Pavel Horák

LINEÁRNÍ ALGEBRA A GEOMETRIE I.

UČEBNÍ TEXT

Tento učební text je určen pro předmět Lineární algebra a geometrie I., který je povinným předmětem ve všech studijních oborech studijnho programu Aplikovaná matematika, včetně distanční formy studia, na přírodovědecké fakultě Masarykovy Univerzity v Brně. Jedná se o jednosemestrální kurz, který je doporučen absolvovat ve 2. semestru studia a který navazuje na předmět Základy matematiky.

Učební text předpokládá jednak elementární znalosti středoškolské matematiky a dále pak základní znalosti látky absolvované v předmětu Základy matematiky. Po formální stránce je výklad veden co nejpodrobněji, přičemž se vždy výslovně připomínají drobná úskalí a důležité maličkosti, které by méně zkušený čtenář mohl často přehlédnout. Z těchto důvodů má podrobné studium poznámek a komentářů přinejmenším stejný význam jako „učení se" definic a vět. Totéž platí i pro důkazy jednotlivých tvrzení, které jsou zde v převážné většině naprosto přirozené, průhledné a bez umělých obratů. Konec důkazu je v textu vždy opticky označen symbolem $\square$, umístěným na konci příslušného řádku.

Pro označování základních číselných množin jsou v textu použity následující standardní symboly:

$\mathbb{N}$ ... množina všech přirozených čísel, tzn. čísel $1, 2, 3, \ldots$
$\mathbb{Z}$ ... množina všech celých čísel
$\mathbb{Q}$ ... množina všech racionálních čísel
$\mathbb{R}$ ... množina všech reálných čísel
$\mathbb{C}$ ... množina všech komplexních čísel.

Obsah

Kapitola 1

Vektorové prostory

§1. Vektorový prostor nad číselným tělesem

Pojem vektoru a vektorového prostoru je jedním ze základních pojmů moderní matematiky, kterého se využívá nejenom v řadě disciplín ryzí matematiky, ale rovněž v mnoha aplikacích, ať už v přírodních vědách nebo jinde.

Při zavádění pojmu vektorového prostoru se oproti předchozí kapitole situace poněkud komplikuje v tom, že tentokrát vycházíme ze dvou algebraických struktur, a to z jisté komutativní grupy $(V, +)$, jejíž prvky budeme označovat tučnými písmeny, a dále z jistého číselného tělesa $(T, +, \cdot)$. Mezi těmito dvěma strukturami pak budou platit určité vazby. Pro zjednodušení vyjadřování si zaveďme následující úmluvu.

Úmluva. Při zapisování algebraických struktur už nebudeme vždy důsledně vypisovat symboly operací jako doposud, ale často budeme k označení celé struktury používat pouze symbol nosné množiny.

Tedy např. místo o grupě $(V, +)$ budeme stručně hovořit o grupě V, místo o tělese $(T, +, \cdot)$ budeme stručně hovořit o tělese T, atd. Přitom je však třeba mít stále na paměti, že se jedná o zjednodušené označení, protože, jak víme, algebraickou strukturu nelze ztotožňovat pouze s její nosnou množinou.

Definice. Nechť $(V, +)$ je komutativní grupa (jejíž prvky nazýváme vektory) a $(T, +, \cdot)$ je číselné těleso. Nechť pro každé číslo $t \in T$ a každý vektor $\boldsymbol{u} \in V$ je definován vektor $t \cdot \boldsymbol{u} \in V$ tak, že platí:

(1) $t \cdot (\boldsymbol{u} + \boldsymbol{v}) = t \cdot \boldsymbol{u} + t \cdot \boldsymbol{v}$,
(2) $(t + s) \cdot \boldsymbol{u} = t \cdot \boldsymbol{u} + s \cdot \boldsymbol{u}$,
(3) $(t \cdot s) \cdot \boldsymbol{u} = t \cdot (s \cdot \boldsymbol{u})$,
(4) $1 \cdot \boldsymbol{u} = \boldsymbol{u}$

pro lib. $t, s \in T$ a $\boldsymbol{u}, \boldsymbol{v} \in V$. Potom V se nazývá *vektorový prostor nad tělesem T*.

Označení. Nulový prvek z $(V, +)$ se nazývá *nulový vektor* a označuje se symbolem $\boldsymbol{o}$. Opačný prvek k vektoru $\boldsymbol{u} \in V$ se nazývá *opačný vektor k vektoru $\boldsymbol{u}$* a označuje se symbolem $-\boldsymbol{u}$. Vektor $t \cdot \boldsymbol{u}$ se nazývá *součin čísla t s vektorem $\boldsymbol{u}$*.

Poznámka. Výše definovaný součin čísla s vektorem je vlastně speciálním typem zobrazení, a sice zobrazením $T \times V \to V$, které se někdy nazývá vnější operace, na rozdíl od (binární) operace na množině, např. V, což je zobrazení $V \times V \to V$, které se pak nazývá vnitřní operace.

V definici vektorového prostoru se setkáváme se třemi vnitřními operacemi a jednou vnější operací, přičemž některé z nich označujeme stejnými symboly (sčítání ve V a sčítání v T symbolem $+$, resp. násobení v T a součin čísla s vektorem symbolem $\cdot$). I když nemůže dojít k nedorozumění (vzhledem k tomu, že vektory z V a čísla z T odlišujeme graficky), je třeba si tuto skutečnost dobře uvědomit.

Připomeňme, že máme-li korektně definovat nějaký konkrétní vektorový prostor, pak z předchozí definice plyne, že musíme:
(1) zadat číselné těleso T,
(2) zadat množinu vektorů V,
(3) zadat, jak je definováno sčítání vektorů,
(4) zadat, jak je definován součin čísla z T s vektorem z V,
(5) ověřit, že $(V, +)$ je komutativní grupa a že platí axiomy (1) – (4) z definice vektorového prostoru.

Příklad 1.1.
1. Nechť T je libovolné číselné těleso, n je pevné přirozené číslo a nechť:

$$T^n = \{(x_1, \dots, x_n) \mid x_1, \dots, x_n \in T\}$$

(tzn. T^n je množina všech uspořádaných n-tic prvků z tělesa T) je množina vektorů. Definujme pro lib. $\boldsymbol{u} = (u_1, \ldots, u_n)$, $\boldsymbol{v} = (v_1, \ldots, v_n) \in T^n$ a $t \in T$:

$$\boldsymbol{u} + \boldsymbol{v} = (u_1 + v_1, \ldots, u_n + v_n),$$
$$t \cdot \boldsymbol{u} = (t \cdot u_1, \ldots, t \cdot u_n),$$

kde symboly $+$, resp. $\cdot$ na pravých stranách značí obyčejné sčítání, resp. násobení čísel (stručně říkáme, že sčítání vektorů a násobení čísla s vektorem je definováno „po složkách"). Pak $(T^n, +)$ je komutativní grupa (viz příklad 1.7.4, kap. II) a lehce se ověří, že platí axiomy (1) – (4) z definice vektorového prostoru. Tedy T^n je vektorovým prostorem nad tělesem T.

Poznamenejme, že nulovým vektorem je v T^n zřejmě uspořádaná n-tice $(0, 0, \ldots, 0)$ a opačným vektorem k $(u_1, \ldots, u_n)$ je vektor $(-u_1, \ldots, -u_n)$.

Specielně, např. $\mathbb{R}^3$, $\mathbb{Q}^5$, $\mathbb{C}^2$, $\mathbb{Q}(\sqrt{2}\,)^4$, atd. jsou různé vektorové prostory tohoto typu.

2. Vezměme těleso $\mathbb{R}$ reálných čísel. Množinou vektorů bude množina všech polynomů o neurčité x s reálnými koeficienty, kterou označme $\mathbb{R}[x]$. Sčítání vektorů definujeme jako obvyklé sčítání polynomů a součin čísla s vektorem definujeme jako obvyklé násobení polynomu reálným číslem.

Lehce se ověří, že $(\mathbb{R}[x], +)$ je komutativní grupa a že platí axiomy (1) – (4). Tedy $\mathbb{R}[x]$ je vektorovým prostorem nad tělesem $\mathbb{R}$ (nulovým vektorem tohoto vektorového prostoru je pak zřejmě tzv. nulový polynom, tj. polynom, jehož všechny koeficienty jsou nulové).

3. Nechť n je pevné přirozené číslo. Vezměme opět těleso $\mathbb{R}$ reálných čísel a množinou vektorů nechť je množina sestávající z nulového polynomu a dále ze všech polynomů o neurčité x s reálnými koeficienty stupně $\leq n$, kterou označíme symbolem $\mathbb{R}_n[x]$. Tedy:

$$\mathbb{R}_n[x] = \{a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \mid a_0, a_1, \ldots, a_n \in \mathbb{R}\}.$$

Sčítání vektorů a součin čísla s vektorem definujeme stejně jako v předchozím příkladu.

Lehce se ověří, že $(\mathbb{R}_n[x], +)$ je komutativní grupa a že platí axiomy (1) – (4). Tedy $\mathbb{R}_n$ je vektorovým prostorem nad tělesem $\mathbb{R}$.

4. Nechť T je libovolné číselné těleso a $V = \{\boldsymbol{v}\}$ je libovolná jednoprvková množina. Sčítání vektorů a součin čísla s vektorem definujeme (jediným možným způsobem, a sice): $\boldsymbol{v} + \boldsymbol{v} = \boldsymbol{v}$, resp. $t \cdot \boldsymbol{v} = \boldsymbol{v}$ pro každé $t \in T$. Pak zřejmě $(V, +)$ je komutativní grupa a platí axiomy (1) – (4). Tedy V je vektorový prostor nad tělesem T, který budeme nazývat *nulový vektorový prostor* (nad T). Je to tedy vektorový prostor obsahující jediný vektor – a to nulový, tzn. $\boldsymbol{v} = \boldsymbol{o}$.

Poznámka. Uvědomme si, že množina vektorů V je vždy neprázdná, dále že nulový vektor ve V existuje jediný a opačný vektor k libovolnému vektoru z V existuje rovněž jediný (to vše plyne ihned z faktu, že $(V,+)$ je grupa). Přitom je potřeba důsledně rozlišovat symboly $\boldsymbol{o}$ a 0, tzn. nulový vektor a číslo nula.

Dále připomeňme, že podle dříve zavedené úmluvy budeme místo $\boldsymbol{u} + (-\boldsymbol{v})$ psát stručně $\boldsymbol{u} - \boldsymbol{v}$. Následující věta nám pak dá další pravidla pro počítání s vektory.

Věta 1.1. *Nechť V je vektorový prostor nad tělesem T, nechť $t, s, \in T$, $\boldsymbol{u}, \boldsymbol{v} \in V$ lib. Pak platí:*

(1) $t \cdot (\boldsymbol{u} - \boldsymbol{v}) = t \cdot \boldsymbol{u} - t \cdot \boldsymbol{v}$,

(2) $(t - s) \cdot \boldsymbol{u} = t \cdot \boldsymbol{u} - s \cdot \boldsymbol{u}$,

(3) $t \cdot \boldsymbol{u} = \boldsymbol{o} \iff t = 0$ *nebo* $\boldsymbol{u} = \boldsymbol{o}$,

(4) $t \cdot (-\boldsymbol{u}) = (-t) \cdot \boldsymbol{u} = -(t \cdot \boldsymbol{u})$.

Důkaz. Provedeme většinou užitím axiomů (1) – (4) vektorového prostoru.

(1): $t\cdot(\boldsymbol{u}-\boldsymbol{v}) = t\cdot\big(\boldsymbol{u}+(-\boldsymbol{v})\big)+t\cdot\boldsymbol{v}-t\cdot\boldsymbol{v} = t\cdot\big(\boldsymbol{u}+(-\boldsymbol{v})+\boldsymbol{v}\big)-t\cdot\boldsymbol{v} = t\cdot\boldsymbol{u}-t\cdot\boldsymbol{v}$.

(2): $(t-s)\cdot\boldsymbol{u} = \big(t+(-s)\big)\cdot\boldsymbol{u}+s\cdot\boldsymbol{u}-s\cdot\boldsymbol{u} = \big(t+(-s)+s\big)\cdot\boldsymbol{u}-s\cdot\boldsymbol{u} = t\cdot\boldsymbol{u}-s\cdot\boldsymbol{u}$.

(3): „$\Leftarrow$“: Je-li $t = 0$, pak $0 \cdot \boldsymbol{u} = (0 - 0) \cdot \boldsymbol{u} = 0 \cdot \boldsymbol{u} - 0 \cdot \boldsymbol{u} = \boldsymbol{o}$ podle (2). Je-li $\boldsymbol{u} = \boldsymbol{o}$, pak $t \cdot \boldsymbol{o} = t \cdot (\boldsymbol{o} - \boldsymbol{o}) = t \cdot \boldsymbol{o} - t \cdot \boldsymbol{o} = \boldsymbol{o}$ podle (1).

„$\Rightarrow$“: Nechť $t \cdot \boldsymbol{u} = \boldsymbol{o}$ a $t \neq 0$. Potom $\boldsymbol{u} = 1 \cdot \boldsymbol{u} = \big(\frac{1}{t} \cdot t\big) \cdot \boldsymbol{u} = \frac{1}{t} \cdot (t \cdot \boldsymbol{u}) = \frac{1}{t} \cdot \boldsymbol{o} = \boldsymbol{o}$.

(4): Plyne z (1), (2) a (3), a sice: $t \cdot (-\boldsymbol{u}) = t \cdot (\boldsymbol{o} - \boldsymbol{u}) = t \cdot \boldsymbol{o} - t \cdot \boldsymbol{u} = \boldsymbol{o} - t \cdot \boldsymbol{u} = -t \cdot \boldsymbol{u}$, resp. $(-t) \cdot \boldsymbol{u} = (0 - t) \cdot \boldsymbol{u} = 0 \cdot \boldsymbol{u} - t \cdot \boldsymbol{u} = -t \cdot \boldsymbol{u}$. □

Poznámka. Pomocí předchozí věty můžeme upřesnit naši představu o počtu vektorů ve vektorovém prostoru. Je-li totiž V libovolný vektorový prostor nad T různý od nulového prostoru (jinými slovy řečeno – V obsahuje alespoň jeden nenulový vektor), pak musí prostor V obsahovat nekonečně mnoho vektorů. Vezmeme-li totiž libovolný vektor $\boldsymbol{u} \in V$, $\boldsymbol{u} \neq \boldsymbol{o}$ a tvoříme součiny všech prvků z číselného tělesa T (kterých je nekonečně mnoho) s tímto vektorem $\boldsymbol{u}$, dostáváme nekonečně mnoho navzájem různých vektorů (je-li totiž $t_1 \cdot \boldsymbol{u} = t_2 \cdot \boldsymbol{u}$, pro $t_1, t_2 \in T$, pak $(t_1 - t_2) \cdot \boldsymbol{u} = \boldsymbol{o}$, odkud podle věty 1.1. (3) je $(t_1 - t_2) = 0$, neboli $t_1 = t_2$).

§2. Podprostory vektorového prostoru

Definice. Nechť V je vektorový prostor nad tělesem T. Neprázdná podmnožina W množiny V se nazývá *podprostor vektorového prostoru* V, jestliže platí:

(1) $\boldsymbol{u}, \boldsymbol{v} \in W$ libololné $\implies \boldsymbol{u} + \boldsymbol{v} \in W$,

(2) $t \in T$, $\boldsymbol{u} \in W$ libovolné $\implies t \cdot \boldsymbol{u} \in W$.

Poznámka. 1. Lehce se dá ověřit (proveďte si podrobně sami!), že podmínky (1) a (2) z předchozí definice jsou ekvivalentní následující jediné podmínce:

(3) $\boldsymbol{u}, \boldsymbol{v} \in W$, $t, s \in T$ libovolné $\implies t \cdot \boldsymbol{u} + s \cdot \boldsymbol{v} \in W$.

2. Každý podprostor W vektorového prostoru V musí vždycky obsahovat nulový vektor (je-li $\boldsymbol{u} \in W$ libovolný, pak podle (2) a podle věty 1.1. (3) je $0 \cdot \boldsymbol{u} = \boldsymbol{o} \in W$). Vidíme tedy, že se např. nemůže stát, aby dva podprostory vektorového prostoru V byly disjunktní.

Věta 2.1. *Nechť W je podprostor vektorového prostoru V nad tělesem T. Pak W je sám vektorovým prostorem nad tělesem T.*

Důkaz. Součet dvou vektorů z W, resp. součin čísla z T s vektorem z W jsou definovány stejně jako ve V. Definice podprostoru nám zaručuje, že jde o vnitřní, resp. vnější operaci na W.

Dále nechť $\boldsymbol{u}, \boldsymbol{v} \in W$ libovolné. Pak $(-1) \cdot \boldsymbol{v} = -\boldsymbol{v} \in W$, a tedy $\boldsymbol{u} - \boldsymbol{v} = \boldsymbol{u} + (-\boldsymbol{v}) \in W$ (podle věty 1.1. (4) a definice podprostoru). Podle V.2.3., kap. II je pak $(W, +)$ podgrupou komutativní grupy $(V, +)$, tzn. $(W, +)$ je komutativní grupou.

Axiomy (1) – (4) z definice vektorového prostoru jsou ve W zřejmě splněny (poněvadž jsou splněny v celém V).

Tedy W je vektorový prostor nad tělesem T. $\square$

Příklad 2.1.

1. Nechť V je libovolný vektorový prostor nad tělesem T. Pak zřejmě $W = \{\boldsymbol{o}\}$ a $W = V$ jsou vždy podprostory ve V. Tyto dva podprostory se nazývají *triviální podprostory* ve V. Všechny ostatní podprostory ve V (pokud existují) se pak nazývají *netriviální podprostory* ve V.

2. Uvažme vektorový prostor $\mathbb{R}^3$ (viz příklad 1.1. 1.). Potom např.:

(a) $W_1 = \{(x, y, 0) \mid x, y \in \mathbb{R} \text{ lib.}\}$ je podprostor vektorového prostoru $\mathbb{R}^3$.

(b) $W_2 = \{(x, y, z) \mid x, y, z \in \mathbb{R} \wedge x - 2y + 3z = 0\}$ je podprostor v $\mathbb{R}^3$.

(c) Nechť (u, v, w) je pevný vektor prostoru $\mathbb{R}^3$. Potom $W_3 = \{k \cdot (u, v, w) \mid k \in \mathbb{R}\}$ je podprostor v $\mathbb{R}^3$.

Je vidět, že vektorový prostor $\mathbb{R}^3$ obsahuje nekonečně mnoho podprostorů. Na druhé straně samozřejmě ne každá podmnožina v $\mathbb{R}^3$ je podprostorem $\mathbb{R}^3$. Např. $W_4 = \{(x, y, 1) \mid x, y \in \mathbb{R}\}$ není podprostorem v $\mathbb{R}^3$ (zdůvodněte proč!).

3. Uvažme vektorový prostor $\mathbb{R}[x]$ všech polynomů (viz příklad 1.1. 2.). Pak např.:

(a) $W_1 = \{f(x) \in \mathbb{R}[x] \mid f(x) = f(-x)\}$ je podprostor v $\mathbb{R}[x]$.

(b) $W_2 = \{f(x) \in \mathbb{R}[x] \mid 2 \cdot f(0) + 3 \cdot f(1) = 0\}$ je podprostorem v $\mathbb{R}[x]$.

(c) Vektorový prostor $\mathbb{R}_n[x]$ (viz příklad 1.1. 3.) je podprostorem v $\mathbb{R}[x]$.

Na druhé straně např. množina $W_3 = \{x^2 + ax + b \mid a, b \in \mathbb{R} \text{ lib.}\}$ není podprostorem v $\mathbb{R}[x]$.

