslu a $m \geq 2$ je celé číslo, $\mathbb{F}_n \neq \mathbb{Z}_n$ (protože $\mathbb{F}_n$ je těleso, zatímco $\mathbb{Z}_n$ **není** těleso).

- Nechť $\mathbb{F}$ je těleso. Pro $a \in \mathbb{F} \setminus \{0\}$ občas píšeme $\frac{1}{a}$ namísto a^{-1} (inverzní prvek k a v tělese $\mathbb{F}$).
 - Např. v $\mathbb{Z}_3$ máme $\frac{1}{1} = 1^{-1} = 1$ a $\frac{1}{2} = 2^{-1} = 2$ (protože v $\mathbb{Z}_3$ platí $2 \cdot 2 = 1$).
- Podobně pro $a, b \in \mathbb{F}$ t.ž. $b \neq 0$, občas píšeme $\frac{a}{b}$ namísto $b^{-1}a$.
 - Např. v $\mathbb{Z}_5$ máme $3^{-1} = 2$ (protože $3 \cdot 2 = 1$), a tedy $\frac{4}{3} = 3^{-1} \cdot 4 = 2 \cdot 4 = 3$.
- Občas je pohodlné používat značení
 - $\frac{1}{a}$ namísto a^{-1} , nebo
 - $\frac{a}{b}$ namísto $b^{-1}a$.
- Ovšem, když pracujeme nad konečným tělesem jako např. $\mathbb{Z}_p$ (pro prvočíslo p), náš konečný výsledek **nikdy** nesmí být zlomek a vždy musíme výsledek zjednodušit.

Definice

Charakteristika tělesa $\mathbb{F}$, značená $\text{char}(\mathbb{F})$, je nejmenší $n \in \mathbb{N}$ t.ž. v tělese $\mathbb{F}$ platí

$$\underbrace{1 + \cdots + 1}_n = 0,$$

kde 1 a 0 jsou neutrální prvky pro sčítání a pro násobení v tělese $\mathbb{F}$. Pokud takové n neexistuje, pak definujeme $\text{char}(\mathbb{F}) := 0$.

- Tělesa $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ mají charakteristiku 0.
 - **Pozor:** Existují nekonečná tělesa, která mají kladnou charakteristiku! (Ale příklady uvádět nebudeme.)
- Pro každé prvočíslo p platí $\text{char}(\mathbb{Z}_p) = p$.

Věta 4

Charakteristika tělesa je buď nula, nebo prvočíslo.

Věta 4

Charakteristika tělesa je buď nula, nebo prvočíslo.

Důkaz. Nechť $\mathbb{F}$ je těleso. Můžeme předpokládat, že $\text{char}(\mathbb{F}) \neq 0$, protože jinak máme hotovo. Tedy $\text{char}(\mathbb{F})$ je kladné celé číslo.

Dle definice tělesa platí $1 \neq 0$, a proto $\text{char}(\mathbb{F}) \geq 2$.

Předpokládejme nyní, že $\text{char}(\mathbb{F})$ není prvočíslo, a nechte $p, q \geq 2$ jsou celá čísla t.ž. $\text{char}(\mathbb{F}) = pq$. Tedy

$$\underbrace{(1 + \cdots + 1)}_p \underbrace{(1 + \cdots + 1)}_q = \underbrace{1 + \cdots + 1}_{pq} = 0.$$

Jelikož je $\mathbb{F}$ těleso, plyne z Tvzení 1(b), že alespoň jedno z čísel $\underbrace{1 + \cdots + 1}_p$ a $\underbrace{1 + \cdots + 1}_q$ je rovno 0, což je spor, protože

$0 < p, q < \text{char}(\mathbb{F})$. $\square$

2 Vektorové prostory (část 1)

Definice

Nechť $\mathbb{F}$ je těleso (jehož prvky budeme nazývat *skaláry*), s neutrálními prvky 0 pro sčítání a 1 pro násobení. *Vektorový prostor* nad tělesem $\mathbb{F}$ je množina V (jejíž prvky budeme nazývat *vektory*) s operacemi sčítání vektorů $+: V \times V \rightarrow V$ a násobení vektoru skalárem $\cdot: \mathbb{F} \times V \rightarrow V$, splňující následující axiomy:

- 1 $(V, +)$ je Abelova grupa; neutrální prvek grupy $(V, +)$ značíme $\mathbf{0}$ („nulový vektor“), zatímco inverzní prvek k vektoru $\mathbf{v} \in V$ v grupě $(V, +)$ značíme $-\mathbf{v}$ („opačný prvek k vektoru $\mathbf{v}$ “);
- 2 $\forall \mathbf{v} \in V: 1\mathbf{v} = \mathbf{v}$;
- 3 $\forall \mathbf{v} \in V, \alpha, \beta \in \mathbb{F}: (\alpha + \beta)\mathbf{v} = \alpha\mathbf{v} + \beta\mathbf{v}$;
- 4 $\forall \mathbf{v} \in V, \alpha, \beta \in \mathbb{F}: (\alpha\beta)\mathbf{v} = \alpha(\beta\mathbf{v})$;
- 5 $\forall \mathbf{u}, \mathbf{v} \in V, \alpha \in \mathbb{F}: \alpha(\mathbf{u} + \mathbf{v}) = \alpha\mathbf{u} + \alpha\mathbf{v}$.

- **Terminologie:**

- *Reálný vektorový prostor* je vektorový prostor nad tělesem $\mathbb{R}$.
- *Komplexní vektorový prostor* je vektorový prostor nad tělesem $\mathbb{C}$.

Příklad

Nechť $\mathbb{F}$ je těleso. Pak všechny následující struktury jsou vektorové prostory nad $\mathbb{F}$ (v každém případě jsou sčítání vektorů a násobení skalárem definovány přirozeným způsobem):

- 1 $\mathbb{F}^n$;
- 2 $\mathbb{F}^{n \times m}$;
- 3 množina všech funkcí z $\mathbb{F}$ do $\mathbb{F}$;
- 4 množina $\mathbb{P}_{\mathbb{F}}$ všech polynomů (v jedné proměnné, obvykle x) s koeficienty v tělese $\mathbb{F}$;^a
 - **Značení:** Některé učebnice používají značení $\mathbb{F}[x]$ místo $\mathbb{P}_{\mathbb{F}}$ (kde polynomy jsou v proměnné x).
- 5 pro celé číslo $n \geq 0$, množina $\mathbb{P}_{\mathbb{F}}^n$ všech polynomů stupně $\leq n$ s koeficienty v $\mathbb{F}$.^b

^aLze samozřejmě uvažovat i polynomy ve více proměnných (např. $x_1, \dots, x_k$) s koeficienty v $\mathbb{F}$. Také tato množina je vektorovým prostorem nad $\mathbb{F}$.

^bZnačení $\mathbb{P}_{\mathbb{F}}^n$ není úplně standardní (úplně standardní značení pro tento vektorový prostor neexistuje).