Věta 2.2. *Nechť V je vektorový prostor nad tělesem T, nechť I je neprázdná indexová množina a nechť pro každé $\alpha \in I$ je W_α podprostor ve V. Potom $\bigcap_{\alpha \in I} W_\alpha$ je podprostor ve V.*

Důkaz. Množina $\bigcap_{\alpha \in I} W_\alpha$ je zřejmě neprázdná (neboť obsahuje jistě nulový vektor $\boldsymbol{o}$). Zbývá tedy ověřit platnost podmínek (1) a (2) z definice podprostoru. Nechť $\boldsymbol{u}, \boldsymbol{v} \in \bigcap_{\alpha \in I} W_\alpha$, $t \in T$ libovolné. Potom $\boldsymbol{u}, \boldsymbol{v} \in W_\alpha$ pro každé $\alpha \in I$, a tedy (poněvadž W_α je podprostor) je $\boldsymbol{u} + \boldsymbol{v} \in W_\alpha$ a $t \cdot \boldsymbol{u} \in W_\alpha$ pro každé $\alpha \in I$. Pak ale $\boldsymbol{u} + \boldsymbol{v} \in \bigcap_{\alpha \in I} W_\alpha$ a $t \cdot \boldsymbol{u} \in \bigcap_{\alpha \in I} W_\alpha$. □

Poznamenejme, že indexová množina I byla libovolná (neprázdná), a tedy předchozí věta platí jak pro konečný, tak pro nekonečný počet podprostorů. Stručně řečeno, věta tvrdí, že průnikem libovolného počtu podprostorů ve V je opět podprostor ve V. Tohoto faktu využijeme v následující důležité úvaze.

Nechť M je libovolná podmnožina vektorového prostoru V (tzn. M obecně není podprostorem!). Pak existuje alespoň jeden podprostor obsahující množinu M (např. celý prostor V má tuto vlastnost). Můžeme tedy utvořit průnik všech podprostorů ve V obsahujících množinu M, který označme symbolem $[M]$. Tedy:

$$[M] = \bigcap W_\alpha \tag{1}$$

(W_α je podprostor ve V takový, že $W_\alpha \supseteq M$) a platí následující tvrzení.

Věta 2.3. *Nechť M je libovolná podmnožina ve vektorovém prostoru V. Potom:*

(1) *$[M]$ je podprostor ve V,*

(2) *$[M]$ je nejmenší (vzhledem k $\subseteq$) podprostor ve V obsahující množinu M.*

Důkaz. (1): Plyne ihned z věty 2.2.

(2): Plyne z (1) a ze základních vlastností množinového průniku. □

Je-li množina M konečná, např. $M = \{\boldsymbol{u}_1, \dots, \boldsymbol{u}_k\}$, pak místo symbolu $[\{\boldsymbol{u}_1, \dots, \boldsymbol{u}_k\}]$ budeme psát stručněji $[\boldsymbol{u}_1, \dots, \boldsymbol{u}_k]$. V tomto případě je tedy:

$$[\boldsymbol{u}_1, \dots, \boldsymbol{u}_k] = \bigcap W_\alpha$$

(W_α je podprostor ve V takový, že $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k \in W_\alpha$). Může se samozřejmě též stát, že množina M je prázdná. V takovém případě zřejmě je $[\emptyset] = \{\boldsymbol{o}\}$.

Definice. Nechť M je podmnožina ve vektorovém prostoru V a nechť $W = [M]$. Pak podprostor W se nazývá *podprostor generovaný množinou M.*

Je-li specielně $M = \{\boldsymbol{u}_1, \dots, \boldsymbol{u}_k\}$, pak W se nazývá *podprostor generovaný vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$* a vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ se nazývají *generátory podprostoru W.*

Uvědomme si, že na rozdíl od průniku podprostorů není množinové sjednocení podprostorů (dokonce ani dvou) obecně podprostorem daného vektorového prostoru. Například pro podprostory W_1 a W_2 vektorového prostoru $\mathbb{R}^3$ z příkladu 2.1. 2. jejich sjednocení $W_1 \cup W_2$ není podprostorem v $\mathbb{R}^3$ (neboť např. $(1,1,0), (1,2,1) \in W_1 \cup W_2$, ale $(1,1,0) + (1,2,1) = (2,3,1) \notin W_1 \cup W_2$). V dalším si nyní zavedeme pojem tzv. součtu podprostorů, ukážeme, že je podprostorem a jaký má vztah k množinovému sjednocení těchto podprostorů.

Definice. Nechť W_1, W_2, ..., W_k ($k \geq 2$) jsou podprostory vektorového prostoru V. Pak množina $W_1 + W_2 + \cdots + W_k$ definovaná:

$$W_1 + W_2 + \cdots + W_k = \{\boldsymbol{u}_1 + \boldsymbol{u}_2 + \cdots + \boldsymbol{u}_k \mid \boldsymbol{u}_1 \in W_1,\ \boldsymbol{u}_2 \in W_2,\ \dots,\ \boldsymbol{u}_k \in W_k\}$$

se nazývá *součet podprostorů* $W_1, \ldots, W_k$.

Věta 2.4. *Nechť $W_1, W_2, \ldots, W_k$ $(K \geq 2)$ jsou podprostory ve V. Pak platí:*

(1) *součet podprostorů $W_1 + W_2 + \cdots + W_k$ je podprostorem ve V,*
(2) *$W_1 + W_2 + \cdots + W_k = [W_1 \cup W_2 \cup \cdots \cup W_k]$, tzn. součet podprostorů $W_1, \ldots, W_k$ je roven podprostoru generovanému jejich množinovým sjednocením.*

Důkaz. (1): Zřejmě je $W_1 + \cdots + W_k \neq \emptyset$ (neboť $W_i \neq \emptyset$). Dále nechť $\boldsymbol{u}, \boldsymbol{v} \in W_1 + \cdots + W_k$, $t \in T$ libovolné. Potom $\boldsymbol{u} = \boldsymbol{u}_1 + \cdots + \boldsymbol{u}_k$, $\boldsymbol{v} = \boldsymbol{v}_1 + \cdots + \boldsymbol{v}_k$, kde $\boldsymbol{u}_i, \boldsymbol{v}_i \in W_i$, $i = 1, \ldots, k$. Potom ale:

$$\boldsymbol{u} + \boldsymbol{v} = (\boldsymbol{u}_1 + \cdots + \boldsymbol{u}_k) + (\boldsymbol{v}_1 + \cdots + \boldsymbol{v}_k) = (\boldsymbol{u}_1 + \boldsymbol{v}_1) + \cdots + (\boldsymbol{u}_k + \boldsymbol{v}_k) \in W_1 + \cdots + W_k,$$
$$t \cdot \boldsymbol{u} = t \cdot (\boldsymbol{u}_1 + \cdots + \boldsymbol{u}_k) = t \cdot \boldsymbol{u}_1 + \cdots + t \cdot \boldsymbol{u}_k \in W_1 + \cdots + W_k,$$

a tedy $W_1 + \cdots + W_k$ je podprostor ve V.

(2): Vzhledem k (1) budeme dokazovat množinovou rovnost:

$$W_1 + \cdots + W_k = \bigcap U_\alpha$$

(U_α je podprostor ve V takový, že $U_\alpha \supseteq W_1 \cup \cdots \cup W_k$).

„$\subseteq$“: Nechť $\boldsymbol{u} \in W_1 + \cdots + W_k$. Potom $\boldsymbol{u} = \boldsymbol{u}_1 + \cdots + \boldsymbol{u}_k$, kde $\boldsymbol{u}_i \in W_i$. Je tedy $\boldsymbol{u}_i \in U_\alpha$, kde U_α je libovolný podprostor ve V takový, že $U_\alpha \supseteq W_1 \cup \cdots \cup W_k$. Potom však $\boldsymbol{u}_1 + \cdots + \boldsymbol{u}_k = \boldsymbol{u} \in U_\alpha$, a tedy $\boldsymbol{u} \in \bigcap U_\alpha$ (U_α je podprostor ve V a $U_\alpha \supseteq W_1 \cup \cdots \cup W_k$).

„$\supseteq$“: Zřejmě je $W_i \subseteq W_1 + \cdots + W_k$ (neboť pro $\boldsymbol{u}_i \in W_i$ libovolný je $\boldsymbol{u}_i = \boldsymbol{o} + \cdots + \boldsymbol{u}_i + \cdots + \boldsymbol{o} \in W_1 + \cdots + W_k$), a tedy $W_1 \cup \cdots \cup W_k \subseteq W_1 + \cdots + W_k$. Podle 1. části věty je však $W_1 + \cdots + W_k$ podprostorem ve V, tzn. z vlastností množinového průniku pak již plyne žádaná množinová inkluze. $\square$

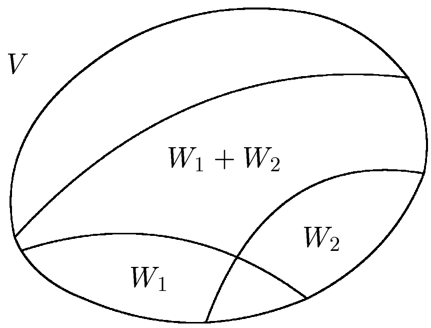
Vidíme tedy, že součet podprostorů $W_1 + \cdots + W_k$ je nejmenším podprostorem ve V obsahujícím množinové sjednocení $W_1 \cup \cdots \cup W_k$ těchto podprostorů. Samozřejmě, že součet podprostorů obecně není roven jejich množinovému sjednocení. Dále si uvědomme, že vyjádření vektoru $\boldsymbol{u} \in W_1 + \cdots + W_k$ ve tvaru:

$$\boldsymbol{u} = \boldsymbol{u}_1 + \cdots + \boldsymbol{u}_k,$$

kde $\boldsymbol{u}_1 \in W_1, \ldots, \boldsymbol{u}_k \in W_k$, nemusí být jednoznačné. Obojí se ukáže na jednoduchém příkladu, a to pro $k = 2$, což je situace, s níž se budeme v praxi nejčastěji setkávat. V tomto případě je tedy:

$$W_1 + W_2 = \{\boldsymbol{u}_1 + \boldsymbol{u}_2 \mid \boldsymbol{u}_1 \in W_1,\ \boldsymbol{u}_2 \in W_2\} = [W_1 \cup W_2].$$

Schematicky je tato situace znázorněna na obr. 8.



obr. 8.

Příklad 2.2. Ve vektorovém prostoru $\mathbb{R}^3$ mějme dány dva podprostory:

$$W_1 = \{(x, y, 0) \mid x, y \in \mathbb{R}\},$$
$$W_2 = \{(u, 0, v) \mid u, v \in \mathbb{R}\}.$$

Zřejmě platí, že:

$$W_1 \cup W_2 = \{(a, b, c) \mid a, b, c \in \mathbb{R},\ b = 0 \text{ nebo } c = 0\},$$

resp.

$$W_1 + W_2 = \mathbb{R}^3.$$

Vidíme tedy, že $W_1 \cup W_2 \subsetneqq W_1 + W_2$.

Dále, vyjádření vektoru $\boldsymbol{u} \in W_1 + W_2$ ve tvaru:

$$\boldsymbol{u} = \boldsymbol{u}_1 + \boldsymbol{u}_2, \tag{2}$$

kde $\boldsymbol{u}_1 \in W_1$, $\boldsymbol{u}_2 \in W_2$, zde obecně není jednoznačné, neboť např. $(0,0,0) \in W_1 + W_2$, přičemž třeba $(0,0,0) = (0,0,0) + (0,0,0) = (1,0,0) + (-1,0,0)$ jsou dvě různá vyjádření tvaru (2). Poznamenejme, že v tomto případě má každý vektor z $W_1 + W_2$ dokonce nekonečně mnoho různých vyjádření tvaru (2).

Definice. Nechť W_1, W_2, …, W_k ($k \geq 2$) jsou podprostory vektorového prostoru V. Součet podprostorů $W_1, \ldots, W_k$ se nazývá *přímý součet* a označuje $W_1 \dot{+} W_2 \dot{+} \cdots \dot{+} W_k$, jestliže libovolný vektor $\boldsymbol{u} \in W_1 + \cdots + W_k$ lze vyjádřit jediným způsobem ve tvaru:

$$\boldsymbol{u} = \boldsymbol{u}_1 + \cdots + \boldsymbol{u}_k, \tag{3}$$

kde $\boldsymbol{u}_1 \in W_1$, …, $\boldsymbol{u}_k \in W_k$.

Věta 2.5. *Nechť W_1, W_2, …, W_k ($k \geq 2$) jsou podprostory vektorového prostoru V. Pak součet podprostorů $W_1, \ldots, W_k$ je přímým součtem $\iff$ pro každé $i = 1, 2, \ldots, k$ platí:*

$$W_i \cap (W_1 + \cdots + W_{i-1} + W_{i+1} + \cdots + W_k) = \{\boldsymbol{o}\}. \tag{4}$$

Důkaz. „$\Rightarrow$“: Nechť součet podprostorů W_1, …, W_k je přímý a nechť pro $1 \leq i \leq k$ je $\boldsymbol{x} \in W_i \cap (W_1 + \cdots + W_{i-1} + W_{i+1} + \cdots + W_k)$ libovolný. Potom je $\boldsymbol{x} = \boldsymbol{u}_1 + \cdots + \boldsymbol{u}_{i-1} + \boldsymbol{u}_{i+1} + \cdots + \boldsymbol{u}_k$, kde $\boldsymbol{u}_j \in W_j$, a dále $\boldsymbol{x} \in W_i$, tzn. také $-\boldsymbol{x} \in W_i$. Pak ale:

$$\boldsymbol{o} = \boldsymbol{u}_1 + \cdots + \boldsymbol{u}_{i-1} + (-\boldsymbol{x}) + \boldsymbol{u}_{i+1} + \cdots + \boldsymbol{u}_k,$$

resp.

$$\boldsymbol{o} = \boldsymbol{o} + \boldsymbol{o} + \cdots + \boldsymbol{o}$$

jsou dvě vyjádření nulového vektoru $\boldsymbol{o}$ ve tvaru (3), tzn. podle předpokladu musí být $\boldsymbol{x} = \boldsymbol{o}$. Tedy je $W_i \cap (W_1 + \cdots + W_{i-1} + W_{i+1} + \cdots + W_k) \subseteq \{\boldsymbol{o}\}$. Opačná inkluze je však triviální, tzn. dohromady platí rovnost. Poněvadž i bylo libovolné (s vlastností $1 \leq i \leq k$), platí všechny podmínky (4).

„$\Leftarrow$“: Nechť platí podmínky (4), nechť $\boldsymbol{x} \in W_1 + \cdots + W_k$ libovolný a nechť:

$$\boldsymbol{x} = \boldsymbol{u}_1 + \cdots + \boldsymbol{u}_k = \boldsymbol{u}'_1 + \cdots + \boldsymbol{u}'_k,$$

kde $\boldsymbol{u}_i, \boldsymbol{u}'_i \in W_i$, $i = 1, 2, \ldots, k$ jsou dvě vyjádření vektoru $\boldsymbol{x}$ ve tvaru (3). Potom pro libovolné $i = 1, 2, \ldots, k$ dostáváme:

$$(\boldsymbol{u}_i - \boldsymbol{u}'_i) = (\boldsymbol{u}'_1 - \boldsymbol{u}_1) + \cdots + (\boldsymbol{u}'_{i-1} - \boldsymbol{u}_{i-1}) + (\boldsymbol{u}'_{i+1} - \boldsymbol{u}_{i+1}) + \cdots + (\boldsymbol{u}'_k - \boldsymbol{u}_k),$$

tzn.:

$$(\boldsymbol{u}_i - \boldsymbol{u}'_i) \in W_i \cap (W_1 + \cdots + W_{i-1} + W_{i+1} + \cdots + W_k),$$

odkud však podle (4) plyne, že $(\boldsymbol{u}_i - \boldsymbol{u}'_i) = \boldsymbol{o}$, neboli $\boldsymbol{u}_i = \boldsymbol{u}'_i$. Tedy vyjádření vektoru $\boldsymbol{x}$ ve tvaru (3) je jednoznačné a součet podprostorů $W_1, \dots, W_k$ je přímý. $\square$

Poznámka. Rozepíšeme-li si předchozí větu pro některá konkrétní k, pak dostáváme např.:

pro $k = 2$: *součet podprostorů* W_1, W_2 *je přímým součtem* $\iff W_1 \cap W_2 = \{\boldsymbol{o}\}$,

pro $k = 3$: *součet podprostorů* W_1, W_2, W_3 *je přímým součtem* $\iff W_1 \cap (W_2 + W_3) = \{\boldsymbol{o}\} \wedge W_2 \cap (W_1 + W_3) = \{\boldsymbol{o}\} \wedge W_3 \cap (W_1 + W_2) = \{\boldsymbol{o}\}$.

Příklad 2.3. Ve vektorovém prostoru $\mathbb{R}^3$ mějme dány podprostory:

$$\begin{aligned} W_1 &= \{(x, x, 0) \mid x \in \mathbb{R}\}, \\ W_2 &= \{(u, 0, v) \mid u, v \in \mathbb{R}\}, \\ W_3 &= \{(0, k, k) \mid k \in \mathbb{R}\}. \end{aligned}$$

Potom užitím věty 2.5. dostáváme, že:

1. součet podprostorů W_1, W_2 je přímý (je-li $\boldsymbol{w} \in W_1 \cap W_2$, pak $\boldsymbol{w} = (x, x, 0) = (u, 0, v) \implies x = 0$, tzn. $\boldsymbol{w} = (0, 0, 0)$ a podle věty 2.5. je součet přímý),

2. součet podprostorů W_1, W_3 je přímý,

3. součet podprostorů W_2, W_3 je přímý,

4. součet podprostorů W_1, W_2, W_3 není přímý (neboť např. $W_1 \cap (W_2 + W_3) = W_1 \cap \mathbb{R}^3 = W_1 \neq \{\boldsymbol{o}\}$, a tedy podle věty 2.5. součet není přímý).

§3. Lineární závislost a nezávislost vektorů

Definice. Nechť V je vektorový prostor nad T a nechť $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ je konečná posloupnost vektorů z V. Pak vektor:

$$\boldsymbol{u} = t_1 \cdot \boldsymbol{u}_1 + \dots + t_k \cdot \boldsymbol{u}_k,$$

kde $t_1, \dots, t_k \in T$, se nazývá lineární kombinace konečné posloupnosti vektorů $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ nebo stručně *lineární kombinace vektorů* $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$.

Množina všech lineárních kombinací vektorů $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ se bude označovat symbolem $L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k)$, tzn.:

$$L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k) = \{t_1 \cdot \boldsymbol{u}_1 + \dots + t_k \cdot \boldsymbol{u}_k \mid t_1, \dots, t_k \in T \text{ libovolné}\}.$$

Poznámka. 1. Všimněme si, že v předchozí definici hovoříme o „konečné posloupnosti vektorů $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$“. Tímto obratem chceme říct, že je možné, aby se zde některý z vektorů vyskytoval případně vícekrát (tzn. může se stát, že $\boldsymbol{u}_i = \boldsymbol{u}_j$ pro $i \neq j$) a dále, že vektory chápeme v uvedeném pořadí (tento fakt však bude hrát důležitou roli až v dalším paragrafu). Z důvodů stručnosti budeme však v dalším místo „konečná posloupnost vektorů $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$“ říkat obvykle pouze „vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$“.

2. Symbol $L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k)$ znamená množinu všech (možných) lineárních kombinací vektorů $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$, kterých je zřejmě obecně nekonečně mnoho. Uvědomme si dále, že množina $L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k)$ obsahuje vždy mimo jiné:
- každý z vektorů $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ (neboť $\boldsymbol{u}_i = 0 \cdot \boldsymbol{u}_1 + \dots + 0 \cdot \boldsymbol{u}_{i-1} + 1 \cdot \boldsymbol{u}_i + 0 \cdot \boldsymbol{u}_{i+1} + \dots + 0 \cdot \boldsymbol{u}_k$),
- nulový vektor (neboť $\boldsymbol{o} = 0 \cdot \boldsymbol{u}_1 + \dots + 0 \cdot \boldsymbol{u}_k$).

3. V předchozím paragrafu jsme hovořili o podprostoru generovaném konečnou množinou vektorů. Je zřejmě, že místo „konečné množiny vektorů“ můžeme vzít též „konečnou posloupnost vektorů“ (případné opakující se vektory zde nehrají žádnou roli) a použít stejnou symboliku. Je-li tedy $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ konečná posloupnost vektorů z V, pak:

$$[\boldsymbol{u}_1, \dots, \boldsymbol{u}_k] = \bigcap W_\alpha \tag{1}$$

(W_α je podprostor ve V takový, že $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k \in W_\alpha$) je *podprostor generovaný vektory* $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$. Následující věta nám pak ukáže, že $[\boldsymbol{u}_1, \dots, \boldsymbol{u}_k]$ a $L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k)$ jsou vlastně jedno a totéž.

Věta 3.1. *Nechť V je vektorový prostor nad T a nechť $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ je konečná posloupnost vektorů z V. Pak platí:*
(1) *$L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k)$ je podprostor ve V,*
(2) *$[\boldsymbol{u}_1, \dots, \boldsymbol{u}_k] = L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k)$, tzn. podprostor generovaný vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ je roven množině všech lineárních kombinací vektorů $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$.*

Důkaz. (1): Zřejmé (ověřením definice podprostoru).

(2): Vzhledem k (1) budeme dokazovat množinovou rovnost:

$$\bigcap W_\alpha = L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k) \tag{2}$$

(W_α je podprostor ve V $\wedge$ $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k \in W_\alpha$).

„$\subseteq$“: Plyne z vlastností množinového průniku, uvědomíme-li si, že

$L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k)$ je podprostor ve V (podle 1. části) a že $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k \in L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k)$.

„$\supseteq$“: Množina na levé straně (2) je podprostor ve V obsahující vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$, tzn. musí pak obsahovat také jejich libovolnou lineární kombinaci. □

Důsledek. *Nechť V je vektorový prostor nad T, nechť $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ je konečná posloupnost vektorů z V a nechť $\boldsymbol{v}_1, \dots, \boldsymbol{v}_s \in L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k)$. Pak platí:*
(1) *$L(\boldsymbol{v}_1, \dots, \boldsymbol{v}_s) \subseteq L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k)$ (neboli $[\boldsymbol{v}_1, \dots, \boldsymbol{v}_s] \subseteq [\boldsymbol{u}_1, \dots, \boldsymbol{u}_k]$),*
(2) *$[\boldsymbol{u}_1, \dots, \boldsymbol{u}_k, \boldsymbol{v}_1, \dots, \boldsymbol{v}_s] = [\boldsymbol{u}_1, \dots, \boldsymbol{u}_k]$.*

Důkaz. (1): Plyne ihned z (1) a z předchozí věty, část (2).
(2): Inkluze „$\supseteq$“ plyne z (1). Dokažme inkluzi „$\subseteq$“. Ale triviálně je $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k \in L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k)$, resp. podle předpokladu je $\boldsymbol{v}_1, \dots, \boldsymbol{v}_s \in L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k)$. Podle části (1) je pak $[\boldsymbol{u}_1, \dots, \boldsymbol{u}_k, \boldsymbol{v}_1, \dots, \boldsymbol{v}_s] \subseteq [\boldsymbol{u}_1, \dots, \boldsymbol{u}_k]$. Dohromady pak platí dokazovaná rovnost. □

Vidíme tedy, že přidáme-li ke generátorům daného podprostoru W libovolný vektor, který je jejich lineární kombinací, dostáváme opět generátory W, resp. (totéž – jinak řečeno) odstraníme-li z generátorů podprostoru W vektor, který je lineární kombinací zbývajících, dostáváme opět generátory W.

Příklad 3.1.
1. Rozepsáním se lehce ověří, že např.:

$$\mathbb{R}^2 = [(1,0),(0,1)] = [(1,1),(1,2)] = [(0,2),(1,1),(0,1)] = \\ [(1,3),(2,1),(1,-1),(-2,3)], \text{ atd.}$$

Vidíme tedy, že vektorový prostor $\mathbb{R}^2$ je možno generovat dvěma a více vektory (zřejmě i nekonečně mnoha). Na druhé straně, prostor $\mathbb{R}^2$ evidentně nelze generovat jedním vektorem (neboť $[(a,b)] = L((a,b)) = \{(k \cdot a, k \cdot b) \mid k \in \mathbb{R}\} \subsetneqq \mathbb{R}^2$).
2. Ve vektorovém prostoru T^n označme vektory:

$$\begin{aligned} \boldsymbol{e}_1 &= (1,0,0,\dots,0,0), \\ \boldsymbol{e}_2 &= (0,1,0,\dots,0,0), \\ &\vdots \\ \boldsymbol{e}_n &= (0,0,0,\dots,0,1). \end{aligned}$$

Pak platí, že $T^n = [\boldsymbol{e}_1, \dots, \boldsymbol{e}_n]$, tzn. vektory $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ jsou generátory vektorového prostoru T^n (zřejmě pro libovolný vektor $\boldsymbol{u} = (u_1, \dots, u_n) \in$

T^n je $\boldsymbol{u} = u_1 \cdot \boldsymbol{e}_1 + \cdots + u_n \cdot \boldsymbol{e}_n$, tzn. $T^n \subseteq [\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n]$ a opačná inkluze je triviální).

3. Ve vektorovém prostoru $\mathbb{R}_n[x]$ označme vektory (tj. polynomy):

$$\begin{aligned} \boldsymbol{f}_1 &= 1, \\ \boldsymbol{f}_2 &= x, \\ \boldsymbol{f}_3 &= x^2, \\ &\vdots \\ \boldsymbol{f}_{n+1} &= x^n. \end{aligned}$$

Pak zřejmě $\mathbb{R}_n[x] = [\boldsymbol{f}_1, \ldots, \boldsymbol{f}_{n+1}]$, tzn. polynomy $1, x, x^2, \ldots, x^n$ jsou generátory vektorového prostoru $\mathbb{R}_n[x]$.

Definice. Nechť V je vektorový prostor nad T a nechť:

$$\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k \tag{3}$$

je konečná posloupnost vektorů z V. Jestliže existují čísla $t_1, \ldots, t_k \in T$, z nichž alespoň jedno je různé od nuly, tak, že:

$$t_1 \cdot \boldsymbol{u}_1 + \cdots + t_k \cdot \boldsymbol{u}_k = \boldsymbol{o}, \tag{4}$$

pak říkáme, že *vektory* $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ *jsou lineárně závislé.*

V opačném případě říkáme, že *vektory* $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ *jsou lineárně nezávislé.*

Poznámka. Vidíme, že pojem lineární nezávislosti je negací pojmu lineární závislosti. Explicitně vyjádřeno to znamená:

> *Vektory* $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ *jsou lineárně nezávislé, jestliže pro všechna* $t_1, \ldots, t_k \in T$, *z nichž alespoň jedno je různé od nuly, platí:* $t_1 \cdot \boldsymbol{u}_1 + \cdots + t_k \cdot \boldsymbol{u}_k \neq \boldsymbol{o}$.

S touto definicí by se však zřejmě nešikovně pracovalo, a proto ji přeformulujeme do ekvivalentního, ale praktičtějšího tvaru:

> *Vektory* $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ *jsou lineárně nezávislé, jestliže platí:*
> $t_1 \cdot \boldsymbol{u}_1 + \cdots + t_k \cdot \boldsymbol{u}_k = \boldsymbol{o} \implies t_1 = t_2 = \cdots = t_k = 0.$

Praktické zjišťování závislosti či nezávislosti daných vektorů (3) provádíme obvykle tak, že hledáme všechna čísla $t_1, \ldots, t_k \in T$ splňující rovnost (4). Zjistíme-li, že (4) je splněno pouze pro $t_1 = \cdots = t_k = 0$, pak jsou vektory (3) lineárně nezávislé. Je-li rovnost (4) splněna i pro nějaké $t_i \neq 0$, pak jsou dané vektory lineárně závislé.

Příklad 3.2.
1. Ve vektorovém prostoru $\mathbb{R}^2$ jsou např. vektory $(1,0)$, $(0,1)$ lineárně nezávislé. Podobně vektory $(1,1)$, $(1,2)$ jsou též lineárně nezávislé (obojí dostaneme rozepsáním podle předchozího návodu).

Na druhé straně např. vektory $(0,2)$, $(1,1)$, $(0,1)$ jsou lineárně závislé a podobně vektory $(1,3)$, $(2,1)$, $(1,-1)$, $(-2,3)$ jsou též lineárně závislé (ověřte si sami!).

2. Ve vektorovém prostoru T^n jsou vektory $\boldsymbol{e}_1 = (1,0,\dots,0)$, $\boldsymbol{e}_2 = (0,1,0,\dots,0)$, $\dots$, $\boldsymbol{e}_n = (0,\dots,0,1)$ lineárně nezávislé (neboť je-li $t_1 \cdot \boldsymbol{e}_1 + \dots + t_n \cdot \boldsymbol{e}_n = (0,\dots,0)$, pak $(t_1,\dots,t_n) = (0,\dots,0)$, a tedy $t_1 = t_2 = \dots = t_n = 0$).

3. Ve vektorovém prostoru $\mathbb{R}_n[x]$ jsou vektory (polynomy) $\boldsymbol{f}_1 = 1$, $\boldsymbol{f}_2 = x, \dots, \boldsymbol{f}_{n+1} = x^n$ lineárně nezávislé (je-li $t_1 \cdot 1 + t_2 \cdot x + \dots + t_{n+1} \cdot x^n = o$, kde o značí nulový polynom, tj. polynom, jehož všechny koeficienty jsou rovny nule, potom je $t_1 = t_2 = \dots = t_n = 0$, neboť dva polynomy se rovnají, právě když se rovnají jejich koeficienty u stejných mocnin x).

Jestliže uvažovaná posloupnost vektorů obsahuje pouze jediný vektor, např. $\boldsymbol{u}$, pak je zjišťování lineární závislosti či nezávislosti velmi jednoduché, neboť z předchozí definice a z věty 1.1. (3) plyne (rozmyslete si podrobně jak!), že platí:

$$\textit{vektor } \boldsymbol{u} \textit{ je lineárně závislý} \iff \boldsymbol{u} = \boldsymbol{o}. \tag{5}$$

O trošku složitější je situace, když uvažovaná posloupnost (3) obsahuje alespoň dva vektory. Kriteria lineární závislosti nám pro tento případ udává následující věta.

Věta 3.2. *Nechť V je vektorový prostor nad T, nechť $k \geq 2$ a $\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_k \in V$. Pak následující výroky jsou ekvivalentní:*
(1) *vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ jsou lineárně závislé,*
(2) *$\exists i$ $(1 \leq i \leq k)$ tak, že vektor $\boldsymbol{u}_i$ je lineární kombinací zbývajících vektorů (tj. vektorů $\boldsymbol{u}_1, \dots, \boldsymbol{u}_{i-1}, \boldsymbol{u}_{i+1}, \dots, \boldsymbol{u}_k$),*
(3) *$\exists i$ $(1 \leq i \leq k)$ tak, že $[\boldsymbol{u}_1, \dots, \boldsymbol{u}_k] = [\boldsymbol{u}_1, \dots, \boldsymbol{u}_{i-1}, \boldsymbol{u}_{i+1}, \dots, \boldsymbol{u}_k]$.*

Důkaz. „(1) $\Rightarrow$ (2)“: Nechť $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ jsou lineárně závislé. Pak existují čísla $t_1, \dots, t_k \in T$, z nichž alespoň jedno je nenulové, tak, že $t_1 \cdot \boldsymbol{u}_1 + \dots + t_k \cdot \boldsymbol{u}_k = \boldsymbol{o}$. Nechť např. $t_i \neq 0$. Pak ale úpravou z předchozí rovnice dostáváme:

$$\boldsymbol{u}_i = -\tfrac{t_1}{t_i} \cdot \boldsymbol{u}_1 - \cdots - \tfrac{t_{i-1}}{t_i} \cdot \boldsymbol{u}_{i-1} - \tfrac{t_{i+1}}{t_i} \cdot \boldsymbol{u}_{i+1} - \cdots - \tfrac{t_k}{t_i} \cdot \boldsymbol{u}_k,$$

což znamená, že vektor $\boldsymbol{u}_i$ je lineární kombinací zbývajících vektorů.

„(2) $\Rightarrow$ (3)“: Plyne přímo z 2. části důsledku věty 3.1.

„(3) $\Rightarrow$ (1)“: Nechť platí (3). Pak ale $\boldsymbol{u}_i \in [\boldsymbol{u}_1, \dots, \boldsymbol{u}_k] = [\boldsymbol{u}_1, \dots, \boldsymbol{u}_{i-1}, \boldsymbol{u}_{i+1}, \dots, \boldsymbol{u}_k] = L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_{i-1}, \boldsymbol{u}_{i+1}, \dots, \boldsymbol{u}_k)$, tzn. $\boldsymbol{u}_i = p_1 \cdot \boldsymbol{u}_1 + \cdots + p_{i-1} \cdot \boldsymbol{u}_{i-1} + p_{i+1} \cdot \boldsymbol{u}_{i+1} + \cdots + p_k \cdot \boldsymbol{u}_k$, kde $p_j \in T$. Pak po úpravě dostáváme:

$$p_1 \cdot \boldsymbol{u}_1 + \cdots + p_{i-1} \cdot \boldsymbol{u}_{i-1} + (-1) \cdot \boldsymbol{u}_i + p_{i+1} \cdot \boldsymbol{u}_{i+1} + \cdots + p_k \cdot \boldsymbol{u}_k = \boldsymbol{o},$$

odkud již plyne, že vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ jsou lineárně závislé. □

Poznámka. Je třeba si uvědomit, že část (2) předchozí věty nám zajišťuje pouze existenci vektoru, který lze vyjádřit jako lineární kombinaci zbývajících vektorů. Nelze tedy obecně tvrdit, že každý z lineárně závislých vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_k$ se dá vyjádřit jako lineární kombinace zbývajících vektorů. Např. ve vektorovém prostoru $\mathbb{R}^2$ jsou vektory:

$$\boldsymbol{u}_1 = (0, 1), \quad \boldsymbol{u}_2 = (1, 1), \quad \boldsymbol{u}_3 = (0, -2)$$

lineárně závislé (neboť $2 \cdot \boldsymbol{u}_1 + 0 \cdot \boldsymbol{u}_2 + 1 \cdot \boldsymbol{u}_3 = \boldsymbol{o}$), ale přitom je zřejmé, že vektor $\boldsymbol{u}_2$ nelze vyjádřit jako lineární kombinaci vektorů $\boldsymbol{u}_1, \boldsymbol{u}_3$.

Důsledek. *Nechť V je vektorový prostor nad T a nechť* (3) *je konečná posloupnost vektorů z V. Pak platí:*

(1) *obsahuje-li posloupnost* (3) *nulový vektor, pak je lineárně závislá,*
(2) *obsahuje-li posloupnost* (3) *dva stejné vektory, pak je lineárně závislá,*
(3) *je-li nějaká posloupnost vybraná ze* (3) *lineárně závislá, pak je i* (3) *lineárně závislá,*
(4) *je-li* (3) *lineárně nezávislá, pak každá posloupnost vybraná ze* (3) *je lineárně nezávislá.*

Důkaz. Všechna tvrzení důsledku plynou přímo z definice lineární závislosti, resp. z předchozí věty. □

Na závěr paragrafu uvedeme nyní větu, která patří k nejdůležitějším větám celé teorie vektorových prostorů.

Věta 3.3. (Steinitzova věta o výměně) *Nechť V je vektorový prostor nad T, $\boldsymbol{u}_1, \dots, \boldsymbol{u}_r, \boldsymbol{v}_1, \dots, \boldsymbol{v}_s \in V$. Nechť vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_r$ jsou lineárně nezávislé a nechť $\boldsymbol{u}_i \in L(\boldsymbol{v}_1, \dots, \boldsymbol{v}_s)$ pro $i = 1, \dots, r$. Potom platí:*

(1) $r \leq s$,
(2) *při vhodném přečíslování vektorů* $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s$ *je:*

$$L(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s) = L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r, \boldsymbol{v}_{r+1}, \ldots, \boldsymbol{v}_s).$$

Důkaz. Provedeme matematickou indukcí vzhledem k r.

α) Nechť $r = 1$. Pak je jistě $r \leq s$. Z předpokladů věty dále plyne, že $\boldsymbol{u}_1 \neq \boldsymbol{o}$ (podle (5)) a je $\boldsymbol{u}_1 = t_1 \cdot \boldsymbol{v}_1 + \cdots + t_s \cdot \boldsymbol{v}_s$. Pak ale alespoň jedno z čísel $t_1, \ldots, t_s$ musí být nenulové. Přečíslujeme vektory $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s$ tak, aby $t_1 \neq 0$. Potom:

$$\boldsymbol{v}_1 = \tfrac{1}{t_1} \cdot \boldsymbol{u}_1 - \tfrac{t_2}{t_1} \cdot \boldsymbol{v}_2 - \cdots - \tfrac{t_s}{t_1} \cdot \boldsymbol{v}_s,$$

tzn. $\boldsymbol{v}_1 \in L(\boldsymbol{u}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_s)$. Triviálně je $\boldsymbol{v}_2, \ldots, \boldsymbol{v}_s \in L(\boldsymbol{u}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_s)$, a tedy podle důsledku věty 3.1. je $L(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s) \subseteq L(\boldsymbol{u}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_s)$. Opačnou inkluzi dostaneme stejným způsobem (užitím předpokladu $\boldsymbol{u}_1 \in L(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s)$), a tedy platí žádaná rovnost $L(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_s) = L(\boldsymbol{u}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_s)$.

β) Přepokládáme, že tvrzení věty platí pro $1, 2, \ldots, r-1$ ($r \geq 2$), a dokážeme jej pro r.

Podle předpokladu a předchozího důsledku jsou vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{r-1}$ lineárně nezávislé, tzn. (podle indukčního předpokladu) $r - 1 \leq s$ a po vhodném přečíslování je:

$$L(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s) = L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{r-1}, \boldsymbol{v}_r, \ldots, \boldsymbol{v}_s). \tag{6}$$

Ale podle předpokladu věty je $\boldsymbol{u}_r \in L(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s) = L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{r-1}, \boldsymbol{v}_r, \ldots, \boldsymbol{v}_s)$, odkud především plyne, že $r - 1 < s$ (jinak spor s lineární nezávislostí vektorů $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r$), tzn. platí $r \leq s$.

Dále lze psát:

$$\boldsymbol{u}_r = t_1 \cdot \boldsymbol{u}_1 + \cdots + t_{r-1} \cdot \boldsymbol{u}_{r-1} + t_r \cdot \boldsymbol{v}_r + \cdots + t_s \cdot \boldsymbol{v}_s, \tag{7}$$

přičemž alespoň jedno z čísel $t_1, \ldots, t_s$ musí být nenulové (jinak opět spor s lineární nezávislostí vektorů $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r$). Přečíslujme je tak, aby $t_r \neq 0$. Potom:

$$\boldsymbol{v}_r = -\frac{t_1}{t_r} \cdot \boldsymbol{u}_1 - \cdots - \frac{t_{r-1}}{t_r} \cdot \boldsymbol{u}_{r-1} + \frac{1}{t_r} \cdot \boldsymbol{u}_r - \frac{t_{r+1}}{t_r} \cdot \boldsymbol{v}_{r+1} - \cdots - \frac{t_s}{t_r} \cdot \boldsymbol{v}_s. \tag{8}$$

Podle důsledku věty 3.1. (užitím (7) a (8)) dostáváme, že $L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{r-1}, \boldsymbol{v}_r, \ldots, \boldsymbol{v}_s) = L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r, \boldsymbol{v}_{r+1}, \ldots, \boldsymbol{v}_s)$. Odsud a z (6) pak plyne, že $L(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s) = L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r, \boldsymbol{v}_{r+1}, \ldots, \boldsymbol{v}_s)$, což je žádaná rovnost. □

§4. Báze a dimenze vektorového prostoru

Definice. Nechť V je vektorový prostor nad T. Konečná posloupnost vektorů $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ z V se nazývá *báze vektorového prostoru* V, jestliže platí:
(1) vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ jsou lineárně nezávislé,
(2) vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ generují vektorový prostor V, tzn. $[\boldsymbol{u}_1, \dots, \boldsymbol{u}_n] = V$.

Poznámka. Místo obratu „konečná posloupnost vektorů $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ je bází V“ budeme častěji říkat stručně „vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ jsou bází V“.

Dále si uvědomme, že předchozí definice nezaručuje existenci báze ani nic neříká o počtu bází ve V. Celou situaci si nejprve ilustrujeme na několika příkladech.