- Další příklad (pokud znáte matematickou analýzu):

Příklad

Následující množiny jsou reálné vektorové prostory (se sčítáním vektorů a násobením skalárem definovanými obvyklým způsobem):

- 1 množina všech spojitých funkcí z $\mathbb{R}$ do $\mathbb{R}$;
- 2 množina všech diferencovatelných funkcí z $\mathbb{R}$ do $\mathbb{R}$.

- **Terminologie:**

- Prvky libovolného vektorového prostoru nazýváme „vektory“ (dokonce i v případě, že „nevypadají“ jako vektory, tj. když jsou např. matice, funkce nebo polynomy).

- Pro libovolné těleso $\mathbb{F}$ máme *triviální* vektorový prostor $\{\mathbf{0}\}$ nad tělesem $\mathbb{F}$.
 - V tomto vektorovém prostoru jsou sčítání vektorů a násobení vektorů skalárem definovány očividným způsobem:
 - $\mathbf{0} + \mathbf{0} = \mathbf{0}$;
 - $\forall \alpha \in \mathbb{F}: \alpha \mathbf{0} = \mathbf{0}$.
- Vektorový prostor je *netriviální*, pokud má alespoň jeden nenulový vektor.

Tvrzení 5

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

- (a) $\forall \mathbf{v} \in V: 0\mathbf{v} = \mathbf{0};^a$
- (b) $\forall \alpha \in \mathbb{F}: \alpha\mathbf{0} = \mathbf{0};$
- (c) $\forall \mathbf{v} \in V, \alpha \in \mathbb{F}: \alpha\mathbf{v} = \mathbf{0} \implies (\alpha = 0 \vee \mathbf{v} = \mathbf{0});$
- (d) $\forall \mathbf{v} \in V: (-1)\mathbf{v} = -\mathbf{v}.^b$

^aTady je 0 neutrální prvek pro sčítání v tělese $\mathbb{F}$, zatímco $\mathbf{0}$ je nulový vektor ve vektorovém prostoru V .

^bTady je -1 opačný prvek k neutrálnímu prvku pro násobení v tělese $\mathbb{F}$, a zejména je -1 skalár. Tedy $(-1)\mathbf{v}$ je součin skaláru -1 a vektoru $\mathbf{v}$. Na druhou stranu $-\mathbf{v}$ je opačný prvek k vektoru $\mathbf{v}$.

Důkaz. Vynechán (ale jednoduchý).

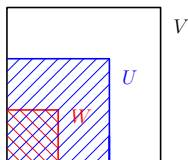
Definice

Nechť V je vektorový prostor nad tělesem $\mathbb{F}$. *Vektorový podprostor* (nebo prostě *podprostor*) vektorového prostoru V je podmnožina $U \subseteq V$ t.ž. samotné U je vektorový prostor nad tělesem $\mathbb{F}$, s operacemi „převzatými“ z V .^a

^aVšimněme si, že musíme mít stejné těleso $\mathbb{F}$ pro U a V !

- To znamená, že sčítáme vektory v U stejným způsobem jako ve V , a stejně tak pro násobení skalárem.
- Navíc musí množina U být “uzavřená vzhledem k” sčítání vektorů a násobení skalárem, tj. platí:
 - $\forall \mathbf{u}_1, \mathbf{u}_2 \in U: \mathbf{u}_1 + \mathbf{u}_2 \in U$,
 - $\forall \mathbf{u} \in U, \alpha \in \mathbb{F}: \alpha \mathbf{u} \in U$,

kde sčítání vektorů a násobení skalárem jsou převzaty z vektorového prostoru V .



- **Poznámka:** Je zřejmé, že je-li W podprostor U a U podprostor V , pak je W podprostor V .
 - Neformálně: „Podprostor podprostoru je podprostor.”

Příklad

Nechť V je vektorový prostor nad tělesem $\mathbb{F}$. Pak je samotné V podprostorem vektorového prostoru V , a zároveň je $\{\mathbf{0}\}$ podprostorem V .

- **Terminologie:** Nechť V je vektorový prostor nad tělesem $\mathbb{F}$.
 - *Triviální podprostor* vektorového prostoru V je podprostor $\{\mathbf{0}\}$.
 - *Netriviální podprostor* vektorového prostoru V je podprostor, který má alespoň jeden nenulový vektor.
 - Podprostor U vektorového prostoru V je *vlastní*, pokud $U \subsetneq V$.

Příklad

Nechť $n \in \mathbb{N}$ a necht $\mathbb{F}$ je těleso. Pak je $\mathbb{P}_{\mathbb{F}}^n$ podprostor vektorového prostoru $\mathbb{P}_{\mathbb{F}}$.

- Další příklad (pokud znáte matematickou analýzu):

Příklad

- Reálný prostor **diferencovatelných funkcí** z $\mathbb{R}$ do $\mathbb{R}$ je podprostorem reálného prostoru **spojitých funkcí** z $\mathbb{R}$ do $\mathbb{R}$.
- Reálný prostor **spojitých funkcí** z $\mathbb{R}$ do $\mathbb{R}$ je podprostorem reálného prostoru **všech funkcí** z $\mathbb{R}$ do $\mathbb{R}$.

Věta 6

Nechť V je vektorový prostor nad tělesem $\mathbb{F}$ a necht' $U \subseteq V$. Pak je U podprostorem V právě tehdy, když platí:

- i) $\mathbf{0} \in U$; ^a
- ii) množina U je uzavřena vzhledem k sčítání, tj. $\forall \mathbf{u}, \mathbf{v} \in U$:
 $\mathbf{u} + \mathbf{v} \in U$;
- iii) množina U je uzavřena vzhledem k násobení skalárem, tj.
 $\forall \mathbf{u} \in U, \alpha \in \mathbb{F}: \alpha \mathbf{u} \in U$.

^aTady je $\mathbf{0}$ nulový vektor vektorového prostoru V .

Důkaz. Vynechán.

- Detaily viz skripta (Penev, Theorem 3.1.7 - nepovinná četba)

Definice

Nechť V je vektorový prostor nad tělesem $\mathbb{F}$. Vektor $\mathbf{v} \in V$ je *lineární kombinací* vektorů $\mathbf{u}_1, \dots, \mathbf{u}_k \in V$, pokud existují skaláry $\alpha_1, \dots, \alpha_k \in \mathbb{F}$ t.ž.

$$\mathbf{v} = \alpha_1 \mathbf{u}_1 + \dots + \alpha_k \mathbf{u}_k.$$

Lineární obal množiny $\{\mathbf{u}_1, \dots, \mathbf{u}_k\}$, značený $\text{Span}(\{\mathbf{u}_1, \dots, \mathbf{u}_k\})$ nebo $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$, je množina všech lineárních kombinací vektorů $\mathbf{u}_1, \dots, \mathbf{u}_k$, tj.

$$\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k) = \{\alpha_1 \mathbf{u}_1 + \dots + \alpha_k \mathbf{u}_k \mid \alpha_1, \dots, \alpha_k \in \mathbb{F}\}.$$

Dohodou je „prázdný součet“ vektorů v V definován jako $\mathbf{0}$ (nulový vektor),^a a tedy $\text{Span}(\emptyset) = \{\mathbf{0}\}$.