Příklad 4.1. Z příkladů 3.1. a 3.2. bezprostředně plyne, že:

1. Vektory $(1,0)$, $(0,1)$ jsou bází vektorového prostoru $\mathbb{R}^2$. Podobně vektory $(1,1)$, $(1,2)$ jsou též bází $\mathbb{R}^2$. Zřejmě vektorový prostor $\mathbb{R}^2$ má nekonečně mnoho různých bází. Na druhé straně, např. vektory $(0,2)$, $(1,1)$, $(0,1)$, resp. $(1,3)$, $(2,1)$, $(1,-1)$, $(-2,3)$, resp. $(1,2)$, $(2,4)$, resp. $(1,2)$ nejsou bází $\mathbb{R}^2$.

2. Vektory $\boldsymbol{e}_1 = (1,0,\dots,0)$, $\dots$, $\boldsymbol{e}_n = (0,\dots,0,1)$ jsou bází vektorového prostoru T^n.

3. Vektory (polynomy) $\boldsymbol{f}_1 = 1$, $\boldsymbol{f}_2 = x$, $\dots$, $\boldsymbol{f}_{n+1} = x^n$ jsou bází vektorového prostoru $\mathbb{R}_n[x]$.

Příklad 4.2.

1. Nulový vektorový prostor $V = \{\boldsymbol{o}\}$ nemá bázi, neboť libovolná konečná posloupnost vektorů z V má tvar $\boldsymbol{o}, \boldsymbol{o}, \dots, \boldsymbol{o}$, a je tedy lineárně závislá.

2. Vektorový prostor $\mathbb{R}[x]$ nemá bázi, neboť žádná konečná posloupnost vektorů (polynomů) z $\mathbb{R}[x]$ negeneruje celý prostor $\mathbb{R}[x]$. Je-li totiž $\boldsymbol{g}_1, \dots, \boldsymbol{g}_n$ libovolná konečná posloupnost polynomů z $\mathbb{R}[x]$ a jestliže polynom $\boldsymbol{g}_i$ má stupeň k_i, potom jistě existuje přirozené číslo t s vlastností: $t > k_i$ pro každé $i = 1, \dots, n$. Pak ale např. polynom $\boldsymbol{g} = x^t$ se nedá napsat jako lineární kombinace polynomů $\boldsymbol{g}_1, \dots, \boldsymbol{g}_n$, a je tedy $[\boldsymbol{g}_1, \dots, \boldsymbol{g}_n] \subsetneqq \mathbb{R}[x]$.

Rozebereme-li si předchozí definici podrobněji, pak vidíme, že báze $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ vektorového prostoru V je z hlediska generátorů „nejchudobnější“ posloupností vektorů. Přesněji řečeno, pokud bychom některý z vektorů $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$

vypustili, pak zbývající vektory už nebudou generovat vektorový prostor V (plyne z věty 3.2. – rozmyslete si podrobně jak). Na druhé straně, z hlediska lineární nezávislosti je báze „nejbohatší" posloupností vektorů z V, jak v dalším ukážeme.

Definice. Řekneme, že konečná posloupnost vektorů $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ z V je *maximální lineárně nezávislá posloupnost vektorů* ve V, jestliže:
(1) vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ jsou lineárně nezávislé,
(2) pro libovolné $\boldsymbol{w} \in V$ jsou vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n, \boldsymbol{w}$ lineárně závislé.

Věta 4.1. *Konečná posloupnost vektorů $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ je bází vektorového prostoru V, právě když je maximální lineárně nezávislou posloupností vektorů ve V.*

Důkaz. „$\Rightarrow$": Nechť $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ je báze ve V. Pak vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ jsou lineárně nezávislé a pro libovolný vektor $\boldsymbol{w} \in V$ je $\boldsymbol{w} \in [\boldsymbol{u}_1, \dots, \boldsymbol{u}_n] = L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$. Podle věty 3.2. jsou pak vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n, \boldsymbol{w}$ lineárně závislé, a tedy $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ je maximální lineárně nezávislá posloupnost vektorů.

„$\Leftarrow$": Nechť $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ je maximální lineárně nezávislá posloupnost vektorů ve V. Pak $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ jsou lineárně nezávislé. Dokážeme, že $[\boldsymbol{u}_1, \dots, \boldsymbol{u}_n] = V$, neboli $L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n) = V$. Ale inkluze „$\subseteq$" je triviální. Naopak, nechť $\boldsymbol{w} \in V$ libovolné. Pak podle předpokladu jsou vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n, \boldsymbol{w}$ lineárně závislé, tzn. existují čísla $t_1, \dots, t_n, t \in T$, z nichž alespoň jedno je různé od nuly, tak, že:

$$t_1 \cdot \boldsymbol{u}_1 + \dots + t_n \cdot \boldsymbol{u}_n + t \cdot \boldsymbol{w} = \boldsymbol{o}.$$

Musí však být $t \neq 0$ (jinak spor s lineární nezávislostí vektorů $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$), a tedy:

$$\boldsymbol{w} = -\tfrac{t_1,}{t} \cdot \boldsymbol{u}_1 - \dots - \tfrac{t_n}{t} \cdot \boldsymbol{u}_n \in L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n),$$

což jsme chtěli ukázat. $\square$

Následující věta nám pak podá ještě jednu charakterizaci báze vektorového prostoru.

Věta 4.2. *Konečná posloupnost vektorů $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ je bází vektorového prostoru V, právě když každý vektor $\boldsymbol{w} \in V$ je možno jediným způsobem vyjádřit ve tvaru:*

$$\boldsymbol{w} = t_1 \cdot \boldsymbol{u}_1 + \dots + t_n \cdot \boldsymbol{u}_n, \tag{1}$$

kde $t_1, \ldots, t_n \in T$.

Důkaz. „$\Rightarrow$“: Nechť $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ je báze ve V. Pak existence vyjádření (1) plyne z definice báze. Dokážeme jeho jednoznačnost. Nechť tedy:

$$\boldsymbol{w} = t_1 \cdot \boldsymbol{u}_1 + \cdots + t_n \cdot \boldsymbol{u}_n = r_1 \cdot \boldsymbol{u}_1 + \cdots + r_n \cdot \boldsymbol{u}_n,$$

kde $t_i, r_i \in T$. Pak odečtením a úpravou dostáváme:

$$(t_1 - r_1) \cdot \boldsymbol{u}_1 + \cdots + (t_n - r_n) \cdot \boldsymbol{u}_n = \boldsymbol{o}.$$

Vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ jsou však lineárně nezávislé, tzn. musí být $(t_i - r_i) = 0$, neboli $t_i = r_i$ pro každé $i = 1, \ldots, n$.

„$\Leftarrow$“: Nechť každý vektor $\boldsymbol{w} \in V$ se dá jednoznačně vyjádřit ve tvaru (1). Potom je $V = L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n) = [\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n]$. Zbývá ukázat, že vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ jsou lineárně nezávislé. Nechť tedy:

$$t_1 \cdot \boldsymbol{u}_1 + \cdots + t_n \cdot \boldsymbol{u}_n = \boldsymbol{o}.$$

Zřejmě však je $0 \cdot \boldsymbol{u}_1 + \cdots + 0 \cdot \boldsymbol{u}_n = \boldsymbol{o}$, a tedy z jednoznačnosti vyjádření (1) plyne, že $t_1 = \cdots = t_n = 0$, tzn. $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ jsou lineárně nezávislé. Dohromady pak dostáváme, že vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ jsou bází V. □

Věta 4.3. *Nechť* $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ *je báze vektorového prostoru* V. *Pak platí:*

(1) *jestliže* $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m$ *je báze prostoru* V, *pak je* $m = n$,

(2) *jestliže vektory* $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_s$ *generují prostor* V, *pak z nich lze vybrat bázi,*

(3) *každou konečnou posloupnost lineárně nezávislých vektorů z* V *lze doplnit na bázi* V.

Důkaz. (1): Aplikujeme-li dvakrát Steinitzovu větu, dostáváme $n \leq m$ a $m \leq n$, odkud plyne, že $m = n$.

(2): Podle předpokladu má prostor V bázi, tzn. musí být $V \neq \{\boldsymbol{o}\}$. Nechť vektory $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_s$ generují prostor V. Pak alespoň jeden z nich je různý od nulového vektoru a zřejmě je lze přečíslovat tak, že $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_i$ jsou lineárně nezávislé a $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_i, \boldsymbol{w}_j$ jsou lineárně závislé pro každé j s vlastností $i < j \leq n$. Odtud (podobnou úvahou jako v závěru důkazu věty 4.1.) plyne, že $\boldsymbol{w}_j \in L(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_i)$, a tedy $V = L(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_s) \subseteq L(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_i)$. Opačná inkluze je však triviální, tzn. je $V = L(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_i)$ a vektory $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_i$ jsou bází prostoru V.

(3): Nechť $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_r$ jsou lineárně nezávislé vektory z V. Podle Steinitzovy věty je (po vhodném přečíslování) $V = L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n) = L(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_r, \boldsymbol{u}_{r+1}, \ldots, \boldsymbol{u}_n)$, odkud podle právě dokázaných částí (1) a (2) dostáváme, že $\boldsymbol{w}_1, \dots, \boldsymbol{w}_r, \boldsymbol{u}_{r+1}, \dots, \boldsymbol{u}_n$ je báze V. □

První část předchozí věty nám říká, že má-li vektorový prostor nějakou bázi, pak všechny jeho báze sestávají vždy ze stejného počtu vektorů. Na základě tohoto faktu můžeme vyslovit následující definici.

Definice. Nechť V je vektorový prostor nad T. Pak:

(1) je-li V nulovým vektorovým prostorem (tzn. $V = \{\boldsymbol{o}\}$), říkáme, že *dimenze* V je nula,

(2) existuje-li báze $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ prostoru V, pak říkáme, že dimenze V je n,

(3) je-li $V \neq \{\boldsymbol{o}\}$ a nemá-li žádnou bázi, pak říkáme, že dimenze V je nekonečno.

Píšeme: $\dim V = 0$, resp. $\dim V = n$, resp. $\dim V = \infty$.

Vektorové prostory z (1) a (2) se nazývají *konečnědimenzionální*, vektorové prostory z (3) se nazývají *nekonečnědimenzionální*.

Příklad 4.3. Z příkladů 4.1. a 4.2. bezprostředně plyne, že:

1. $\dim \mathbb{R}^2 = 2$,

2. $\dim T^n = n$ (tzn. specielně např. $\dim \mathbb{R}^3 = 3$, $\dim \mathbb{Q}^5 = 5$, $\dim \mathbb{C}^4 = 4$, atd.),

3. $\dim \mathbb{R}_n[x] = n + 1$ (tzn. specielně např. $\dim \mathbb{R}_5[x] = 6$, atd.),

4. $\dim \mathbb{R}[x] = \infty$.

Úmluva. *Všude v dalším se budeme zabývat pouze konečnědimenzionálními vektorovými prostory.*

Řekneme-li tedy, že V je vektorový prostor nad T, bude to automaticky znamenat, že V je konečnědimenzionální, tzn. buď nulový prostor, nebo vektorový prostor, v němž existuje báze. K tomu ještě poznamenejme, že každý podprostor konečnědimenzionálního vektorového prostoru je sám také konečnědimenzionálním vektorovým prostorem (plyne z vět 2.1. a 4.1.).

V praxi se poměrně často setkáme s úlohou, že ve vektorovém prostoru V, jehož dimenzi známe, např. $\dim V = n$, ověřujeme, zda nějaká posloupnost sestávající z n vektorů je bází. V takovém případě stačí ověřovat pouze jednu z podmínek (1) a (2) z definice báze, jak ukazuje následující věta.

Věta 4.4. *Nechť V je vektorový prostor nad T, $\dim V = n$ $(n \geq 1)$ a nechť $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ je konečná posloupnost n vektorů z V. Pak následující výroky jsou ekvivalentní:*

(1) *vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ jsou bází prostoru V,*
(2) *vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ jsou lineárně nezávislé,*
(3) *vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ generují prostor V.*

Důkaz. „(1) $\Rightarrow$ (2)": Zřejmé (plyne z definice báze).

„(2) $\Rightarrow$ (3)": Nechť $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ jsou lineárně nezávislé. Podle věty 4.3. (3) (vzhledem k předpokladu $\dim V = n$) jsou však vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ bází prostoru V, tzn. generují prostor V.

„(3) $\Rightarrow$ (1)": Nechť $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ generují prostor V. Podle věty 4.3. (2) (vzhledem k tomu, že $\dim V = n$) však jsou vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ bází prostoru V. □

Věta 4.5. *Nechť W_1, W_2 jsou podprostory vektorového prostoru V. Potom platí:*

(1) $W_1 \subseteq W_2 \implies \dim W_1 \leq \dim W_2$,
(2) $W_1 \subseteq W_2 \wedge \dim W_1 = \dim W_2 \implies W_1 = W_2$.

Důkaz. Pokud $W_1 = \{\boldsymbol{o}\}$ nebo $W_2 = \{\boldsymbol{o}\}$, pak obě tvrzení zřejmě platí. Nechť tedy $W_1, W_2 \neq \{\boldsymbol{o}\}$ a nechť $\boldsymbol{u}_1, \dots, \boldsymbol{u}_r$ je báze W_1, resp. $\boldsymbol{v}_1, \dots, \boldsymbol{v}_s$ je báze W_2. Jestliže $W_1 \subseteq W_2$, pak $\boldsymbol{u}_i \in W_2 = L(\boldsymbol{v}_1, \dots, \boldsymbol{v}_s)$, $i = 1, \dots, r$, přičemž vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_r$ jsou lineárně nezávislé, tzn. jsou splněny předpoklady Steinitzovy věty. Potom:

(1): podle Steinitzovy věty je $r \leq s$, neboli $\dim W_1 \leq \dim W_2$,

(2): je-li navíc $\dim W_1 = \dim W_2$, tzn. $r = s$, pak opět podle Steinitzovy věty je $L(\boldsymbol{v}_1, \dots, \boldsymbol{v}_s) = L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_r)$, neboli $W_1 = W_2$. □

Poznámka. Z předchozí věty plyne několik zřejmých, ale důležitých důsledků:

1. Dimenze podprostoru je vždy menší nebo rovna dimenzi celého prostoru.

2. Je-li podprostor W_1 vlastní podmnožinou podprostoru W_2 (tzn. $W_1 \subsetneqq W_2$), potom je $\dim W_1 < \dim W_2$. Jinými slovy řečeno, nemůže se stát, aby dva podprostory stejné dimenze byly ostře v inkluzi.

3. Předpoklad $W_1 \subseteq W_2$ v předchozí větě byl podstatný, tzn. pokud dva podprostory nejsou v inkluzi, pak o vzájemném vztahu jejich dimenzí nemůžeme nic říct.

Věta 4.6. (Věta o dimenzi součtu a průniku podprostorů) *Nechť* W_1, W_2 *jsou podprostory vektorového prostoru* V. *Pak platí:*

$$\dim(W_1 + W_2) + \dim(W_1 \cap W_2) = \dim W_1 + \dim W_2.$$

Důkaz. Je-li $W_1 = \{\boldsymbol{o}\}$ nebo $W_2 = \{\boldsymbol{o}\}$, pak tvrzení zřejmě platí (rozmyslete si podrobně proč!). Nechť tedy $\dim W_1 = r \neq 0$ a $\dim W_2 = s \neq 0$.

Průnik $W_1 \cap W_2$ je podprostorem ve V, a tedy je buď $W_1 \cap W_2 = \{\boldsymbol{o}\}$, nebo existuje báze $W_1 \cap W_2$, tj. lineárně nezávislé vektory $\boldsymbol{w}_1, \dots, \boldsymbol{w}_k$ s vlastností $W_1 \cap W_2 = L(\boldsymbol{w}_1, \dots, \boldsymbol{w}_k)$.

Podle věty 4.3. (3) existují vektory $\boldsymbol{u}_{k+1}, \dots, \boldsymbol{u}_r \in W_1$ tak, že $\boldsymbol{w}_1, \dots, \boldsymbol{w}_k, \boldsymbol{u}_{k+1}, \dots, \boldsymbol{u}_r$ je báze W_1, a podobně existují vektory $\boldsymbol{v}_{k+1}, \dots, \boldsymbol{v}_s \in W_2$ tak, že $\boldsymbol{w}_1, \dots, \boldsymbol{w}_k, \boldsymbol{v}_{k+1}, \dots, \boldsymbol{v}_s$ je báze W_2 (v případě $W_1 \cap W_2 = \{\boldsymbol{o}\}$ je zřejmě $k = 0$).

Nyní dokážeme, že vektory:

$$\boldsymbol{w}_1, \dots, \boldsymbol{w}_k, \boldsymbol{u}_{k+1}, \dots, \boldsymbol{u}_r, \boldsymbol{v}_{k+1}, \dots, \boldsymbol{v}_s \tag{2}$$

jsou bází podprostoru $W_1 + W_2$.

α) Dokážeme, že vektory (2) jsou lineárně nezávislé. Nechť:

$$t_1 \cdot \boldsymbol{w}_1 + \cdots + t_k \cdot \boldsymbol{w}_k + t_{k+1} \cdot \boldsymbol{u}_{k+1} + \cdots + t_r \cdot \boldsymbol{u}_r + t'_{k+1} \cdot \boldsymbol{v}_{k+1} + \cdots + t'_s \cdot \boldsymbol{v}_s = \boldsymbol{o}. \tag{3}$$

Označme:

$$\boldsymbol{x} = t_1 \cdot \boldsymbol{w}_1 + \cdots + t_k \cdot \boldsymbol{w}_k + t_{k+1} \cdot \boldsymbol{u}_{k+1} + \cdots + t_r \cdot \boldsymbol{u}_r. \tag{4}$$

Ze (3) dostáváme, že $\boldsymbol{x} = -t'_{k+1} \cdot \boldsymbol{v}_{k+1} - \cdots - t'_s \cdot \boldsymbol{v}_s$, tzn. $\boldsymbol{x} \in W_1 \cap W_2$ a lze psát:

$$\boldsymbol{x} = g_1 \cdot \boldsymbol{w}_1 + \cdots + g_k \cdot \boldsymbol{w}_k = g_1 \cdot \boldsymbol{w}_1 + \cdots + g_k \cdot \boldsymbol{w}_k + 0 \cdot \boldsymbol{u}_{k+1} + \cdots + 0 \cdot \boldsymbol{u}_r. \tag{5}$$

Ale $\boldsymbol{w}_1, \dots, \boldsymbol{w}_k, \boldsymbol{u}_{k+1}, \dots, \boldsymbol{u}_r$ je báze W_1, tzn. že z (4) a (5) podle věty 4.2. plyne, že $t_{k+1} = \cdots = t_r = 0$. Dosadíme-li tyto hodnoty do (3), dostáváme:

$$t_1 \cdot \boldsymbol{w}_1 + \cdots + t_k \cdot \boldsymbol{w}_k + t'_{k+1} \cdot \boldsymbol{v}_{k+1} + \cdots + t'_s \cdot \boldsymbol{v}_s = \boldsymbol{o},$$

odkud plyne (poněvadž $\boldsymbol{w}_1, \dots, \boldsymbol{w}_k, \boldsymbol{v}_{k+1}, \dots, \boldsymbol{v}_s$ jsou lineárně nezávislé), že $t_1 = \cdots = t_k = t'_{k+1} = \cdots = t'_s = 0$. Dohromady dostáváme, že vektory (2) jsou lineárně nezávislé.

β) Dokážeme, že vektory (2) generují podprostor $W_1 + W_2$, tzn. že platí:

$$W_1 + W_2 = L(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k, \boldsymbol{u}_{k+1}, \ldots, \boldsymbol{u}_r, \boldsymbol{v}_{k+1}, \ldots, \boldsymbol{v}_s). \tag{6}$$

Inkluze „$\supseteq$" je zřejmá. Naopak, nechť $\boldsymbol{x} \in W_1 + W_2$ libovolný. Potom $\boldsymbol{x} = \boldsymbol{x}_1 + \boldsymbol{x}_2$, kde $\boldsymbol{x}_1 \in W_1$, $\boldsymbol{x}_2 \in W_2$. Ale $\boldsymbol{x} \in W_1 = L(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k, \boldsymbol{u}_{k+1}, \ldots, \boldsymbol{u}_r) \subseteq L(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k, \boldsymbol{u}_{k+1}, \ldots, \boldsymbol{u}_r, \boldsymbol{v}_{k+1}, \ldots, \boldsymbol{v}_s)$ a podobně pro $\boldsymbol{x}_2$. Tedy $\boldsymbol{x} = \boldsymbol{x}_1 + \boldsymbol{x}_2 \in L(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k, \boldsymbol{u}_{k+1}, \ldots, \boldsymbol{u}_r, \boldsymbol{v}_{k+1}, \ldots, \boldsymbol{v}_s)$ a dohromady pak dostáváme žádanou rovnost (6).

Dokázali jsme, že vektory (2) jsou bází $W_1 + W_2$, tzn. $\dim(W_1 + W_2) = r + s - k$. Potom však $\dim(W_1 + W_2) + \dim(W_1 \cap W_2) = r + s - k + k = r + s = \dim W_1 + \dim W_2$. $\square$

Poznamenejme, že předchozí větu nelze přímo zobecnit pro více než dva podprostory daného vektorového prostoru, jak plyne z následujícího příkladu.

Příklad 4.4. Ve vektorovém prostoru $\mathbb{R}^3$ uvažme podprostory:

$$\begin{aligned} W_1 &= \{(x_1, x_2, 0) \mid x_1, x_2 \in \mathbb{R}\}, \\ W_2 &= \{(y_1, 0, y_3) \mid y_1, y_3 \in \mathbb{R}\}, \\ W_3 &= \{(0, z_2, z_3) \mid z_2, z_3 \in \mathbb{R}\}. \end{aligned}$$

Zřejmě je $\dim W_1 = \dim W_2 = \dim W_3 = 2$ a dále je $W_1 + W_2 + W_3 = \mathbb{R}^3$, resp. $W_1 \cap W_2 \cap W_3 = \{\boldsymbol{o}\}$. Je tedy $\dim(W_1 + W_2 + W_3) + \dim(W_1 \cap W_2 \cap W_3) = 3 + 0 = 3$, ale $\dim W_1 + \dim W_2 + \dim W_3 = 2 + 2 + 2 = 6$.

Poznámka. V našich úvahách o konečných posloupnostech vektorů v předchozím paragrafu (tj. v úvahách o lineární závislosti a nezávislosti) nehrálo pořadí vektorů žádnou podstatnou roli. Se zavedením pojmu báze se však otázka pořadí vektorů okamžitě vynoří a je zřejmě podstatné, v jakém pořadí vektory báze uvažujeme (i když doposud, kdy jsme pracovali vždy jen s jednou bází, se to možná na první pohled nezdálo). Přesněji řečeno, danou bází $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ vektorového prostoru V chápeme jako uspořádanou n-tici vektorů z V, a tedy např. rovnost dvou bází znamená rovnost dvou uspořádaných n-tic vektorů z V. Důležitost této poznámky se ukáže v dalším, při zavádění pojmu souřadnic vektoru.

Definice. Nechť:

$$\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n \tag{7}$$

je báze vektorového prostoru V a nechť vektor $\boldsymbol{w} \in V$ je vyjádřen ve tvaru:

$$\boldsymbol{w} = t_1 \cdot \boldsymbol{u}_1 + \cdots + t_n \cdot \boldsymbol{u}_n, \tag{8}$$

kde $t_1, \ldots, t_n \in T$. Pak číslo t_i nazýváme i-tou souřadnicí vektoru $\boldsymbol{w}$ v bázi (7) a uspořádanou n-tici $(t_1, \ldots, t_n)$ nazýváme *souřadnicemi vektoru* $\boldsymbol{w}$ *v bázi* (7).

Poznámka. Je nutné si uvědomit, že pojem souřadnic vektoru je vždy vázán na nějakou pevnou bázi prostoru V. Zřejmě jeden vektor má v různých bázích obecně různé souřadnice.

Dále si uvědomme, že věta 4.2. zajišťuje korektnost předchozí definice, tzn. při dané bázi (7) má každý vektor $\boldsymbol{w} \in V$ souřadnice (v bázi (7)), které jsou stanoveny jednoznačně. Také naopak, ke každé uspořádané n-tici $(t_1, \ldots, t_n)$ čísel z T existuje zřejmě jediný vektor, jehož souřadnice v bázi (7) jsou právě $(t_1, \ldots, t_n)$.

Konečně poznamenejme, že souřadnice vektoru v dané bázi budeme psát nejen do řádku, jak bylo výše zavedeno, ale také někdy podle potřeby i do sloupce.

Příklad 4.5. Ve vektorovém prostoru $\mathbb{R}^3$ vezměme vektor $\boldsymbol{w} = (1, -2, 3)$. Potom:

(a) vektor $\boldsymbol{w}$ má v bázi $\boldsymbol{e}_1 = (1, 0, 0)$, $\boldsymbol{e}_2 = (0, 1, 0)$, $\boldsymbol{e}_3 = (0, 0, 1)$ souřadnice $(1, -2, 3)$,

(b) vektor $\boldsymbol{w}$ má v bázi $\boldsymbol{e}_2 = (0, 1, 0)$, $\boldsymbol{e}_1 = (1, 0, 0)$, $\boldsymbol{e}_3 = (0, 0, 1)$ souřadnice $(-2, 1, 3)$,

(c) vektor $\boldsymbol{w}$ má v bázi $\boldsymbol{u}_1 = (1, 1, 1)$, $\boldsymbol{u}_2 = (0, 1, 1)$, $\boldsymbol{u}_3 = (1, 0, 1)$ souřadnice $(-4, 2, 5)$,

jak se lehce zjistí rozepsáním z definice.

Věta 4.7. *Nechť* (7) *je báze vektorového prostoru* V. *Nechť* $t \in T$ *a nechť vektor* $\boldsymbol{x} \in V$, *resp.* $\boldsymbol{y} \in V$ *má v bázi* (7) *souřadnice* $(x_1, \ldots, x_n)$, *resp.* $(y_1, \ldots, y_n)$. *Potom:*

(1) *vektor* $\boldsymbol{x} + \boldsymbol{y}$ *má v bázi* (7) *souřadnice* $(x_1 + y_1, \ldots, x_n + y_n)$,

(2) *vektor* $t \cdot \boldsymbol{x}$ *má v bázi* (7) *souřadnice* $(t \cdot x_1, \ldots, t \cdot x_n)$.

Důkaz. Podle předpokladu je $\boldsymbol{x} = x_1 \cdot \boldsymbol{u}_1 + \cdots + x_n \cdot \boldsymbol{u}_n$, resp. $\boldsymbol{y} = y_1 \cdot \boldsymbol{u}_1 + \cdots + y_n \cdot \boldsymbol{u}_n$, tzn. potom (po úpravě):

$$\begin{aligned} \boldsymbol{x} + \boldsymbol{y} &= (x_1 + y_1) \cdot \boldsymbol{u}_1 + \cdots + (x_n + y_n) \cdot \boldsymbol{u}_n, \\ t \cdot \boldsymbol{x} &= (t \cdot x_1) \cdot \boldsymbol{u}_1 + \cdots + (t \cdot x_n) \cdot \boldsymbol{u}_n, \end{aligned}$$

odkud již plyne tvrzení věty. □

Kapitola 2

Matice a determinanty

§1. Pořadí a permutace

Permutací libovolné množiny M se obecně rozumí každé bijektivní zobrazení množiny M na sebe samu. Naším cílem však není studium obecných vlastností permutací libovolných množin, nýbrž permutace nám budou pouze pomocným nástrojem ke studiu dalších algebraických pojmů. Omezíme se proto v tomto paragrafu jen na výklad nejzákladnějších vlastností permutací konečné množiny M, řekněme n-prvkové. Pro zjednodušení vyjadřování budeme v dalším předpokládat, že množina M se skládá z prvních n přirozených čísel, tzn. $M = \{1, 2, \dots, n\}$.

Definice. Nechť $M = \{1, 2, \dots, n\}$. Pak libovolná uspořádaná n-tice utvořená z prvků množiny M se nazývá pořadí z n prvků $1, 2, \dots, n$ nebo stručně *pořadí.*

Nechť $R = (r_1, \dots, r_n)$ je libovolné pořadí. Řekneme, že dvojice r_i, r_j je *inverze* v pořadí R, jestliže $i < j$ a $r_i > r_j$ (tj. jestliže větší z obou čísel předchází v daném pořadí číslu menšímu).

Pořadí, v němž celkový počet inverzí je sudé číslo (resp. liché číslo), se nazývá *sudé pořadí* (resp. *liché pořadí*). Hovoříme pak též o paritě pořadí.

Příklad 1.1. Nechť $n = 8$. Potom:

1. pořadí $(1, 2, 3, 4, 5, 6, 7, 8)$ je sudé (celkový počet inverzí je 0),

2. pořadí $(3, 1, 2, 7, 5, 8, 6, 4)$ je liché (celkový počet inverzí je 9).

Celkový počet inverzí v daném konkrétním pořadí zřejmě nejrychleji zjistíme tak, že bereme odleva jedno číslo po druhém a pro každé z nich spočítáme, kolik menších čísel stojí za ním (napravo). Sečtením těchto hodnot pak dostaneme celkový počet inverzí v daném pořadí.

Definice. Nechť $R = (r_1, \dots, r_n)$, $S = (s_1, \dots, s_n)$ jsou dvě pořadí. Nechť existují indexy $i \neq j$ tak, že $s_i = r_j$, $s_j = r_i$ a dále $r_k = s_k$ pro $k \neq i, j$. Potom řekneme, že pořadí S vzniklo z pořadí R provedením jedné *transpozice*.

Poznámka. Jinými slovy řečeno, provedení jedné transpozice znamená vzájemnou záměnu dvou různých prvků v daném pořadí, přičemž všechny ostatní prvky zůstávají na původním místě.

Věta 1.1. *Nechť n je pevné přirozené číslo. Pak platí:*

(1) *z n prvků lze utvořit celkem $n!$ různých pořadí,*

(2) *všech $n!$ pořadí z n prvků lze seřadit tak, že každé následující pořadí obdržíme z předcházejícího provedením jedné transpozice. Přitom lze vyjít z libovolného pořadí.*

Důkaz. Připomeňme, že symbol $n!$ (čti „n faktoriál") značí přirozené číslo definované: $n! = n \cdot (n-1) \cdot \cdots \cdot 2 \cdot 1$. Dokazovat budeme obě části věty najednou, a to matematickou indukcí.

α) Pro $n = 1$ obě tvrzení triviálně platí.

β) Předpokládejme, že obě tvrzení platí pro $1, \dots, n-1$, a budeme je dokazovat pro n. Nechť $(r_1, \dots, r_n)$ je libovolné pořadí z n prvků. Podle indukčního předpokladu je všech pořadí, která mají na posledním místě prvek r_n, celkem $(n-1)!$ a lze je seřadit tak, že následující vznikne z předchozího provedením jedné transpozice. V posledním z těchto pořadí proveďme transpozici prvků r_n a r_i $(1 \leq i \leq n-1)$ a stejnou úvahou jako výše dostaneme $(n-1)!$ pořadí s prvkem r_i na posledním místě. Takto vystřídáme na posledním místě všech n prvků, čímž dostaneme všechna různá pořadí z n prvků, kterých je tedy $n \cdot (n-1)! = n!$, přičemž následující pořadí vzniklo vždy z předchozího provedením jedné transpozice. $\square$

Věta 1.2. *Provedení jedné transpozice změní paritu daného pořadí.*

Důkaz. Provedeme ve dvou krocích. Nejprve pro transpozici sousedních prvků a potom pro transpozici libovolných dvou různých prvků daného pořadí.

α) Nechť v pořadí $R = (r_1, \dots, r_i, r_{i+1}, \dots, r_n)$ je t inverzí. Provedením transpozice sousedních prvků r_i a r_{i+1} dostaneme pořadí $R' = (r_1, \dots, r_{i+1}, r_i, \dots, r_n)$, v němž je buď $t-1$, nebo $t+1$ inverzí. Tedy R' má opačnou paritu než R.

β) Nechť $R = (r_1, \dots, r_i, \dots, r_j, \dots, r_n)$ je dané pořadí. Provedením transpozice prvků r_i a r_j dostaneme pořadí $R' = (r_1, \dots, r_j, \dots, r_i, \dots, r_n)$. Tuto transpozici však lze realizovat postupným provedením $(j-i)+(j-i-1) = 2(j-i)-1$ transpozic sousedních prvků. Ale číslo $2(j-i)-1$ je liché, tzn. užitím α) dostáváme tvrzení. $\square$

Věta 1.3. *Nechť $n \geq 2$. Pak z celkového počtu $n!$ různých pořadí z n prvků je $\frac{n!}{2}$ sudých a $\frac{n!}{2}$ lichých pořadí.*

Důkaz. Tvrzení věty plyne ihned v vět 1.1. a 1.2. $\square$

Definice. Nechť $M = \{1, 2, \dots, n\}$ je konečná množina o n prvcích. Pak bijektivní zobrazení P množiny M na sebe se nazývá permutace množiny M nebo krátce *permutace*.

Permutaci P definovanou: $P(i_t) = j_r$, pro $t = 1, \dots, n$, budeme zapisovat ve formě dvouřádkové tabulky tvaru:

$$\begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix}.$$

Poznámka. Permutace množiny M je tedy bijekce $M \to M$, kterou zapisujeme ve tvaru dvouřádkové tabulky. Znamená to, že v horním i dolním řádku této tabulky musí být vždy nějaké pořadí z n prvků. Zřejmě lze tutéž permutaci P zapsat v uvedeném tvaru celkem $n!$ formálně různými způsoby (zaměníme-li pořadí sloupců v tabulce permutace). Všech těchto $n!$ zápisů permutace P je samozřejmě naprosto rovnocenných, i když nejčastěji budeme permutaci zapisovat v tzv. základním tvaru:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}.$$

Příklad 1.2. Pro $n = 5$ jsou:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix}, \text{ resp. } \begin{pmatrix} 3 & 2 & 1 & 4 & 5 \\ 5 & 3 & 2 & 4 & 1 \end{pmatrix}, \text{ resp. } \begin{pmatrix} 4 & 1 & 5 & 2 & 3 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix}$$

tři formálně různé zápisy téže permutace (z celkového počtu $5! = 120$ možných zápisů této jedné permutace).

Věta 1.4. *Počet různých permutací n-prvkové množiny je roven $n!$.*

Důkaz. Zapíšeme-li každou permutaci v základním tvaru:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix},$$

pak různých permutací bude přesně tolik, kolik bude různých pořadí v dolním řádku. Těch je však $n!$ podle věty 1.1. (1). $\square$

Definice. Permutace P se nazývá *sudá permutace*, resp. *lichá permutace*, jestliže počtu inverzí v horním a dolním řádku tabulky permutace P je sudé číslo, resp. liché číslo. Hovoříme pak též o paritě permutace.

Poznámka. I když danou permutaci P můžeme zapsat $n!$ formálně různými tabulkami, je předchozí definice korektní, neboť při libovolném zápisu permutace P je parita horního a dolního řádku (chápaných jako pořadí) buď vždy stejná, nebo vždy rozdílná. Tento fakt plyne z toho, že při přechodu od jednoho zápisu permutace P k jinému provádíme totiž jistý počet transpozic, a to současně v horním i dolním řádku.

Věta 1.5. *Nechť $n \geq 2$. Pak z celkového počtu $n!$ různých permutací n-prvkové množiny je $\frac{n!}{2}$ sudých permutací a $\frac{n!}{2}$ lichých permutací.*

Důkaz. Každou permutaci zapíšeme v základním tvaru:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}.$$

Parita permutace je pak shodná s paritou pořadí v dolním řádku a věta plyne bezprostředně z věty 1.3. $\square$

Na závěr paragrafu využijeme příležitosti, kterou nám permutace poskytují, a vrátíme se krátce k algebraickým strukturám. Jak bylo výše řečeno, permutace n-prvkové množiny M je bijekce $M \to M$, tedy zobrazení. Pro permutace tak platí všechny základní poznatky o zobrazeních, uvedené dříve. Například můžeme permutace skládat (ve smyslu skládání zobrazení), přičemž zřejmě výsledné zobrazení (tj. složení dvou bijekcí) je také bijekce $M \to M$, čili permutace. Konkrétně, zapíšeme-li permutace P, R ve tvaru:

$$P = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}, \quad R = \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix},$$

pak složením P a R (v tomto pořadí) dostaneme permutaci:

$$R \circ P = \begin{pmatrix} 1 & 2 & \cdots & n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix}.$$

Tedy množina všech permutací n-prvkové množiny M s operací $\circ$ skládání permutací je grupoid, který podle V.5.2. kap. I. je pologrupou. Platí však ještě více, jak ukazuje následující věta.

Věta 1.6. *Množina všech permutací n-prvkové množiny s operací $\circ$ skládání permutací je grupou. Tato grupa je pro $n \geq 3$ nekomutativní.*

Důkaz. Podle předchozí poznámky jde o pologrupu. Dále zřejmě permutace:

$$E = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

je jedničkou a k libovolné permutaci:

$$P = \begin{pmatrix} i_1 & \cdots & i_n \\ j_1 & \cdots & j_n \end{pmatrix}$$

existuje inverzní permutace, a sice:

$$\begin{pmatrix} j_1 & \cdots & j_n \\ i_1 & \cdots & i_n \end{pmatrix}.$$

Tedy množina všech permutací n-prvkové množiny s operací $\circ$ je grupa.

Nechť $n \geq 3$. Pak pro:

$$P = \begin{pmatrix} 1 & 2 & 3 & \cdots \\ 3 & 1 & 2 & \cdots \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 2 & 3 & \cdots \\ 1 & 3 & 2 & \cdots \end{pmatrix}$$

platí $R \circ P \neq P \circ R$ (ověřte si detailně sami!), a tedy operace $\circ$ není komutativní. $\square$

Poznámka. Předchozí věta udává jeden z nejjednodušších příkladů nekomutativní grupy. Tato grupa se obvykle nazývá *grupa permutací* (na n-prvkové množině M) nebo též symetrická grupa permutací stupně n.

§2. Determinanty

Jedním ze základních pojmů celé moderní matematiky je pojem matice. Teorie matic hraje ústřední úlohu v tzv. lineární algebře. Její výsledky se pak aplikují při řešení soustav lineárních rovnic, při studiu vektorových prostorů a v celé řadě dalších odvětví nejenom matematiky.

Definice. Nechť T je číselné těleso, m, n jsou přirozená čísla. Pak obdélníkové schéma tvaru:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}, \tag{1}$$

kde $a_{ij} \in T$ pro $i = 1, \dots, m$ a $j = 1, \dots, n$, se nazývá *matice typu m/n* (nad tělesem T). Označení: $A = (a_{ij})$ typu m/n. Čísla $a_{ij} \in T$ se nazývají *prvky matice A*.

Matice $A = (a_{ij})$ typu m/n a matice $B = (b_{ij})$ typu p/q jsou si rovny, jestliže jsou stejného typu (tj. $m = p \wedge n = q$) a je-li $a_{ij} = b_{ij}$ pro každé i, j.

Poznámka. 1. Předchozí definice matice je sice názorná, ale přísně vzato není zcela korektní, neboť se v ní používá formálně nejasného a nepřesného pojmu „obdélníkové schéma“ (a je pak nutné hovořit o rovnosti dvou matic). Zcela přesně by bylo třeba matici typu m/n nad tělesem T definovat jakožto zobrazení:

$$f : \{1, 2, \dots, m\} \times \{1, 2, \dots, n\} \to T,$$

kde $f\big((i, j)\big) = a_{ij}$. Při této definici by však většina tvrzení o maticích byla formálně značně komplikovaná a nepřehledná. Ponecháme tedy definici matice tak, jak byla původně uvedena (tj. vypisujeme vlastně funkční hodnoty uvedeného zobrazení f do onoho „obdélníkového schématu“).

2. Každý jednotlivý řádek matice A typu m/n nad tělesem T můžeme zřejmě uvažovat jako uspořádanou n-tici prvků (tj. čísel) z tělesa T, tzn. jinak řečeno, jako vektor z vektorového prostoru T^n. Má smysl pak hovořit o sčítání řádků matice, násobení řádku číslem z T, lineární kombinaci řádků, lineární závislosti a nezávislosti řádků, atd., a to ve smyslu uvedených operací, resp. pojmů tak, jak byly definovány ve vektorovém prostoru T^n. Matici A lze pak též chápat jako uspořádanou m-tici vektorů z T^n.