^a„Prázdný součet“ je součet tvaru $\alpha_1 \mathbf{u}_1 + \dots + \alpha_k \mathbf{u}_k$, kde $k = 0$ (a tedy nemáme žádné $\mathbf{u}_i$ a žádné α_i).

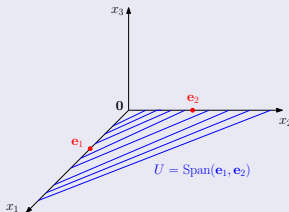
- Před několika týdny (v Přednášce č.3) jsme definovali lineární obal konečné množiny vektorů v $\mathbb{F}^n$ (kde $\mathbb{F}$ je těleso).
- Nyní jsme to zobecnili pro vektory v libovolném vektorovém prostoru.
- **Terminologie:** Nechť V je vektorový prostor nad tělesem $\mathbb{F}$. Vektory $\mathbf{u}_1, \dots, \mathbf{u}_k \in V$ *generují* V (nebo množina $\{\mathbf{u}_1, \dots, \mathbf{u}_k\}$ *generuje* V), pokud $V = \text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$.
 - Všimněme si, že $\emptyset$ generuje triviální vektorový prostor $\{\mathbf{0}\}$ nad tělesem $\mathbb{F}$.

Příklad

Uvažujme vektory $\mathbf{e}_1 = [1 \ 0 \ 0]^T$ a $\mathbf{e}_2 = [0 \ 1 \ 0]^T$ v $\mathbb{R}^3$.

Pak platí $\text{Span}(\mathbf{e}_1, \mathbf{e}_2) = \left\{ \begin{bmatrix} x_1 \\ x_2 \\ 0 \end{bmatrix} \mid x_1, x_2 \in \mathbb{R} \right\}$. Tedy $\text{Span}(\mathbf{e}_1, \mathbf{e}_2)$

je rovina $x_3 = 0$ v $\mathbb{R}^3$.



Příklad

Uvažujme polynomy $1, x, x^2$ v $\mathbb{P}_{\mathbb{R}}$. Pak platí

$\text{Span}(1, x, x^2) = \{a_2x^2 + a_1x + a_0 \mid a_0, a_1, a_2 \in \mathbb{R}\} = \mathbb{P}_{\mathbb{R}}^2$.

- Pro matici $A = [\mathbf{a}_1 \quad \dots \quad \mathbf{a}_m]$ v $\mathbb{F}^{n \times m}$ platí
 $\text{Span}(\mathbf{a}_1, \dots, \mathbf{a}_m) = \{ A\mathbf{x} \mid \mathbf{x} \in \mathbb{F}^m \}.$
- Dokázali jsme to v Přednášce č.3, ale tady je důkaz ještě jednou:

$$\begin{aligned}
 \text{Span}(\mathbf{a}_1, \dots, \mathbf{a}_m) &= \left\{ x_1 \mathbf{a}_1 + \dots + x_m \mathbf{a}_m \mid x_1, \dots, x_m \in \mathbb{F} \right\} \\
 &= \left\{ [\mathbf{a}_1 \quad \dots \quad \mathbf{a}_m] \begin{bmatrix} x_1 \\ \vdots \\ x_m \end{bmatrix} \mid x_1, \dots, x_m \in \mathbb{F} \right\} \\
 &= \left\{ A\mathbf{x} \mid \mathbf{x} \in \mathbb{F}^m \right\}.
 \end{aligned}$$

- Plyne, že $\forall \mathbf{b} \in \mathbb{F}^n$:
 $\mathbf{b} \in \text{Span}(\mathbf{a}_1, \dots, \mathbf{a}_m) \iff$ rovnice $A\mathbf{x} = \mathbf{b}$ je řešitelná.

Tvrzení 7

Nechť $\mathbb{F}$ je těleso a $\mathbf{a}_1, \dots, \mathbf{a}_m$ ($m \geq 1$) jsou vektory v $\mathbb{F}^n$. Položme $A := [\mathbf{a}_1 \ \dots \ \mathbf{a}_m]$. Pak jsou ekvivalentní následující tvrzení:

- Ⓐ vektory $\mathbf{a}_1, \dots, \mathbf{a}_m$ generují $\mathbb{F}^n$, tj. $\text{Span}(\mathbf{a}_1, \dots, \mathbf{a}_m) = \mathbb{F}^n$;
- Ⓑ $\forall \mathbf{b} \in \mathbb{F}^n$ je rovnice $A\mathbf{x} = \mathbf{b}$ řešitelná;
- Ⓒ $\text{rank}(A) = n$ (tj. A má plnou řádkovou hodnotu).

Důkaz. Dle Důsledku 9 z Přednášky č.3 jsou (b) a (c) ekvivalentní.

Na druhou stranu, ekvivalence (a) a (b) plyne z toho, že

$$\text{Span}(\mathbf{a}_1, \dots, \mathbf{a}_m) = \{A\mathbf{x} \mid \mathbf{x} \in \mathbb{F}^m\}.$$

Vskutku, máme následující posloupnost ekvivalentních tvrzení (viz následující slajd):

Důkaz (pokračování).

$$\begin{array}{ll} \underbrace{\text{vektory } \mathbf{a}_1, \dots, \mathbf{a}_m \text{ generují } \mathbb{F}^n}_{(a)} & \iff \text{Span}(\mathbf{a}_1, \dots, \mathbf{a}_m) = \mathbb{F}^n \\ & \iff \{A\mathbf{x} \mid \mathbf{x} \in \mathbb{F}^m\} = \mathbb{F}^n \\ & \iff \forall \mathbf{b} \in \mathbb{F}^n \exists \mathbf{x} \in \mathbb{F}^m \\ & \quad \text{t.ž. } A\mathbf{x} = \mathbf{b} \\ & \iff \forall \mathbf{b} \in \mathbb{F}^n: A\mathbf{x} = \mathbf{b} \text{ je} \\ & \quad \underbrace{\text{řešitelná.}}_{(b)} \end{array}$$

Tedy jsou (a) a (b) ekvivalentní. $\square$

Tvrzení 7

Nechť $\mathbb{F}$ je těleso a $\mathbf{a}_1, \dots, \mathbf{a}_m$ ($m \geq 1$) jsou vektory v $\mathbb{F}^n$. Položme $A := [\mathbf{a}_1 \ \dots \ \mathbf{a}_m]$. Pak jsou ekvivalentní následující tvrzení:

- Ⓐ vektory $\mathbf{a}_1, \dots, \mathbf{a}_m$ generují $\mathbb{F}^n$, tj. $\text{Span}(\mathbf{a}_1, \dots, \mathbf{a}_m) = \mathbb{F}^n$;
- Ⓑ $\forall \mathbf{b} \in \mathbb{F}^n$ je rovnice $A\mathbf{x} = \mathbf{b}$ řešitelná;
- Ⓒ $\text{rank}(A) = n$ (tj. A má plnou řádkovou hodnotu).