Analogicky můžeme sloupce matice A chápat jako vektory z vektorového prostoru T^m a provádět s nimi tytéž úvahy.

Definice. Nechť $A = (a_{ij})$ je matice typu m/n nad T. Potom:

(1) je-li $a_{ij} = 0$ pro každé i, j (tj. všechny prvky matice jsou rovny nule), matice se nazývá *nulová matice* (typu m/n) a označuje se symbolem 0_{mn},

(2) je-li $m = n$ (tj. počet řádků je roven počtu sloupců), matice A se nazývá *čtvercová matice řádu* n,

(3) matice A' typu n/m, která vznikne z matice A záměnou řádků za sloupce, tj.:

$$A' = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{pmatrix},$$

se nazývá *transponovaná matice* k matici A.

Ve zbývající části tohoto paragrafu se budeme zabývat pouze čtvercovými maticemi řádu n nad pevným číselným tělesem T. Pro tyto matice nejprve zavedeme následující pojem.

Definice. Nechť $A = (a_{ij})$ je čtvercová matice řádu n nad tělesem T. Pak *determinant matice* A je číslo z tělesa T označené $\det A$ (nebo též $|A|$) a definované vztahem:

$$\det A = \sum_{(j_1,\ldots,j_n)} (-1)^{I(j_1,\ldots,j_n)} \cdot a_{1j_1} \cdot a_{2j_2} \cdot \; \cdots \; \cdot a_{nj_n},$$

kde $I(j_1, \ldots, j_n)$ značí celkový počet inverzí v permutaci:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix}$$

použitých řádkových a sloupcových indexů. Sčítání se provádí přes všechna různá pořadí $(j_1, \ldots, j_n)$ sloupcových indexů.

Součin:

$$(-1)^{I(j_1,\ldots,j_n)} \cdot a_{1j_1} \cdot a_{2j_2} \cdot \; \cdots \; \cdot a_{nj_n}$$

se nazývá *člen determinantu.*

Poznámka. Rozebereme-li si předchozí definici podrobněji, pak vidíme, že determinant $\det A$ je číslo z T, které dostaneme sečtením celkem $n!$ členů determinantu (viz věta 1.1. (1)). Přitom každý jednotlivý člen determinantu je součinem n prvků matice A vybraných tak, že z každého řádku a každého sloupce je vybrán právě jeden prvek a tento součin je „opatřen znaménkem $+$ nebo $-$“ podle toho, zda permutace utvořená z řádkových a sloupcových indexů vybraných n prvků je sudá nebo lichá.

Dále je třeba si uvědomit zásadní rozdíl mezi pojmem matice (tj. jakýmsi obdélníkovým, resp. čtvercovým schématem) a pojmem determinantu matice (tj. pevným číslem z T).

Příklad 2.1. Rozepišme si předchozí definici determinantu pro nejjednodušší případy, tj. $n = 1, 2, 3$.

$$n=1 \quad \begin{vmatrix} a_{11} \end{vmatrix} = a_{11},$$

$$n=2 \quad \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}\cdot a_{22} - a_{12}\cdot a_{21},$$

$$n=3 \quad \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \begin{array}{l} a_{11}\cdot a_{22}\cdot a_{33} + a_{12}\cdot a_{23}\cdot a_{31} + a_{13}\cdot a_{21}\cdot a_{32} - \\ \quad - a_{13}\cdot a_{22}\cdot a_{31} - a_{12}\cdot a_{21}\cdot a_{33} - a_{11}\cdot a_{23}\cdot a_{32}. \end{array}$$

Je vidět, že výpočet determinantu matice pouze na základě definice by byl neúnosně zdlouhavý a pracný, zejména pro větší n. Např. pro $n = 10$ by bylo nutno spočítat přes tři a půl milionu desetičlenných součinů (neboť $10! = 3\,628\,800$). Z tohoto důvodu uvedeme nyní několik vět popisujících základní vlastnosti determinantů, které mnohdy výpočet determinantu podstatně usnadní.

Všude v dalším v tomto paragrafu budeme symbolem A označovat čtvercovou matici $A = (a_{ij})$ řádu n nad tělesem T.

Věta 2.1. *Transponováním matice A se hodnota determinantu nezmění, tj.* $\det A' = \det A$.

Důkaz. Nechť $(j_1, j_2, \ldots, j_n)$ je libovolné pořadí z n prvků. Pak součin $a_{1j_1}\cdot a_{2j_2}\cdot \,\cdots\, \cdot a_{nj_n}$ se vyskytuje právě jednou v $\det A$ i $\det A'$. Tento součin je v $\det A$ vynásoben číslem $(-1)^r$, resp. v $\det A'$ číslem $(-1)^s$, kde r, resp. s značí celkový počet inverzí v permutaci:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix}, \text{ resp. } \begin{pmatrix} j_1 & j_2 & \cdots & j_n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

Zřejmě však $r = s$, odkud již plyne tvrzení. □

Věta 2.2. *Nechť prvky k-tého řádku matice A mají tvar:*

$$\begin{aligned} a_{k1} &= b_{k1} + c_{k1}, \\ a_{k2} &= b_{k2} + c_{k2}, \\ &\vdots \\ a_{kn} &= b_{kn} + c_{kn} \end{aligned}$$

a nechť matice B, resp. C se liší od matice A pouze v prvcích k-tého řádku, přičemž $b_{k1}, \dots, b_{kn}$, resp. $c_{k1}, \dots, c_{kn}$ je k-tý řádek matice B, resp. C. Potom $\det A = \det B + \det C$.

Schématicky zapsáno, platí:

$$\begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots \\ b_{k1} + c_{k1} & \cdots & b_{kn} + c_{kn} \\ \vdots & \vdots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots \\ b_{k1} & \cdots & b_{kn} \\ \vdots & \vdots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots \\ c_{k1} & \cdots & c_{kn} \\ \vdots & \vdots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix}.$$

Důkaz. Tvrzení plyne přímo z definice determinantu, neboť pro každý člen determinantu $\det A$ platí:

$$(-1)^{I(j_1,\dots,j_n)} \cdot a_{1j_1} \cdot \cdots \cdot (b_{kj_k} + c_{kj_k}) \cdot \cdots \cdot a_{nj_n} =$$
$$(-1)^{I(j_1,\dots,j_n)} \cdot a_{1j_1} \cdot \cdots \cdot b_{kj_k} \cdot \cdots \cdot a_{nj_n} + (-1)^{I(j_1,\dots,j_n)} \cdot a_{1j_1} \cdot \cdots \cdot c_{kj_k} \cdot \cdots \cdot a_{nj_n}.$$

□

Poznámka. Předchozí větu lze zřejmě rozšířit pro libovolný konečný počet sčítanců v k-tém řádku matice A (dokáže se pomocí matematické indukce).

Věta 2.3. *Nechť matice B vznikne z matice A:*

(1) *záměnou dvou různých řádků. Potom je* $\det B = -\det A$.

(2) *vynásobením jednoho řádku pevným číslem $t \in T$. Potom je* $\det B = t \cdot \det A$.

Důkaz. (1): Zaměňme v matici A k-tý řádek s r-tým řádkem, kde $k \neq r$. Pak součiny vyskytující se v $\det A$ a $\det B$ zůstanou stejné, ale mají vždy opačná znaménka, protože permutace:

$$\begin{pmatrix} 1 & \cdots & k & \cdots & r & \cdots & n \\ j_1 & \cdots & j_k & \cdots & j_r & \cdots & j_n \end{pmatrix} \text{ a } \begin{pmatrix} 1 & \cdots & k & \cdots & r & \cdots & n \\ j_1 & \cdots & j_r & \cdots & j_k & \cdots & j_n \end{pmatrix}$$

mají (podle věty 1.2.) různou paritu. Potom však $\det B = -\det A$.

(2): Plyne přímo z definice determinantu, neboť vynásobíme-li v matici A např. k-tý řádek prvkem $t \in T$, potom:

$$\det B = \sum (-1)^{I(j_1,\ldots,j_n)} \cdot a_{1j_1} \cdot \cdots \cdot t \cdot a_{kj_k} \cdot \cdots \cdot a_{nj_n} =$$
$$t \cdot \sum (-1)^{I(j_1,\ldots,j_n)} \cdot a_{1j_1} \cdot \cdots \cdot a_{nj_n} = t \cdot \det A.$$

□

Věta 2.4. *Nechť v matici A:*

(1) *jeden řádek sestává ze samých nul. Potom je* $\det A = 0$.
(2) *dva různé řádky jsou shodné. Potom je* $\det A = 0$.
(3) *jeden řádek je t-násobkem jiného řádku ($t \in T$ lib.). Potom je* $\det A = 0$.
(4) *jeden řádek je lineární kombinací ostatních řádků. Potom je* $\det A = 0$.

Důkaz. (1): Plyne přímo z definice determinantu. Každý člen $\det A$ je totiž roven nule, poněvadž obsahuje nulu (a sice z toho řádku, který sestává ze samých nul).

(2): Zaměníme-li ty dva řádky matice A, které jsou shodné, pak matice A se zřejmě nezmění. Podle věty 2.3. (1) však musí být $\det A = -\det A$, tj. $2 \cdot \det A = 0$, odkud však dostáváme, že $\det A = 0$.

(3): Plyne přímo z věty 2.3. (2) a z právě dokázané části (2).

(4): Nechť např. k-tý řádek matice A je lineární kombinací ostatních řádků. Pak $\det A$ lze podle poznámky za větou 2.2. vyjádřit jako součet $(n-1)$ determinantů, z nichž však v každém je k-tý řádek násobkem nějakého jiného řádku. Podle části (3) této věty je však každý z těchto $(n-1)$ determinantů roven nule, a tedy $\det A = 0 + 0 + \cdots + 0 = 0$. □

Věta 2.5. *Hodnota determinantu matice A se nezmění, jestliže:*

(1) *k jednomu řádku matice A přičteme libovolný násobek jiného řádku,*

(2) *k jednomu řádku matice A přičteme libovolnou lineární kombinaci ostatních řádků,*
(3) *jeden řádek matice A ponecháme beze změny a k ostatním řádkům přičteme jeho libovolné násobky.*

Důkaz. (1): Plyne bezprostředně z vět 2.2. a 2.4. (3).
(2): Plyne z poznámky za větou 2.2. a z věty 2.4. (4).
(3): Plyne z (1), jejím opakováním. □

Poznámka. Z věty 2.1. plyne, že ke každé z následujících vět, tj. 2.2., 2.3. a 2.4. platí analogická věta, kterou získáme tak, že v původní formulaci slovo „řádek" nahradíme slovem „sloupec". Například, platí tedy tvrzení: „jestliže v matici A je jeden sloupec lineární kombinací ostatních sloupců, potom je $\det A = 0$", atd.

Tuto úvahu lze zřejmě uplatnit na každé tvrzení o determinantech matice, týkající se řádků matice. Dostaneme tak stejné tvrzení, týkající se sloupců. Analogicky naopak (tzn. z každého platného tvrzení o determinantech, týkajícího se sloupců dané matice, dostaneme záměnou slova „sloupec" za slovo „řádek" platné tvrzení, týkající se řádků).

Větu 2.5. (a odpovídající větu pro sloupce) často využíváme při konkrétních výpočtech determinantů, kdy se přičítáním vhodných násobků jedněch řádků (resp. sloupců) k jiným řádkům (resp. sloupcům) snažíme matici upravit na takový tvar, z něhož již determinant lehce spočítáme. Například, dojdeme-li k matici A tvaru:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1,(n-1)} & a_{1n} \\ 0 & a_{22} & \cdots & a_{2,(n-1)} & a_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & a_{(n-1),(n-1)} & a_{(n-1),n} \\ 0 & 0 & \cdots & 0 & a_{nn} \end{pmatrix}$$

(tj. všude pod hlavní diagonálou jsou nuly), pak $\det A = a_{11} \cdot a_{22} \cdot \cdots \cdot a_{nn}$, jak plyne ihned z definice determinantu. Stejný výsledek (tzn. hodnota determinantu je rovna součinu prvků v hlavní diagonále) dostaneme, jestliže v matici jsou samé nuly nad hlavní diagonálou.

Ve zbývající části tohoto paragrafu pak odvodíme ještě jeden způsob jak zjednodušit výpočet determinantu.

Definice. Nechť $A = (a_{ij})$ je čtvercová matice řádu n. Nechť je zvoleno k jejích řádků a sloupců ($k < n$), a sice: $1 \leq i_1 < i_2 < \cdots < i_k \leq n$, resp. $1 \leq j_1 < j_2 < \cdots < j_k \leq n$. Pak matice:

$$M = \begin{pmatrix} a_{i_1j_1} & a_{i_1j_2} & \cdots & a_{i_1j_k} \\ a_{i_2j_1} & a_{i_2j_2} & \cdots & a_{i_2j_k} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i_kj_1} & a_{i_kj_2} & \cdots & a_{i_kj_k} \end{pmatrix}$$

se nazývá *submatice* matice A určená řádky $i_1, \dots, i_k$ a sloupci $j_i \dots, j_k$. Její determinant $|M|$ se nazývá *minor* řádu k matice A.

Zbývajícími $(n-k)$ řádky a $(n-k)$ sloupci je určena submatice $\overline{M}$ matice A, která se nazývá *doplňková submatice* k submatici M a její minor $|\overline{M}|$ se nazývá *doplněk* minoru $|M|$.

Označme $s_M = i_1 + i_2 + \cdots + i_k + j_1 + \cdots + j_k$. Pak číslo $(-1)^{s_M} \cdot |\overline{M}|$ se nazývá *algebraický doplněk* minoru $|M|$. Člen doplňku $|\overline{M}|$ vynásobený číslem $(-1)^{s_M}$ se pak nazývá člen algebraického doplňku minoru $|M|$.

Příklad 2.2. Nechť A je čtvercová matice řádu 4 nad tělesem $\mathbb{R}$:

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & -3 \\ -1 & 2 & 0 & 1 \\ 6 & -2 & -1 & 3 \end{pmatrix}.$$

Zvolíme-li $i_1 = 1$, $i_2 = 3$, $j_1 = 2$, $j_2 = 3$, tj. první a třetí řádek, resp. druhý a třetí sloupec, pak submatice M určená zvolenými řádky a sloupci je tvaru:

$$M = \begin{pmatrix} 2 & 3 \\ 2 & 0 \end{pmatrix}, \quad \text{tzn. minor } |M| = -6.$$

Doplňkovou submatici je pak:

$$\overline{M} = \begin{pmatrix} 0 & -3 \\ 6 & 3 \end{pmatrix}, \quad \text{tzn. doplněk } |\overline{M}| = +18.$$

Dále je $s_M = 1 + 3 + 2 + 3 = 9$, tzn. algebraický doplněk minoru $|M|$ je:

$$(-1)^{s_M} \cdot |\overline{M}| = (-1)^9 \cdot 18 = -18.$$

Poznámka. Označíme-li $s_{\overline{M}}$ součet indexů řádků a sloupců určujících doplňkovou submatici $\overline{M}$, pak zřejmě platí $(-1)^{s_M} = (-1)^{s_{\overline{M}}}$, neboť $s_M + s_{\overline{M}} = 2 \cdot (1 + 2 + \cdots + n)$ je sudé číslo, a tedy s_M a $s_{\overline{M}}$ musí být obě buď současně sudá, nebo současně lichá. Tedy algebraický doplněk minoru $|M|$ je též roven číslu $(-1)^{s_{\overline{M}}} \cdot |\overline{M}|$, což lze někdy při praktických výpočtech s výhodou použít.

Věta 2.6. *Nechť A je čtvercová matice řádu n, nechť $|M|$ je minor řádu k matice A ($k < n$). Pak součin libovolného členu minoru $|M|$ s libovolným členem jeho algebraického doplňku je členem determinantu $|A|$.*

Důkaz. Nechť submatice M je určena řádky $i_1, \ldots, i_k$ a sloupci $j_1, \ldots, j_k$ matice A, přičemž $i_1 < i_2 < \cdots < i_k$, resp. $j_1 < j_2 < \cdots < j_k$.

Zaměňme i_1-tý řádek matice A s $(i_1 - 1)$-tým řádkem, pak s $(i_1 - 2)$-tým řádkem, atd., až s prvním řádkem. Celkem jsme takto provedli $(i_1 - 1)$ záměn řádků matice A. Podobně pomocí $(i_2 - 2)$ záměn řádků přemístíme i_2-tý řádek na místo druhého řádku, atd., až pomocí $(i_k - k)$ záměn řádků přemístíme i_k-tý řádek na místo k-tého řádku. Celkem jsme tedy provedli $(i_1 - 1) + (i_2 - 2) + \cdots + (i_k - k) = (i_1 + \cdots + i_k) - (1 + 2 + \cdots + k)$ záměn řádků matice A. Analogicky pomocí $(j_1 + \cdots + j_k) - (1 + 2 + \cdots + k)$ záměn sloupců matice A přemístíme $j_1, \ldots, j_k$-tý sloupec na místo prvního, ..., až k-tého sloupce. (Důležité je, že se po provedení těchto úprav nezměnilo původní pořadí řádků a sloupců submatice M ani její doplňkové submatice $\overline{M}$, tzn. nezměnily se hodnoty jednotlivých členů minoru $|M|$ ani členů jeho doplňku $|\overline{M}|$.)

Tedy pomocí $(i_1 + \cdots + i_k + j_1 + \cdots + j_k) - 2 \cdot (1 + \cdots + k)$ záměn řádků, resp. sloupců jsme z matice A dostali jistou matici B, přičemž podle věty 2.3. (1) platí:

$$|B| = |A| \cdot (-1)^{i_1 + \cdots + i_k + j_1 + \cdots + j_k - 2 \cdot (1 + \cdots + k)} = |A| \cdot (-1)^{i_1 + \cdots + i_k + j_1 + \cdots + j_k},$$

odkud po vynásobení číslem $(-1)^{i_1 + \cdots + i_k + j_1 + \cdots + j_k}$ dostáváme:

$$|A| = |B| \cdot (-1)^{i_1 + \cdots + i_k + j_1 + \cdots + j_k}. \tag{2}$$

Submatice M je v matici B určena prvními k řádky a prvními k sloupci. Potom však součin libovolného členu minoru $|M|$ s libovolným členem doplňku $|\overline{M}|$ je členem determinantu $|B|$, neboť označíme-li $B = (b_{ij})$, pak člen minoru $|M|$, resp. člen doplňku $|\overline{M}|$ jsou tvaru:

$$(-1)^{I(t_1, \ldots, t_k)} \cdot b_{1t_1} \cdot \cdots \cdot b_{kt_k}, \text{ resp. } (-1)^{I(t_{k+1}, \ldots, t_n)} \cdot b_{k+1, t_{k+1}} \cdot \cdots \cdot b_{nt_n}, \tag{3}$$

kde $I(t_1,\dots,t_k)$ značí počet inverzí v permutaci $\begin{pmatrix}1 & \cdots & k\\ t_1 & \cdots & t_k\end{pmatrix}$, resp. $I(t_{k+1},\dots,t_n)$ značí počet inverzí v permutaci $\begin{pmatrix}k+1 & \cdots & n\\ t_{k+1} & \cdots & t_n\end{pmatrix}$. Označíme-li $I(t_1,\dots,t_n)$ počet inverzí v permutaci $\begin{pmatrix}1 & \cdots & n\\ t_1 & \cdots & t_n\end{pmatrix}$, pak platí (rozmyslete si proč!): $I(t_1,\dots,t_k) + I(t_{k+1},\dots,t_n) = I(t_1,\dots,t_n)$. Potom však vynásobením obou členů z (3) dostáváme: $(-1)^{I(t_1,\dots,t_n)} \cdot b_{1t_1} \cdot \cdots \cdot b_{nt_n}$, což je však člen determinantu $|B|$.

Odtud (podle (2)) součin libovolného členu minoru $|M|$ s libovolným členem doplňku $|\overline{M}|$ vynásobený číslem $(-1)^{i_1+\cdots+i_k+j_1+\cdots+j_k}$ je členem determinantu $|A|$. To však je již žádané tvrzení, neboť libovolný člen algebraického doplňku minoru $|M|$ v matici A obdržíme z libovolného členu doplňku $|\overline{M}|$ vynásobením číslem $(-1)^{i_1+\cdots+i_k+j_1+\cdots+j_k}$. □

Věta 2.7. (Laplaceova věta) *Nechť $A = (a_{ij})$ je čtvercová matice řádu n, nechť je pevně zvoleno k řádků matice A, kde $0 < k < n$. Pak determinant $|A|$ je roven součtu všech $\binom{n}{k}$ součinů minorů řádu k vybraných ze zvolených k řádků s jejich algebraickými doplňky.*

Důkaz. Ze zvolených řádků lze zřejmě vybrat minor řádu k právě $\binom{n}{k}$ různými způsoby. Podle věty 2.6. je součin členu takového minoru s členem jeho algebraického doplňku členem determinantu $|A|$. Přitom je zřejmé, že dostáváme navzájem různé členy. K důkazu našeho tvrzení tedy stačí spočítat, zda uvedeným způsobem dostaneme všechny členy determinantu $|A|$ (kterých, jak víme, je $n!$). Ale každý minor řádu k má $k!$ členů, každý jeho algebraický doplněk má $(n-k)!$ členů a vybraných minorů je $\binom{n}{k}$, tzn. celkem dostáváme:

$$k! \cdot (n-k)! \cdot \binom{n}{k} = k! \cdot (n-k)! \cdot \frac{n!}{k! \cdot (n-k)!} = n!$$

členů determinantu $|A|$, a tedy věta platí. □

Poznámka. Laplaceova věta se také někdy nazývá „věta o rozvoji determinantu podle zvolených k řádků“. Její praktický význam spočívá v tom, že výpočet determinantu určitého řádu, např. n, převádíme na výpočet jistého počtu determinantů matic řádu menšího než n.

Připomeňme, že na základě věty 2.1. platí analogická věta k Laplaceově větě zformulovaná pro sloupce (tzn. slovo „řádek“ v Laplaceově větě nahradíme slovem „sloupec"). Říkáme pak, že jsme determinant vyjádřili rozvinutím podle daných k sloupců.

Definice. Nechť $A = (a_{ij})$ je čtvercová matice řádu n. Pak algebraický doplněk jednoprvkové submatice sestávající z prvku a_{ij} budeme krátce nazývat *algebraický doplněk prvku* a_{ij} a označovat symbolem A_{ij}.

Důsledek. *Nechť $A = (a_{ij})$ je čtvercová matice řádu n, nechť i, resp. j je pevně zvolený řádkový, resp. sloupcový index. Pak platí:*

$$|A| = a_{i1} \cdot A_{i1} + a_{i2} \cdot A_{i2} + \cdots + a_{in} \cdot A_{in},$$

resp.

$$|A| = a_{1j} \cdot A_{1j} + a_{2j} \cdot A_{2j} + \cdots + a_{nj} \cdot A_{nj}.$$

Důkaz. Uvedený důsledek je doslovným přepisem Laplaceovy věty, a sice pro $k = 1$. □

Příklad 2.3. Užitím Laplaceovy věty spočtěme determinant $|A|$, kde A je matice řádu 4 (nad $\mathbb{R}$) tvaru:

$$A = \begin{pmatrix} 1 & 1 & 3 & 4 \\ 2 & 0 & 0 & 8 \\ 3 & 0 & 0 & 2 \\ 4 & 4 & 7 & 5 \end{pmatrix}.$$

1. Výpočet provedeme rozvinutím podle 2. a 3. řádku (při praktickém výpočtu je zřejmě nejvýhodnější volit řádky, v nichž se vyskytuje pokud možno hodně nul). Pak:

$$|A| = \begin{vmatrix} 2 & 0 \\ 3 & 0 \end{vmatrix} \cdot \begin{vmatrix} 3 & 4 \\ 7 & 5 \end{vmatrix} \cdot (-1)^8 + \begin{vmatrix} 2 & 0 \\ 3 & 0 \end{vmatrix} \cdot \begin{vmatrix} 1 & 4 \\ 4 & 5 \end{vmatrix} \cdot (-1)^9 + \begin{vmatrix} 2 & 8 \\ 3 & 2 \end{vmatrix} \cdot \begin{vmatrix} 1 & 3 \\ 4 & 7 \end{vmatrix} \cdot (-1)^{10} +$$
$$\begin{vmatrix} 0 & 0 \\ 0 & 0 \end{vmatrix} \cdot \begin{vmatrix} 1 & 4 \\ 4 & 5 \end{vmatrix} \cdot (-1)^{10} + \begin{vmatrix} 0 & 8 \\ 0 & 2 \end{vmatrix} \cdot \begin{vmatrix} 1 & 3 \\ 4 & 7 \end{vmatrix} \cdot (-1)^{11} + \begin{vmatrix} 0 & 8 \\ 0 & 2 \end{vmatrix} \cdot \begin{vmatrix} 1 & 1 \\ 4 & 4 \end{vmatrix} \cdot (-1)^{12} =$$
$$\begin{vmatrix} 2 & 8 \\ 3 & 2 \end{vmatrix} \cdot \begin{vmatrix} 1 & 3 \\ 4 & 7 \end{vmatrix} = (-20) \cdot (-5) = 100.$$

2. Spočtěme tentýž determinant rozvinutím podle 1. sloupce. Pak:

$$|A| = 1 \cdot \begin{vmatrix} 0 & 0 & 8 \\ 0 & 0 & 2 \\ 4 & 7 & 5 \end{vmatrix} \cdot (-1)^2 + 2 \cdot \begin{vmatrix} 1 & 3 & 4 \\ 0 & 0 & 2 \\ 4 & 7 & 5 \end{vmatrix} \cdot (-1)^3 + 3 \cdot \begin{vmatrix} 1 & 3 & 4 \\ 0 & 0 & 8 \\ 4 & 7 & 5 \end{vmatrix} \cdot (-1)^4 + 4 \cdot \begin{vmatrix} 1 & 3 & 4 \\ 0 & 0 & 8 \\ 0 & 0 & 2 \end{vmatrix} \cdot (-1)^5 = 0 - 2 \cdot 10 + 3 \cdot 40 + 0 = 100.$$

§3. Algebra matic

V tomto paragrafu se nejprve vrátíme k maticím typu m/n (tj. obecně k obdélníkovým maticím) a ukážeme si některé algebraické struktury, které lze pomocí matic utvořit. Budeme předpokládat, že všechny matice jsou uvažovány nad pevným číselným tělesem T (nebude-li výslovně řečeno jinak).

Označení. Všude v dalším budeme symbolem $\mathrm{Mat}_{mn}(T)$ označovat množinu všech matic typu m/n nad pevným číselným tělesem T. Napíšeme-li tedy, že $A \in \mathrm{Mat}_{mn}(T)$, pak to bude znamenat, že A je matice typu m/n nad tělesem T.

Definice. Nechť $A = (a_{ij}), B = (b_{ij}) \in \mathrm{Mat}_{mn}(T)$, $t \in T$ libovolné. Pak:
(1) matice $A + B = (c_{ij}) \in \mathrm{Mat}_{mn}(T)$ definovaná:

$$c_{ij} = a_{ij} + b_{ij}$$

pro $i = 1, \ldots, m$, $j = 1, \ldots, n$ se nazývá *součet matic* A, B,
(2) matice $t \cdot A = (d_{ij}) \in \mathrm{Mat}_{mn}(T)$ definovaná:

$$d_{ij} = t \cdot a_{ij}$$

pro $i = 1, \ldots, m$, $j = 1, \ldots, n$ se nazývá *součin čísla* t *s maticí* A.

Vidíme, že součet matic je definován pouze pro matice stejného typu, přičemž pak sčítáme „odpovídající si prvky obou matic“. Sčítání matic je zřejmě operací na množině $\mathrm{Mat}_{mn}(T)$. Podobně, při součinu čísla s maticí násobíme tímto číslem každý prvek dané matice. Součin čísla s maticí tedy můžeme chápat jako vnější operaci.

Věta 3.1. $(\mathrm{Mat}_{mn}(T), +)$ *je komutativní grupa.*

Důkaz. Z předchozí definice a ze známých vlastností obyčejného sčítání čísel plyne, že $(\mathrm{Mat}_{mn}(T), +)$ je pologrupa, která je komutativní. Lehce se ověří, že nulová matice 0_{mn} je nulou, resp. pro libovolnou matici $A = (a_{ij}) \in \mathrm{Mat}_{mn}(T)$ je matice $(-a_{ij}) \in \mathrm{Mat}_{mn}(T)$ opačným prvkem k A. Označujeme $(-a_{ij}) = -A$. Tedy $(\mathrm{Mat}_{mn}(T), +)$ je komutativní grupa. □

Věta 3.2. *Množina* $\mathrm{Mat}_{mn}(T)$ *je vektorový prostor nad* T *(vzhledem k operacím sčítání matic a součinu čísla s maticí), jehož dimenze je rovna* $m \cdot n$.

Důkaz. Podle předchozí věty je $(\mathrm{Mat}_{mn}(T), +)$ komutativní grupou. Dále, rozepsáním se lehce ověří platnost vztahů:
(1) $t \cdot (A + B) = t \cdot A + t \cdot B$,
(2) $(t + s) \cdot A = t \cdot A + s \cdot A$,
(3) $(t \cdot s) \cdot A = t \cdot (s \cdot A)$,
(4) $1 \cdot A = A$
pro lib. $t, s \in T$ a $A, B \in \mathrm{Mat}_{mn}(T)$. Tedy z definice vektorového prostoru plyne, že $\mathrm{Mat}_{mn}(T)$ je vektorový prostor nad T (roli vektorů hrají tedy matice typu m/n nad T).

Zbývá ukázat, že $\dim \mathrm{Mat}_{mn}(T) = m \cdot n$, což provedeme tak, že zkonstruujeme bázi vektorového prostoru $\mathrm{Mat}_{mn}(T)$. Pro $r = 1, \dots, m$, $s = 1, \dots, n$ označme symbolem U_{rs} matici typu m/n, která má na r, s-tém místě (tj. v r-tém řádku a s-tém sloupci) jedničku a všude jinde samé nuly. Tedy:

$$U_{rs} = (u_{ij}) \text{ typu } m/n, \text{ kde } u_{ij} = \begin{cases} 1 & \text{pro } i = r,\ j = s \\ 0 & \text{jinak} \end{cases}$$

Dostáváme tak celkem $m \cdot n$ matic $U_{11}, \dots, U_{1n}, U_{21}, \dots, U_{2n}, \dots, U_{m1}, \dots, U_{mn}$, o nichž se rozepsáním lehce ukáže (proveďte si podrobně sami!), že jsou lineárně nezávislé a že generují celý prostor $\mathrm{Mat}_{mn}(T)$, tzn. jsou jeho bází.

□

Definice. Nechť $A = (a_{ij})$ je matice typu m/n, $B = (b_{ij})$ je matice typu n/p (obě nad týmž tělesem T). Pak matice $A \cdot B = (c_{ij})$ typu m/p, kde:

$$c_{ij} = \sum_{k=1}^{n} a_{ik} \cdot b_{kj},$$

pro $i = 1, \dots, m$, $j = 1, \dots, p$, se nazývá *součin matic* A, B (v tomto pořadí).

Příklad 3.1. Nechť A, B jsou matice nad $\mathbb{R}$ tvaru:

$$A = \begin{pmatrix} 1 & 2 & -1 & 0 \\ 0 & 1 & -1 & -7 \\ -8 & 0 & 0 & -5 \end{pmatrix}, \quad B = \begin{pmatrix} 3 & 2 \\ -4 & 1 \\ 1 & 0 \\ -2 & -3 \end{pmatrix}.$$

Pak:

$$A \cdot B = \begin{pmatrix} -6 & 4 \\ 9 & 22 \\ -14 & -1 \end{pmatrix},$$

resp. součin $B \cdot A$ není vůbec definován.

Poznámka. Při násobení dvou matic A, B zřejmě podstatně záleží na jejich pořadí. Z předchozího příkladu vidíme, že se může stát, že součin $A \cdot B$ je definován, kdežto součin $B \cdot A$ definován není. Ale i v případě, že oba součiny $A \cdot B$ a $B \cdot A$ jsou definovány a jsou stejného typu (tzn. A, B jsou čtvercové matice stejného typu), neznamená to, že $A \cdot B = B \cdot A$, jak je vidět z následujícího příkladu.

Příklad 3.2. Nechť $n \geq 2$ a A, B jsou čtvercové matice řádu n (nad T) tvaru:

$$A = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Pak přímým výpočtem zjistíme, že $A \cdot B = 0_{nn}$, kdežto $B \cdot A = B$, což znamená, že $A \cdot B \neq B \cdot A$.

Vidíme tedy, že násobení matic obecně není komutativní. Na druhé straně, násobení matic je však asociativní a násobení matic je distributivní vzhledem ke sčítání matic (samozřejmě za předpokladu, že všechny použité součty a součiny matic jsou definovány), jak ukazují následující dvě věty.

Věta 3.3. *Násobení matic je asociativní, tj. nechť matice A je typu m/n, B je typu n/p a C je typu p/q. Potom platí:*

$$A \cdot (B \cdot C) = (A \cdot B) \cdot C.$$

Důkaz. Nechť platí předpoklady věty, přičemž $A = (a_{ij})$, $B = (b_{ij})$, $C = (c_{ij})$. Pak matice $A \cdot B = (d_{ij})$ je typu m/p, přičemž $d_{ij} = \sum\limits_{u=1}^{n} a_{iu} \cdot b_{uj}$. Dále pak $(A \cdot B) \cdot C = (f_{ij})$ je matice typu m/q, kde $f_{ij} = \sum\limits_{v=1}^{p} d_{iv} \cdot c_{vj} = \sum\limits_{v=1}^{p} \sum\limits_{u=1}^{n} a_{iu} \cdot b_{uv} \cdot c_{vj}$, přičemž v posledním výrazu není třeba v součinu za sumačními znaky závorkovat, neboť se jedná o součin čísel (z T), pro který platí asociativní zákon.

Podobně, matice $B \cdot C = (g_{ij})$ je typu n/q, kde $g_{ij} = \sum\limits_{v=1}^{p} b_{iv} \cdot c_{vj}$. Dále pak $A \cdot (B \cdot C) = (h_{ij})$ je matice typu m/q, kde:

$$h_{ij} = \sum_{u=1}^{n} a_{iu} \cdot g_{uj} = \sum_{u=1}^{n} a_{iu} \cdot \sum_{v=1}^{p} b_{uv} \cdot c_{vj} = \sum_{v=1}^{p} \sum_{u=1}^{n} a_{iu} \cdot b_{uv} \cdot c_{vj} = f_{ij}.$$

Dohromady tedy platí dokazovaná rovnost. □

Věta 3.4. *Násobení matic je distributivní vzhledem ke sčítání matic, tj.:*

(1) *Nechť matice A je typu m/n, resp. B, C jsou typu n/p. Potom platí:*

$$A \cdot (B + C) = A \cdot B + A \cdot C.$$

(2) *Nechť matice F, G jsou typu m/n, resp. H je typu n/p. Potom platí:*

$$(F + G) \cdot H = F \cdot H + G \cdot H.$$

Důkaz. (1): Nechť $A = (a_{ij})$ je typu m/n, resp. $B = (b_{ij})$, $C = (c_{ij})$ jsou typu n/p. Potom $A \cdot (B + C) = (d_{ij})$ je matice typu m/p, přičemž $d_{ij} = \sum\limits_{k=1}^{n} a_{ik} \cdot (b_{kj} + c_{kj})$. Dále, matice $A \cdot B + A \cdot C = (f_{ij})$ je matice typu m/p a platí:

$$f_{ij} = \sum_{k=1}^{n} a_{ik} \cdot b_{kj} + \sum_{k=1}^{n} a_{ik} \cdot c_{kj} = \sum_{k=1}^{n} a_{ik} \cdot (b_{kj} + c_{kj}) = d_{ij}.$$

Dohromady tedy platí (1).

(2): Dokáže se analogickým způsobem jako (1). □

Definice. Čtvercová matice řádu n (nad T) tvaru:

$$E_n = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

(tj. matice mající v hlavní diagonále samé jedničky a všude jinde samé nuly) se nazývá *jednotková matice* (řádu n).

Věta 3.5. *Množina všech čtvercových matic řádu n (nad T) s operacemi sčítání matic a násobení matic, tj.* $(\mathrm{Mat}_{nn}(T), +, \cdot)$, *je okruhem s jedničkou.*

Tento okruh pro $n \geq 2$ není komutativní a obsahuje dělitele nuly.

Důkaz. Je zřejmé, že sčítání matic, resp. násobení matic jsou operace na množině $\mathrm{Mat}_{nn}(T)$. Z vět 3.1., 3.3. a 3.4. pak ihned plyne, že $(\mathrm{Mat}_{nn}(T), +, \cdot)$ je okruh. Dále, pro libovolnou matici $A \in \mathrm{Mat}_{nn}(T)$ zřejmě platí (ověřte si rozepsáním!), že:

$$E_n \cdot A = A \cdot E_n = A,$$

a tedy jednotková matice E_n je jedničkou okruhu $(\mathrm{Mat}_{nn}(T), +, \cdot)$.

Z příkladu 3.2. pak plyne, že pro $n \geq 2$ tento okruh není komutativní a obsahuje dělitele nuly (nulou je zde zřejmě nulová matice řádu n, tzn. 0_{nn}). □

Poznamenejme, že okruh $(\mathrm{Mat}_{nn}(T), +, \cdot)$, stručně též nazývaný „okruh matic“, je jedním z nejjednodušších příkladů nekomutativního okruhu.

Věta 3.6. *Nechť $A = (a_{ij})$ je matice typu m/n, $B = (b_{ij})$ je matice typu n/p. Pak platí:*

$$(A \cdot B)' = B' \cdot A'$$

(tj. transponovaná matice k součinu matic je rovna součinu transponovaných matic v opačném pořadí).

Důkaz. Matice $(A \cdot B)' = (c_{ij})$ je typu p/m, přičemž c_{ij} je prvek stojící v matici $A \cdot B$ v j-tém řádku a i-tém sloupci, tzn. $c_{ij} = \sum_{k=1}^{n} a_{jk} \cdot b_{ki}$. Dále pak matice $B' \cdot A' = (d_{ij})$ je typu p/m, kde $d_{ij} = \sum_{k=1}^{n} b_{ki} \cdot a_{jk} = \sum_{k=1}^{n} a_{jk} \cdot b_{ki} = c_{ij}$, a tedy platí dokazovaná rovnost. $\square$

Věta 3.7. (Cauchyova věta) *Nechť $A = (a_{ij})$, $B = (b_{ij})$ jsou čtvercové matice řádu n. Pak platí:*

$$|A \cdot B| = |A| \cdot |B|.$$

Důkaz. Uvažme matici H řádu $2n$ tvaru:

$$H = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & 0 & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & a_{2n} & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} & 0 & 0 & \cdots & 0 \\ -1 & 0 & \cdots & 0 & b_{11} & b_{12} & \cdots & b_{1n} \\ 0 & -1 & \cdots & 0 & b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 & b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix}.$$

Užitím Laplaceovy věty (a sice rozvinutím podle prvních n řádků) dostáváme:

$$|M| = |A| \cdot |B|. \tag{1}$$

Nyní ke každému z posledních n sloupců přičteme vhodnou kombinaci prvních n sloupců tak, aby na místě každého b_{ij} vznikla nula (přesněji řečeno: k $(n + j)$-tému sloupci přičteme b_{1j}-krát 1. sloupec $+ \cdots +$ b_{nj}-krát n-tý sloupec, pro $j = 1, \ldots, n$). Dostáváme tak matici:

$$K = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & c_{11} & c_{12} & \cdots & c_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} & c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} & c_{n1} & c_{n2} & \cdots & c_{nn} \\ -1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & -1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 & 0 & 0 & \cdots & 0 \end{pmatrix},$$

v níž $c_{ij} = a_{i1} \cdot b_{1j} + \cdots + a_{in} \cdot b_{nj} = \sum\limits_{k=1}^{n} a_{ik} \cdot b_{kj}$, pro $i, j = 1, \ldots, n$. Při tomto označení je tedy $(c_{ij}) = A \cdot B$. Rozvinutím podle posledních n sloupců matice K pak dostáváme:

$$|K| = |A \cdot B| \cdot (-1)^n \cdot (-1)^{1+\cdots+n+(n+1)+\cdots+2n} = |A \cdot B| \cdot (-1)^{2 \cdot n \cdot (n+1)} = |A \cdot B|. \tag{2}$$

Ale úpravy, pomocí nichž jsme z matice H dostali matici K, nemění hodnotu determinantu (podle věty 2.5. (2) zformulované pro sloupce), a tedy $|H| = |K|$, odkud pomocí (1) a (2) dostáváme:

$$|A| \cdot |B| = |A \cdot B|,$$

což je žádané tvrzení. □

Definice. Čtvercová matice A se nazývá *regulární matice* (resp. *singulární matice*), je-li $|A| \neq 0$ (resp. $|A| = 0$).