Věta 8

Nechť V je vektorový prostor nad tělesem $\mathbb{F}$ a necht' $\mathbf{u}_1, \dots, \mathbf{u}_k \in V$ ($k \geq 0$).^a Pak platí následující tvrzení:

- Ⓐ $\mathbf{u}_1, \dots, \mathbf{u}_k \in \text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$;
- Ⓑ $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$ je podprostorem V ;
- Ⓒ pro každý podprostor U vektorového prostoru V t.ž. $\mathbf{u}_1, \dots, \mathbf{u}_k \in U$, pak $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$ je podprostor U ;
- Ⓓ $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$ je roven průniku všech podprostorů vektorového prostoru V , které obsahují vektory $\mathbf{u}_1, \dots, \mathbf{u}_k$.

^aPokud $k = 0$, pak je množina $\{\mathbf{u}_1, \dots, \mathbf{u}_k\}$ prázdná, a platí $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k) = \{\mathbf{0}\}$.

- Důkaz: za chvíli! Nejprve poznámka.
- **Poznámka:** V některých učebnicích je $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$ **definován** jako průnik všech podprostorů vektorového prostoru V , které obsahují vektory $\mathbf{u}_1, \dots, \mathbf{u}_k$.
 - Dle Věty 8(d) je tato alternativní definice ekvivalentní naší původní definici.

Věta 8

Nechť V je vektorový prostor nad tělesem $\mathbb{F}$ a necht' $\mathbf{u}_1, \dots, \mathbf{u}_k \in V$ ($k \geq 0$).^a Pak platí následující tvrzení:

- (a) $\mathbf{u}_1, \dots, \mathbf{u}_k \in \text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$;
- (b) $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$ je podprostorem V ;
- (c) pro každý podprostor U vektorového prostoru V t.ž. $\mathbf{u}_1, \dots, \mathbf{u}_k \in U$, pak $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$ je podprostor U ;
- (d) $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$ je roven průniku všech podprostorů vektorového prostoru V , které obsahují vektory $\mathbf{u}_1, \dots, \mathbf{u}_k$.

^aPokud $k = 0$, pak je množina $\{\mathbf{u}_1, \dots, \mathbf{u}_k\}$ prázdná, a platí $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k) = \{\mathbf{0}\}$.

Důkaz. Dokažme nejprve (a). Pro každý index $i \in \{1, \dots, k\}$ platí

$$\mathbf{u}_i = 0\mathbf{u}_1 + \dots + 0\mathbf{u}_{i-1} + \mathbf{u}_i + 0\mathbf{u}_{i+1} + \dots + 0\mathbf{u}_k,$$

a tedy $\mathbf{u}_i \in \text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$. Tím jsme dokázali (a).

Důkaz (pokračování). Nyní dokažme (b).

ⓑ $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$ je podprostorem V

Stačí dokázat, že $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$ splňuje (i), (ii) a (iii) z Věty 6, tj. že platí následující tvrzení:

ⓐ $\mathbf{0} \in \text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$;

ⓑ $\forall \mathbf{v}_1, \mathbf{v}_2 \in \text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k): \mathbf{v}_1 + \mathbf{v}_2 \in \text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$;

ⓒ $\forall \mathbf{v} \in \text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k), \alpha \in \mathbb{F}: \alpha \mathbf{v} \in \text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$.

(i). $\mathbf{0} = 0\mathbf{u}_1 + \dots + 0\mathbf{u}_k \in \text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$.

(ii). Nechť $\mathbf{v}_1, \mathbf{v}_2 \in \text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$. Pak existují skaláry $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_k \in \mathbb{F}$ t.ž. $\mathbf{v}_1 = \alpha_1\mathbf{u}_1 + \dots + \alpha_k\mathbf{u}_k$ a $\mathbf{v}_2 = \beta_1\mathbf{u}_1 + \dots + \beta_k\mathbf{u}_k$. Nyní platí

$$\begin{aligned}\mathbf{v}_1 + \mathbf{v}_2 &= (\alpha_1\mathbf{u}_1 + \dots + \alpha_k\mathbf{u}_k) + (\beta_1\mathbf{u}_1 + \dots + \beta_k\mathbf{u}_k) \\ &= (\alpha_1 + \beta_1)\mathbf{u}_1 + \dots + (\alpha_k + \beta_k)\mathbf{u}_k,\end{aligned}$$

a tedy $\mathbf{v}_1 + \mathbf{v}_2 \in \text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$. Tím jsme dokázali (ii).
Důkaz (iii) je velmi podobný. Tím je dokázáno (b).

Důkaz (pokračování).

Tvrzení. Pro každý podprostor U vektorového prostoru V ,
t.ž. $\mathbf{u}_1, \dots, \mathbf{u}_k \in U$, platí $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k) \subseteq U$.

Důkaz Tvrzení. Nechť U je libovolný podprostor vektorového prostoru V , t.ž. $\mathbf{u}_1, \dots, \mathbf{u}_k \in U$; je třeba dokázat, že $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k) \subseteq U$.

Nechť $\mathbf{v} \in \text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$. Pak existují skaláry $\alpha_1, \dots, \alpha_k \in \mathbb{F}$
t.ž.

$$\mathbf{v} = \alpha_1 \mathbf{u}_1 + \dots + \alpha_k \mathbf{u}_k$$

Jelikož je U podprostorem V , U splňuje (ii) a (iii) z Věty 6.

Jelikož $\mathbf{u}_1, \dots, \mathbf{u}_k \in U$, plyne z (iii) (z Věty 6), že $\alpha_1 \mathbf{u}_1, \dots, \alpha_k \mathbf{u}_k \in U$; nyní z (ii) (z Věty 6) plyne, že $\alpha_1 \mathbf{u}_1 + \dots + \alpha_k \mathbf{u}_k \in U$, tj. $\mathbf{v} \in U$.

Tedy $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k) \subseteq U$. ♦

Důkaz (pokračování).

Tvrzení. Pro každý podprostor U vektorového prostoru V , t.ž. $\mathbf{u}_1, \dots, \mathbf{u}_k \in U$, platí $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k) \subseteq U$.

Nyní dokažme (c).

- ☉ pro každý podprostor U vektorového prostoru V t.ž. $\mathbf{u}_1, \dots, \mathbf{u}_k \in U$, pak $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$ je podprostor U

Nechť U je libovolný podprostor vektorového prostoru V t.ž.

$\mathbf{u}_1, \dots, \mathbf{u}_k \in U$. Dle Tvrzení platí $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k) \subseteq U$, zatímco dle (a) je $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$ podprostorem V . Tedy jsou U a $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$ vektorové prostory, oba převzaly své operace (sčítání vektorů a násobení skalárem) z vektorového prostoru V , a zároveň platí, že $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k) \subseteq U$. Dle definice je tedy $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$ podprostorem U . Tím je dokázáno (c).

Důkaz (pokračování).

Tvrzení. Pro každý podprostor U vektorového prostoru V ,
t.ž. $\mathbf{u}_1, \dots, \mathbf{u}_k \in U$, platí $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k) \subseteq U$.

Zbývá dokázat (d).

- ⓓ $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$ je roven průniku všech podprostorů vektorového prostoru V , které obsahují vektory $\mathbf{u}_1, \dots, \mathbf{u}_k$

Nechť $\mathcal{W}$ je množina všech podprostorů vektorového prostoru V , které obsahují vektory $\mathbf{u}_1, \dots, \mathbf{u}_k$, a položme $W_0 := \bigcap_{W \in \mathcal{W}} W$. Je třeba dokázat, že $W_0 = \text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$.

Dle (a) a (b) je samotný $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$ podprostorem V , obsahujícím vektory $\mathbf{u}_1, \dots, \mathbf{u}_k$, tj. $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k) \in \mathcal{W}$. Tedy platí $W_0 = \bigcap_{W \in \mathcal{W}} W \subseteq \text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$.

Na druhou stranu, dle Tvrzení platí, že $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k) \subseteq W$ pro každé $W \in \mathcal{W}$, a tedy $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k) \subseteq \bigcap_{W \in \mathcal{W}} W = W_0$.

Tím jsme dokázali, že $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k) = W_0$, a tedy platí (d). $\square$

Věta 8

Nechť V je vektorový prostor nad tělesem $\mathbb{F}$ a necht' $\mathbf{u}_1, \dots, \mathbf{u}_k \in V$ ($k \geq 0$).^a Pak platí následující tvrzení:

- Ⓐ $\mathbf{u}_1, \dots, \mathbf{u}_k \in \text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$;
- Ⓑ $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$ je podprostorem V ;
- Ⓒ pro každý podprostor U vektorového prostoru V t.ž. $\mathbf{u}_1, \dots, \mathbf{u}_k \in U$, pak $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$ je podprostor U ;
- Ⓓ $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$ je roven průniku všech podprostorů vektorového prostoru V , které obsahují vektory $\mathbf{u}_1, \dots, \mathbf{u}_k$.

^aPokud $k = 0$, pak je množina $\{\mathbf{u}_1, \dots, \mathbf{u}_k\}$ prázdná, a platí $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k) = \{\mathbf{0}\}$.

Tvrzení 9

Nechť V je vektorový prostor nad tělesem $\mathbb{F}$. Nechť $\mathbf{v}_1, \dots, \mathbf{v}_k \in V$ a $\alpha_1, \dots, \alpha_k \in \mathbb{F} \setminus \{0\}$. Pak platí

$$\text{Span}(\mathbf{v}_1, \dots, \mathbf{v}_k) = \text{Span}(\alpha_1 \mathbf{v}_1, \dots, \alpha_k \mathbf{v}_k).$$

Důkaz. Je třeba dokázat následující dvě inkluze:

- ❶ $\text{Span}(\mathbf{v}_1, \dots, \mathbf{v}_k) \subseteq \text{Span}(\alpha_1 \mathbf{v}_1, \dots, \alpha_k \mathbf{v}_k)$;
- ❷ $\text{Span}(\alpha_1 \mathbf{v}_1, \dots, \alpha_k \mathbf{v}_k) \subseteq \text{Span}(\mathbf{v}_1, \dots, \mathbf{v}_k)$.

Dokážeme (i); důkaz (ii) je podobný a je ponechán jako cvičení. Nechť $\mathbf{v} \in \text{Span}(\mathbf{v}_1, \dots, \mathbf{v}_k)$. Pak dle definice existují skaláry $\beta_1, \dots, \beta_k \in \mathbb{F}$ t.ž.

$$\mathbf{v} = \beta_1 \mathbf{v}_1 + \dots + \beta_k \mathbf{v}_k.$$

Jelikož jsou skaláry $\alpha_1, \dots, \alpha_k$ nenulové, mají inverzní prvky $\alpha_1^{-1}, \dots, \alpha_k^{-1}$ respektive. Nyní platí

$$\mathbf{v} = \beta_1 \mathbf{v}_1 + \dots + \beta_k \mathbf{v}_k = (\beta_1 \alpha_1^{-1})(\alpha_1 \mathbf{v}_1) + \dots + (\beta_k \alpha_k^{-1})(\alpha_k \mathbf{v}_k),$$

a tedy $\mathbf{v} \in \text{Span}(\alpha_1 \mathbf{v}_1, \dots, \alpha_k \mathbf{v}_k)$. Tím jsme dokázali (i). $\square$

Tvrzení 9

Nechť V je vektorový prostor nad tělesem $\mathbb{F}$. Nechť $\mathbf{v}_1, \dots, \mathbf{v}_k \in V$ a $\alpha_1, \dots, \alpha_k \in \mathbb{F} \setminus \{0\}$. Pak platí

$$\text{Span}(\mathbf{v}_1, \dots, \mathbf{v}_k) = \text{Span}(\alpha_1 \mathbf{v}_1, \dots, \alpha_k \mathbf{v}_k).$$

- **Poznámka:** V Tvrzení 9 je důležité, že jsou skaláry $\alpha_1, \dots, \alpha_k$ nenulové. Bez této podmínky by tvrzení přestalo platit!
 - Např. pro kanonické jednotkové vektory $\mathbf{e}_1, \mathbf{e}_2$ z $\mathbb{R}^2$ platí $\text{Span}(\mathbf{e}_1, \mathbf{e}_2) = \mathbb{R}^2$, ale

$$\text{Span}(1\mathbf{e}_1, 0\mathbf{e}_2) = \left\{ \begin{bmatrix} x_1 \\ 0 \end{bmatrix} \mid x_1 \in \mathbb{R} \right\},$$

což je vlastní podprostor $\mathbb{R}^2$.

- Nyní zkusme sestavit nové vektorové prostory z těch, které už máme.
- Předpokládejme, že jsou dány vektorové prostory U a W nad tělesem $\mathbb{F}$.
- Pak lze **kartézský součin**

$$U \times W := \{(\mathbf{u}, \mathbf{w}) \mid \mathbf{u} \in U, \mathbf{w} \in W\}$$

přirozeným způsobem vybavit strukturou vektorového prostoru nad $\mathbb{F}$.

- Sčítání vektorů je definováno předpisem

$$(\mathbf{u}_1, \mathbf{w}_1) + (\mathbf{u}_2, \mathbf{w}_2) := (\mathbf{u}_1 + \mathbf{u}_2, \mathbf{w}_1 + \mathbf{w}_2),$$

pro všechny $\mathbf{u}_1, \mathbf{u}_2 \in U$ a $\mathbf{w}_1, \mathbf{w}_2 \in W$.

- Násobení skalárem v $U \times W$ (pro skaláry z $\mathbb{F}$) je definováno předpisem

$$\alpha(\mathbf{u}, \mathbf{w}) := (\alpha\mathbf{u}, \alpha\mathbf{w})$$

pro všechny $\alpha \in \mathbb{F}$, $\mathbf{u} \in U$ a $\mathbf{w} \in W$.

- Nulový vektor ve $U \times W$ je vektor

$$\mathbf{0}_{U \times W} := (\mathbf{0}_U, \mathbf{0}_W),$$

kde $\mathbf{0}_U$ a $\mathbf{0}_W$ jsou neutrální prvky pro sčítání v U a W respektive.

- Opačný vektor k vektoru $(\mathbf{u}, \mathbf{w})$ z $U \times W$ je vektor

$$(-\mathbf{u}, -\mathbf{w}),$$

kde $-\mathbf{u}$ (resp. $-\mathbf{w}$) je opačný prvek k $\mathbf{u}$ (resp. $\mathbf{w}$) ve vektorovém prostoru U (resp. W).

- Nyní lze jednoduše ověřit, že pro $U \times W$ platí všechny axiomy z definice vektorového prostoru.
 - Prostě využijeme toho, že axiomy platí pro U a W .

- Necht U a W jsou podprostory vektorového prostoru V nad tělesem $\mathbb{F}$.
- Pomocí Věty 6 lze jednoduše ověřit, že $U \cap W$ a

$$U + W := \{\mathbf{u} + \mathbf{w} \mid \mathbf{u} \in U, \mathbf{w} \in W\}$$

jsou podprostory vektorového prostoru V .

- Detaily ponecháváme jako cvičení.

Definice

Nechť V je vektorový prostor nad tělesem $\mathbb{F}$, a nechť $\mathbf{v}_1, \dots, \mathbf{v}_k \in V$ jsou vektory. Říkáme, že množina $\{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ je *lineárně nezávislá*, nebo že vektory $\mathbf{v}_1, \dots, \mathbf{v}_k$ jsou *lineárně nezávislé*, pokud pro všechny $\alpha_1, \dots, \alpha_k \in \mathbb{F}$ platí

$$\alpha_1 \mathbf{v}_1 + \dots + \alpha_k \mathbf{v}_k = \mathbf{0} \implies \alpha_1 = \dots = \alpha_k = 0.$$

Jinými slovy, vektory $\mathbf{v}_1, \dots, \mathbf{v}_k$ jsou lineárně nezávislé, pokud rovnice $\alpha_1 \mathbf{v}_1 + \dots + \alpha_k \mathbf{v}_k = \mathbf{0}$ má pouze „triviální řešení“, tj. řešení $\alpha_1 = \dots = \alpha_k = 0$. Na druhou stranu, pokud vektory $\mathbf{v}_1, \dots, \mathbf{v}_k$ nejsou lineárně nezávislé, pak říkáme, že jsou *lineárně závislé*, nebo že množina $\{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ je *lineárně závislá*.

- Jinými slovy, vektory $\mathbf{v}_1, \dots, \mathbf{v}_k$ jsou lineárně závislé právě tehdy, když existují skaláry $\alpha_1, \dots, \alpha_k \in \mathbb{F}$, **alespoň jeden nenulový**, t.ž. $\alpha_1 \mathbf{v}_1 + \dots + \alpha_k \mathbf{v}_k = \mathbf{0}$.
- **Poznámka:** $\emptyset$ je lineárně nezávislá množina ve **každém** vektorovém prostoru.

- Pro speciální případ vektorového prostoru $\mathbb{F}^n$ (kde $\mathbb{F}$ je těleso), máme následující tvrzení.

Tvrzení 10

Nechť $\mathbb{F}$ je těleso, a necht' $\mathbf{a}_1, \dots, \mathbf{a}_m$ ($m \geq 1$) jsou vektory v $\mathbb{F}^n$. Položme $A := [\mathbf{a}_1 \ \dots \ \mathbf{a}_m]$. Pak jsou následující tvrzení ekvivalentní:

- Ⓐ vektory $\mathbf{a}_1, \dots, \mathbf{a}_m$ jsou lineárně nezávislé;
- Ⓑ homogenní rovnice $A\mathbf{x} = \mathbf{0}$ má pouze triviální řešení (tj. řešení $\mathbf{x} = \mathbf{0}$);
- Ⓒ $\text{rank}(A) = m$ (tj. A má plnou sloupcovou hodnot).

Důkaz. Dle Důsledku 8 z Přednášky č.3 jsou (b) a (c) ekvivalentní.

Zbývá ukázat, že (a) a (b) jsou ekvivalentní. Máme následující posloupnost ekvivalentních tvrzení (následující slajd):

Důkaz (pokračování).

vektory $\mathbf{a}_1, \dots, \mathbf{a}_m$ jsou lineárně nezávislé

(a)

$\Leftrightarrow$

rovnice $x_1 \mathbf{a}_1 + \dots + x_m \mathbf{a}_m = \mathbf{0}$ má pouze triviální řešení (tj. řešení $x_1 = \dots = x_m = 0$)

$\Leftrightarrow$

rovnice $\underbrace{\begin{bmatrix} \mathbf{a}_1 & \dots & \mathbf{a}_m \end{bmatrix}}_{=A} \begin{bmatrix} x_1 \\ \vdots \\ x_m \end{bmatrix} = \mathbf{0}$ má pouze triviální řešení (tj. řešení $x_1 = \dots = x_m = 0$)

$\Leftrightarrow$

homogenní rovnice $A\mathbf{x} = \mathbf{0}$ má pouze triviální řešení (tj. řešení $\mathbf{x} = \mathbf{0}$).

(b)

Tím jsme dokázali, že (a) a (b) jsou ekvivalentní. $\square$

Tvrzení 10

Nechť $\mathbb{F}$ je těleso, a nechť $\mathbf{a}_1, \dots, \mathbf{a}_m$ ($m \geq 1$) jsou vektory v $\mathbb{F}^n$. Položme $A := [\mathbf{a}_1 \ \dots \ \mathbf{a}_m]$. Pak jsou následující tvrzení ekvivalentní:

- Ⓐ vektory $\mathbf{a}_1, \dots, \mathbf{a}_m$ jsou lineárně nezávislé;
- Ⓑ homogenní rovnice $A\mathbf{x} = \mathbf{0}$ má pouze triviální řešení (tj. řešení $\mathbf{x} = \mathbf{0}$);
- Ⓒ $\text{rank}(A) = m$ (tj. A má plnou sloupcovou hodnotu).

Tvrzení 11

Nechť V je vektorový prostor nad tělesem $\mathbb{F}$. Nechť $\mathbf{v}_1, \dots, \mathbf{v}_k \in V$ a nechť $\alpha_1, \dots, \alpha_k \in \mathbb{F} \setminus \{0\}$. Pak je množina $\{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ lineárně nezávislá právě tehdy, když je množina $\{\alpha_1\mathbf{v}_1, \dots, \alpha_k\mathbf{v}_k\}$ lineárně nezávislá.

Důkaz. Vyplývá z definice lineární nezávislosti (detaily: zkuste sami). $\square$

Definice

Konečná báze (nebo jenom *báze*) vektorového prostoru V nad tělesem $\mathbb{F}$ je množina $\{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ vektorů z V , která splňuje následující dvě podmínky:

- 1 množina $\{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ je lineárně nezávislá ve V ;
- 2 množina $\{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ generuje V , tj. $\text{Span}(\mathbf{v}_1, \dots, \mathbf{v}_k) = V$.

Příklad

Nechť $\mathbb{F}$ je těleso. Pak je kanonická báze $\mathcal{E}_n = \{\mathbf{e}_1^n, \dots, \mathbf{e}_n^n\}$ opravdu (tj. ve smyslu definice) bází $\mathbb{F}^n$.

Příklad

Nechť $\mathbb{F}$ je těleso. Pak je

$$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix} \right\}$$

bází $\mathbb{F}^{3 \times 2}$.

Definice

Konečná báze (nebo jenom *báze*) vektorového prostoru V nad tělesem $\mathbb{F}$ je množina $\{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ vektorů z V , která splňuje následující dvě podmínky:

- 1 množina $\{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ je lineárně nezávislá ve V ;
- 2 množina $\{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ generuje V , tj. $\text{Span}(\mathbf{v}_1, \dots, \mathbf{v}_k) = V$.

Definice

Vektorový prostor je *konečnědimenzionální* (nebo je *konečně generovaný*, nebo má *konečnou dimenzi*), má-li konečnou bázi. Vektorový prostor, který žádnou konečnou bázi nemá, je *nekonečnědimenzionální* (nebo je *nekonečně generovaný*, nebo má *nekonečnou dimenzi*).

- **Značení:** Nechť V je vektorový prostor nad tělesem $\mathbb{F}$.
 - Je-li V konečnědimenzionální, značíme to $\dim(V) < \infty$.
 - Je-li V nekonečnědimenzionální, značíme to $\dim(V) = \infty$.

Tvrzení 12

Nechť $\mathbb{F}$ je těleso. Pak je $\mathbb{P}_{\mathbb{F}}$ nekonečnědimenzionální. Na druhou stranu, pro každé celé číslo $n \geq 0$, $\{1, x, \dots, x^n\}$ je báze $\mathbb{P}_{\mathbb{F}}^n$, a tedy je $\mathbb{P}_{\mathbb{F}}^n$ konečnědimenzionální.

Důkaz (nástin). Je „zřejmé“ že $\{1, x, \dots, x^n\}$ je báze $\mathbb{P}_{\mathbb{F}}^n$ (pro každé celé číslo $n \geq 0$).

Zbývá dokázat, že $\mathbb{P}_{\mathbb{F}}$ je nekonečnědimenzionální. Stačí ukázat, že žádná konečná množina polynomů v $\mathbb{P}_{\mathbb{F}}$ negeneruje $\mathbb{P}_{\mathbb{F}}$ (a tedy $\mathbb{P}_{\mathbb{F}}$ nemá konečnou bázi).

Nechť $\mathcal{P} = \{p_1(x), \dots, p_k(x)\}$ je libovolná konečná množina polynomů v $\mathbb{P}_{\mathbb{F}}$. Pak existuje $d \in \mathbb{N}$ t.ž.

$\deg(p_1(x)), \dots, \deg(p_k(x)) \leq d$, a tedy $x^{d+1} \notin \text{Span}(\mathcal{P})$.

Plyne, že žádná konečná množina polynomů v $\mathbb{P}_{\mathbb{F}}$ negeneruje $\mathbb{P}_{\mathbb{F}}$, a tedy $\mathbb{P}_{\mathbb{F}}$ nemá konečnou bázi. $\square$

Tvrzení 12

Nechť $\mathbb{F}$ je těleso. Pak je $\mathbb{P}_{\mathbb{F}}$ nekonečnědimenzionální. Na druhou stranu, pro každé celé číslo $n \geq 0$, $\{1, x, \dots, x^n\}$ je báze $\mathbb{P}_{\mathbb{F}}^n$, a tedy je $\mathbb{P}_{\mathbb{F}}^n$ konečnědimenzionální.

- Dle Tvrzení 12 vskutku existují vektorové prostory, které nemají konečnou bázi (a tedy jsou nekonečnědimenzionální).
- Lze také definovat nekonečnou bázi, ale je to technicky náročnější a definici zde neuvádíme.
 - Pro stručnou diskusi viz skriptu (Penev, oddíl 3.2.7 - nepovinná četba).

- Pro speciální případ vektorového prostoru $\mathbb{F}^n$ (kde $\mathbb{F}$ je těleso), máme následující tvrzení.

Tvrzení 13

Nechť $\mathbb{F}$ je těleso a necht' $\mathbf{a}_1, \dots, \mathbf{a}_m$ ($m \geq 1$) jsou vektory z $\mathbb{F}^n$. Položme $A := [\mathbf{a}_1 \ \dots \ \mathbf{a}_m]$. Pak je $\{\mathbf{a}_1, \dots, \mathbf{a}_m\}$ báze $\mathbb{F}^n$ právě tehdy, když $\text{rank}(A) = n = m$ (tj. když A je čtvercová matice plné hodnosti). Zejména každá báze vektorového prostoru $\mathbb{F}^n$ obsahuje právě n vektorů.

Důkaz. Dle Tvrzení 10 jsou vektory $\mathbf{a}_1, \dots, \mathbf{a}_m$ **lineárně nezávislé** právě tehdy, když **$\text{rank}(A) = m$** .

Dle Tvrzení 7 vektory $\mathbf{a}_1, \dots, \mathbf{a}_m$ **generují $\mathbb{F}^n$** právě tehdy, když **$\text{rank}(A) = n$** .

Tedy je $\{\mathbf{a}_1, \dots, \mathbf{a}_m\}$ báze $\mathbb{F}^n$ právě tehdy, když $\text{rank}(A) = \mathbf{m} = \mathbf{n}$. $\square$

Tvrzení 13

Nechť $\mathbb{F}$ je těleso a nechť $\mathbf{a}_1, \dots, \mathbf{a}_m$ ($m \geq 1$) jsou vektory z $\mathbb{F}^n$. Položme $A := [\mathbf{a}_1 \ \dots \ \mathbf{a}_m]$. Pak je $\{\mathbf{a}_1, \dots, \mathbf{a}_m\}$ báze $\mathbb{F}^n$ právě tehdy, když $\text{rank}(A) = n = m$ (tj. když A je čtvercová matice plné hodnosti). Zejména každá báze vektorového prostoru $\mathbb{F}^n$ obsahuje právě n vektorů.

- **Poznámka:** Nechť $\mathbb{F}$ je těleso.
 - Dle Věty o regulárních maticích jsou čtvercové matice plné hodnosti právě regulární matice.
 - Tedy Tvrzení 13 dává další kritérium regularity: matice $v \in \mathbb{F}^{n \times n}$ je regulární právě tehdy, když její sloupce tvoří bázi vektorového prostoru $\mathbb{F}^n$.
 - Dle Tvrzení 13 každá báze $\mathbb{F}^n$ obsahuje právě n vektorů.
 - Později (příští týden) uvidíme, že je-li V **libovolný** konečnědimenzionální vektorový prostor, pak mají **všechny** báze prostoru V stejný počet vektorů.
 - Abychom to dokázali, musíme rozvinout další teorii!

- Připomenutí:

Tvrzení 9

Nechť V je vektorový prostor nad tělesem $\mathbb{F}$. Nechť $\mathbf{v}_1, \dots, \mathbf{v}_k \in V$ a $\alpha_1, \dots, \alpha_k \in \mathbb{F} \setminus \{0\}$. Pak platí

$$\text{Span}(\mathbf{v}_1, \dots, \mathbf{v}_k) = \text{Span}(\alpha_1 \mathbf{v}_1, \dots, \alpha_k \mathbf{v}_k).$$

Tvrzení 11

Nechť V je vektorový prostor nad tělesem $\mathbb{F}$. Nechť $\mathbf{v}_1, \dots, \mathbf{v}_k \in V$ a nechť $\alpha_1, \dots, \alpha_k \in \mathbb{F} \setminus \{0\}$. Pak je množina $\{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ lineárně nezávislá právě tehdy, když je množina $\{\alpha_1 \mathbf{v}_1, \dots, \alpha_k \mathbf{v}_k\}$ lineárně nezávislá.

Tvrzení 14

Nechť V je vektorový prostor nad tělesem $\mathbb{F}$. Nechť $\mathbf{v}_1, \dots, \mathbf{v}_k \in V$ a nechť $\alpha_1, \dots, \alpha_k \in \mathbb{F} \setminus \{0\}$. Pak je množina $\{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ bází V právě tehdy, když je množina $\{\alpha_1 \mathbf{v}_1, \dots, \alpha_k \mathbf{v}_k\}$ bází V .

Důkaz. Vynechán. (Zkuste sami!)

- Naše následující věta říká, že konečná množina vektorů je bází vektorového prostoru V právě tehdy, když **každý** vektor z V lze vyjádřit jako lineární kombinaci těchto vektorů **právě jedním** způsobem.

Věta 15

Nechť V je vektorový prostor nad tělesem $\mathbb{F}$, a nechť $\mathbf{v}_1, \dots, \mathbf{v}_n \in V$. Pak jsou následující tvrzení ekvivalentní:

- (i) $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ je bází V ;
- (ii) $\forall \mathbf{v} \in V \exists! \alpha_1, \dots, \alpha_n \in \mathbb{F}$ t.ž. $\mathbf{v} = \alpha_1 \mathbf{v}_1 + \dots + \alpha_n \mathbf{v}_n$.

Důkaz. Předpokládejme, že platí (i); je třeba ukázat, že platí (ii).
Nechť $\mathbf{v} \in V$. Musíme dokázat, že existují jediné skaláry $\alpha_1, \dots, \alpha_n \in \mathbb{F}$ t.ž. $\mathbf{v} = \alpha_1 \mathbf{v}_1 + \dots + \alpha_n \mathbf{v}_n$.

Jelikož je množina $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ bází V , a tedy generuje V , víme, že každý vektor z V lze vyjádřit jako lineární kombinaci vektorů $\mathbf{v}_1, \dots, \mathbf{v}_n$. Tím je dokázána existence.

Věta 15

Nechť V je vektorový prostor nad tělesem $\mathbb{F}$, a nechť $\mathbf{v}_1, \dots, \mathbf{v}_n \in V$. Pak jsou následující tvrzení ekvivalentní:

- (i) $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ je báze V ;
- (ii) $\forall \mathbf{v} \in V \exists! \alpha_1, \dots, \alpha_n \in \mathbb{F}$ t.ž. $\mathbf{v} = \alpha_1 \mathbf{v}_1 + \dots + \alpha_n \mathbf{v}_n$.

Důkaz (pokračování). Zbývá ukázat jedinečnost. Nechť $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in \mathbb{F}$ jsou skaláry t.ž.

$$\mathbf{v} = \alpha_1 \mathbf{v}_1 + \dots + \alpha_n \mathbf{v}_n \quad \text{a} \quad \mathbf{v} = \beta_1 \mathbf{v}_1 + \dots + \beta_n \mathbf{v}_n.$$

Tedy platí $\alpha_1 \mathbf{v}_1 + \dots + \alpha_n \mathbf{v}_n = \beta_1 \mathbf{v}_1 + \dots + \beta_n \mathbf{v}_n$, z čehož plyne, že

$$(\alpha_1 - \beta_1) \mathbf{v}_1 + \dots + (\alpha_n - \beta_n) \mathbf{v}_n = \mathbf{0}.$$

Jelikož je množina $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ lineárně nezávislá (protože je báze V), plyne, že $\alpha_1 - \beta_1 = \dots = \alpha_n - \beta_n = 0$. Tedy $\alpha_1 = \beta_1, \dots, \alpha_n = \beta_n$. Tím je dokázána jedinečnost, a tedy i (ii).

Věta 15

Nechť V je vektorový prostor nad tělesem $\mathbb{F}$, a nechť $\mathbf{v}_1, \dots, \mathbf{v}_n \in V$. Pak jsou následující tvrzení ekvivalentní:

- (i) $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ je báze V ;
- (ii) $\forall \mathbf{v} \in V \exists! \alpha_1, \dots, \alpha_n \in \mathbb{F}$ t.ž. $\mathbf{v} = \alpha_1 \mathbf{v}_1 + \dots + \alpha_n \mathbf{v}_n$.

Důkaz (pokračování). Předpokládejme nyní, že platí (ii); musíme ukázat, že platí (i).

Dle (ii) je každý vektor z V lineární kombinací vektorů $\mathbf{v}_1, \dots, \mathbf{v}_n$, a tedy množina $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ generuje V .

Zbývá ukázat, že množina $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ je lineárně nezávislá. Je zřejmé, že rovnice $\alpha_1 \mathbf{v}_1 + \dots + \alpha_n \mathbf{v}_n = \mathbf{0}$ má řešení, a to $\alpha_1 = \dots = \alpha_n = 0$; dle (ii) je toto řešení **jediné**, a tedy plyne, že množina $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ je lineárně nezávislá. Tím jsme dokázali (i). $\square$