Důsledek. *Nechť A, B jsou čtvercové matice stejného řádu n. Pak platí: matice $A \cdot B$ je regulární $\iff$ obě matice A i B jsou regulární.*

Důkaz. Tvrzení plyne přímo z definice regulární matice a z Cauchyovy věty. □

Definice. Nechť A je čtvercová matice řádu n. Matice X s vlastností:

$$A \cdot X = E_n \ \wedge \ X \cdot A = E_n \tag{3}$$

(pokud taková existuje) se nazývá *inverzní matice* k matici A a označuje se symbolem A^{-1}.

Poznámka. Z (3) především plyne, že inverzní matice (pokud existuje) musí být také čtvercová a řádu n. Dále, vzhledem k tomu, že $(\mathrm{Mat}_{nn}(T), \cdot)$ je pologrupa s jedničkou E_n (viz věta 3.5.) a pojem inverzní matice je totožný s pojmem inverzního prvku v této pologrupě, může k matici A existovat nejvýše jedna inverzní matice (podle V.1.3., kap. II.) a označení A^{-1} je tedy korektní. Následující věta a její důsledek nám pak udává nutnou a dostatečnou podmínku existence inverzní matice a vzorec pro její výpočet.

Věta 3.8. *Nechť $A = (a_{ij})$ je čtvercová matice řádu n. Potom platí: k matici A existuje matice inverzní $\iff$ A je regulární matice.*

Důkaz. „$\Rightarrow$“: Nechť k A existuje inverzní matice A^{-1}. Pak platí $E_n = A \cdot A^{-1}$, odkud $1 = |E_n| = |A \cdot A^{-1}| = |A| \cdot |A^{-1}|$. Pak ale je $|A| \neq 0$, a tedy A je regulární matice.

„$\Leftarrow$“: Nechť A je regulární matice, tzn. $|A| \neq 0$. Označme:

$$A^* = \begin{pmatrix} A_{11} & A_{21} & \cdots & A_{n1} \\ A_{12} & A_{22} & \cdots & A_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ A_{1n} & A_{2n} & \cdots & A_{nn} \end{pmatrix}$$

matici, v níž na i, j-tém místě je A_{ji} (pozor na pořadí indexů!), tzn. algebraický doplněk prvku stojícího na j, i-tém místě v původní matici A. Poznamenejme, že matice A^* se nazývá *adjungovaná matice* k matici A.

Nyní dokážeme, že matice $X = \frac{1}{|A|} \cdot A^*$ je inverzní maticí k matici A. Nechť $A \cdot X = (c_{ij})$, tzn. $c_{ij} = \frac{1}{|A|} \cdot \sum_{k=1}^{n} a_{ik} \cdot A_{jk}$. Potom ale:

- pro $i = j$ je $c_{ii} = \frac{1}{|A|} \cdot \sum_{k=1}^{n} a_{ik} \cdot A_{ik} = \frac{1}{|A|} \cdot |A| = 1$ (užitím důsledku Laplaceovy věty),
- pro $i \neq j$ je $c_{ij} = \frac{1}{|A|} \cdot \sum_{k=1}^{n} a_{ik} \cdot A_{jk} = \frac{1}{|A|} \cdot 0 = 0$ (výraz $\sum_{k=1}^{n} a_{ik} \cdot A_{jk}$ je roven nule, neboť podle důsledku Laplaceovy věty se jedná o determinant matice, v níž i-tý a j-tý řádek jsou stejné).

Vidíme tedy, že $A \cdot X = (c_{ij}) = E_n$.

Analogickou úvahou se zjistí, že $X \cdot A = E_n$, tzn. dohromady dostáváme, že $X = A^{-1}$, a tedy k matici A existuje matice inverzní. $\square$

Důsledek. *Nechť A je regulární matice. Pak $A^{-1} = \left(\frac{1}{|A|}\right) \cdot A^*$.*

Důkaz. Tvrzení plyne ihned z 2. části důkazu předchozí věty. $\square$

Některé jednoduché základní vlastnosti inverzních matic, resp. regulárních matic nám popisují následující dvě věty.

Věta 3.9. *Nechť A, B jsou regulární matice řádu n. Pak platí:*

(1) $(A^{-1})^{-1} = A$,

(2) $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$,
(3) $|A^{-1}| = \frac{1}{|A|}$,
(4) $(A')^{-1} = (A^{-1})'$.

Důkaz. (1) a (2) plynou z věty 1.4., kap. II., a z věty 3.8., uvědomíme-li si, že $(\mathrm{Mat}_{nn}(T), \cdot)$ je pologrupa s jedničkou.

(3): Zřejmě $A \cdot A^{-1} = E_n$, odkud podle Cauchyovy věty je $|A| \cdot |A^{-1}| = |E_n| = 1$, tzn. $|A^{-1}| = \frac{1}{|A|}$.

(4): Podle věty 3.6. je $(A^{-1})' \cdot A' = (A \cdot A^{-1})' = E_n' = E_n$ a analogicky též $A' \cdot (A^{-1})' = E_n$, tzn. podle (3) je $(A^{-1})'$ inverzní maticí k matici A', neboli platí (4). □

Věta 3.10. *Nechť $\overline{\mathrm{Mat}_{nn}(T)}$ značí množinu všech regulárních matic řádu n (nad T). Pak $(\overline{\mathrm{Mat}_{nn}(T)}, \cdot)$ je grupa, která je pro $n \geq 2$ nekomutativní.*

Důkaz. Zřejmě $E_n \in \overline{\mathrm{Mat}_{nn}(T)}$. Podle důsledku Cauchyovy věty a podle vět 3.3. a 3.8. ihned dostáváme, že $(\overline{\mathrm{Mat}_{nn}(T)}, \cdot)$ je grupa.

Dále nechť $n \geq 2$. Vezměme matice A, B řádu n tvaru:

$$A = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & 1 \\ 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ \vdots & \vdots & ⋰ & \vdots & \vdots & \vdots \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix}.$$

Potom zřejmě A, B jsou regulární, tj. $A, B \in \overline{\mathrm{Mat}_{nn}(T)}$ a platí $A \cdot B \neq B \cdot A$ (ověřte si výpočtem!). Tedy uvažovaná grupa není komutativní. □

Multiplikativní grupa regulárních matic řádu n ($n \geq 2$) je dalším poměrně jednoduchým příkladem nekomutativní grupy.

Poznámka. Všimněme si, že z věty 3.8. bezprostředně plyne, že při praktickém ověřování, zda matice X je inverzní maticí k A, stačí ověřovat pouze jednu z rovností (3), tzn. rovností:

$$A \cdot X = E_n,$$
$$X \cdot A = E_n,$$

poněvadž druhá rovnost je již vynucena. (Je-li např. $A \cdot X = E_n$, pak A je regulární a existuje matice A^{-1}. Pak vynásobením výchozího vztahu zleva maticí A^{-1} a zprava maticí A dostáváme: $A^{-1} \cdot (A \cdot X) \cdot A = A^{-1} \cdot E_n \cdot A$, tzn. po úpravě: $X \cdot A = E_n$.)

§4. Hodnost matice

V tomto paragrafu bude $A = (a_{ij})$ značit matici typu m/n nad číselným tělesem T, tzn.:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix},$$

kde $a_{ij} \in T$. Jak již bylo dříve řečeno, řádky matice A můžeme chápat jako vektory z vektorového prostoru T^n. Potom vektory – řádky matice A generují v T^n jistý podprostor W a my se v dalším budeme zajímat o jeho dimenzi.

Podobně, sloupce matice A lze chápat též jako vektory – tentokrát z vektorového prostoru T^m, přičemž tyto vektory – sloupce matice A generují v T^m jistý podprostor H. Je samozřejmé, že T^n a T^m jsou obecně dva zcela rozdílné vektorové prostory a totéž platí i o podprostorech W a H. Přesto však ukážeme, že dimenze obou těchto podprostorů musí být stejné, tzn. $\dim W = \dim H$.

Definice. Nechť $A = (a_{ij})$ je matice typu m/n nad T. Pak dimenze vektorového podprostoru v T^n generovaného řádky matice A se nazývá *hodnost matice* A a označuje se symbolem $h(A)$.

Věta 4.1. *Hodnost matice je rovna maximálnímu počtu jejích lineárně nezávislých řádků.*

Důkaz. Tvrzení plyne ihned z definice hodnosti matice, definice dimenze, definice báze a z věty 4.1., kap. I. □

Poznámka. Z předchozího je zřejmé, že hodnost matice A je rovna nule, právě když A je nulovou maticí. Je-li tedy matice A nenulová, pak její hodnost je rovna některému přirozenému číslu.

Další možnost vyjádření hodnosti matice nám ukáže následující věta. Poznamenejme k ní ještě to, že pojem minoru řádu k matice A lze zřejmě stejným způsobem jako v §2 definovat i pro libovolnou (obecně obdélníkovou) matici A typu m/n za předpokladu, že $k \leq \min\{m, n\}$. Je-li však $m \neq n$, nelze pak již samozřejmě hovořit o doplňku tohoto minoru.

Věta 4.2. *Nechť A je nenulová matice typu m/n. Pak hodnost matice A je rovna maximálnímu z řádů nenulových minorů matice A.*

Důkaz. Nechť $A = (a_{ij})$ je nenulová matice typu m/n. Pak zřejmě existuje minor $|M|$ řádu $k > 0$ tak, že $|M| \neq 0$ a všechny minory řádu většího než k (pokud vůbec existují) jsou rovny nule. Bez újmy na obecnosti lze předpokládat, že submatice M je určena prvními k řádky a prvními k sloupci matice A. Chceme nyní dokázat, že $h(A) = k$. Ale platí:

α) Prvních k řádků matice A je lineárně nezávislých.

V opačném případě by byly i řádky submatice M lineárně závislé a podle věty 3.2., kap. I., resp. věty 2.4. by byl $|M| = 0$, což je spor.

β) r-tý řádek ($k < r \leq m$) matice A je lineární kombinací prvních k řádků.

Nechť tedy $k < r \leq m$ a nechť $1 \leq j \leq n$ libovolné. Utvořme matici:

$$D_j = \begin{pmatrix} a_{11} & \cdots & a_{1k} & a_{1j} \\ \vdots & \ddots & \vdots & \vdots \\ a_{k1} & \cdots & a_{kk} & a_{kj} \\ a_{r1} & \cdots & a_{rk} & a_{rj} \end{pmatrix}$$

tak, že matici M „ovroubíme" odpovídajícími prvky r-tého řádku a j-tého sloupce matice A. Determinant $|D_j|$ je zřejmě roven nule, neboť pro $j > k$ je $|D_j|$ minorem řádu $k+1$, resp. pro $j \leq k$ obsahuje matice D_j dva stejné sloupce. Rozviňme nyní $|D_j|$ podle posledního sloupce. Dostáváme:

$$0 = |D_j| = a_{1j} \cdot L_1 + a_{2j} \cdot L_2 + \cdots + a_{kj} \cdot L_k + a_{rj} \cdot |M|,$$

kde L_i ($i = 1, \ldots, k$) jsou algebraické doplňky prvků posledního sloupce (uvědomme si, že L_i nezávisí na j). Poněvadž $|M| \neq 0$, můžeme psát:

$$a_{rj} = -\tfrac{L_1}{|M|} \cdot a_{1j} - \cdots - \tfrac{L_k}{|M|} \cdot a_{kj}$$

pro každé $j = 1, 2, \ldots, n$, což však znamená, že r-tý řádek je lineární kombinací prvních k řádků.

Z α) a β) plyne, že maximální počet lineárně nezávislých řádků matice A je roven číslu k, a tedy podle věty 4.1. je $h(A) = k$. $\square$

Důsledek. *Transponováním matice se její hodnost nezmění, tj.* $h(A) = h(A')$.

Důkaz. Je-li A nulová matice, pak A' je též nulová matice a tvrzení platí. Nechť tedy A je nenulová matice a nechť $h(A) = k$. Pak podle předchozí věty existuje v A nenulový minor řádu k a všechny minory řádu většího než k jsou rovny nule. Uvažme nyní transponovanou matici A'. Vzhledem k tomu, že transponováním se nemění hodnoty minorů (plyne z věty 2.1.), existuje tedy i v matici A' nenulový minor řádu k a všechny minory řádu většího než k v A' jsou rovny nule. To ale znamená (opět podle předchozí věty), že $h(A') = k$, a tedy $h(A) = h(A')$. $\square$

Věta 4.3. *Hodnost matice je rovna maximálnímu počtu jejích lineárně nezávislých sloupců.*

Důkaz. Podle předchozího důsledku a podle věty 4.1. je hodnost matice A rovna maximálnímu počtu lineárně nezávislých řádků transponované matice A', tj. maximálnímu počtu lineárně nezávislých sloupců původní matice A. $\square$

Z předchozích tvrzení již vyplývá to, o čem jsme hovořili na začátku paragrafu, a sice je-li matice A matice typu m/n, pak dimenze podprostoru (v T^n) generovaného řádky matice A je rovna dimenzi podprostoru (v T^m) generovaného sloupci matice A.

V dalším si nejprve všimneme případu, kdy matice A je čtvercová.

Věta 4.4. *Nechť A je čtvercová matice řádu n. Pak následující výroky jsou ekvivalentní:*

(1) *matice A je regulární,*
(2) $h(A) = n$,
(3) *řádky matice A jsou lineárně nezávislé,*
(4) *sloupce matice A jsou lineárně nezávislé.*

Důkaz. „(1) $\Rightarrow$ (2)“: Nechť A je regulární, tzn. $|A| \neq 0$. Pak z věty 4.2. plyne, že $h(A) = n$.

„(2) $\Rightarrow$ (3)“: Plyne z věty 4.1.

„(3) $\Rightarrow$ (4)“: Plyne z vět 4.1. a 4.3.
„(4) $\Rightarrow$ (1)“: Plyne z vět 4.3. a 4.2. $\square$

Předchozí věta nám samozřejmě zároveň podává i charakterizaci singulární matice. Provedením obměn všech implikací totiž dostáváme, že ekvivalentní jsou též výroky:
(1) matice A je singulární,
(2) $h(A) < n$,
(3) řádky matice A jsou lineárně závislé,
(4) sloupce matice A jsou lineárně závislé.

Věta 4.5. *Nechť A je matice typu m/n. Pak platí:*
(1) *je-li B matice typu n/p, pak:*

$$h(A \cdot B) \leq h(A) \quad a \quad h(A \cdot B) \leq h(B),$$

(2) *je-li R (resp. S) regulární čtvercová matice řádu n (resp. řádu m), pak:*

$$h(A \cdot R) = h(A) \quad a \quad h(S \cdot A) = h(A).$$

Důkaz. (1): Nechť $A = (a_{ij})$, $B = (b_{ij})$. Označme $A \cdot B = (c_{ij})$ a dále označme:

$$D = \begin{pmatrix} a_{11} & \cdots & a_{1n} & c_{11} & \cdots & c_{1p} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} & c_{m1} & \cdots & c_{mp} \end{pmatrix}.$$

Matici D můžeme chápat jakožto matici A, k níž bylo přidáno jistých p sloupců. Ale poněvadž:

$$c_{ij} = \sum_{k=1}^{n} a_{ik} \cdot b_{kj} = b_{1j} \cdot a_{i1} + b_{2j} \cdot a_{i2} + \cdots + b_{nj} \cdot a_{in}$$

pro pevné j a $i = 1, \ldots, m$, vidíme, že přidané sloupce jsou vždy lineární kombinací prvních n sloupců, a tedy je $h(D) = h(A)$.

Matici D však můžeme též chápat jako matici $A \cdot B$, k níž jsme (zleva) přidali jistých n sloupců, tzn. pak zřejmě platí $h(A \cdot B) \leq h(D)$. Dohromady dostáváme, že $h(A \cdot B) \leq h(A)$.

Analogickým způsobem (přidáním všech řádků matice $A \cdot B$ k řádkům matice B) se dokáže, že $h(A \cdot B) \leq h(B)$.

(2): Podle právě dokázané části (1) je $h(A \cdot R) \leq h(A)$. Ale zřejmě $A = (A \cdot R) \cdot R^{-1}$, a tedy opět podle (1) je $h(A) = h((A \cdot R) \cdot R^{-1}) \leq h(A \cdot R)$. Dohromady pak dostáváme, že $h(A \cdot R) = h(A)$.

Druhá část tvrzení (2) se dokáže analogicky. □

§5. Další vlastnosti a užití matic

V první části tohoto paragrafu si odvodíme jednoduché metody výpočtu hodnosti matice, resp. výpočtu inverzní matice a ukážeme si některé možnosti aplikací těchto postupů při řešení úloh o vektorových prostorech.

Definice. Nechť A je matice typu m/n nad tělesem T. Pak každá z následujících úprav matice A se nazývá *elementární řádková úprava matice* A:

(1) libovolná záměna pořadí řádků,
(2) vynásobení libovolného řádku nenulovým číslem z T,
(3) k jednomu řádku přičtení jiného řádku vynásobeného libovolným číslem z T.

Poznámka. Řekli jsme si, že řádky matice A budeme chápat jako vektory z vektorového prostoru T^n. V tomto smyslu pak elementární řádkové úpravy matice A chápeme jako výše popsané manipulace s vektory z T^n.

Řádky matice A generují ve vektorovém prostoru T^n jistý podprostor W. Důležité je (jak ukáže následující věta), že provedení elementární řádkové úpravy neovlivní tento podprostor W.

Věta 5.1. *Nechť A je matice typu m/n nad T a nechť matice B vznikne z matice A provedením elementární řádkové úpravy. Pak podprostor (ve vektorovém prostoru T^n) generovaný řádky matice A je roven podprostoru generovanému řádky matice B.*

Důkaz. Řádky matice A (chápané jako vektory ve vektorovém prostoru T^n) označme $\boldsymbol{u}_1, \dots, \boldsymbol{u}_m$. Podle věty 3.1. (2), kap. I., je podprostor generovaný řádky matice A roven množině všech lineárních kombinací těchto řádků, tzn.:

$$[\boldsymbol{u}_1, \dots, \boldsymbol{u}_m] = L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_m).$$

Podprostor $[\boldsymbol{u}_1, \dots, \boldsymbol{u}_m]$ se nezmění, jestliže:

α) zaměníme libovolně pořadí řádků matice A,
neboť zřejmě $L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_m) = L(\boldsymbol{u}_{i_1}, \dots, \boldsymbol{u}_{i_m})$, kde $(i_1, \dots, i_m)$ je libovolné pořadí indexů $1, \dots, m$,

β) vynásobíme i-tý řádek matice A nenulovým číslem $t \in T$,
neboť $L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_i, \dots, \boldsymbol{u}_m) = L(\boldsymbol{u}_1, \dots, t \cdot \boldsymbol{u}_i, \dots, \boldsymbol{u}_m)$, jak se lehce ověří rozepsáním,

γ) přičteme k i-tému řádku matice A t-násobek j-tého řádku $(i \neq j)$,
neboť $L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_i, \dots, \boldsymbol{u}_m) = L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_i + t \cdot \boldsymbol{u}_j, \dots, \boldsymbol{u}_m)$, jak se opět ověří rozepsáním.

Ukázali jsme tedy, že podprostor $[\boldsymbol{u}_1, \dots, \boldsymbol{u}_m]$ v T^n se nezmění provedením libovolné elementární řádkové úpravy matice A. $\square$

Důsledek. *Provedení libovolné elementární řádkové úpravy matice A nezmění hodnost matice A.*

Důkaz. Tvrzení plyne bezprostředně z definice hodnosti matice a z předchozí věty. $\square$

Z předchozích úvah vyplývá, že při praktickém zjišťování hodnosti dané matice A bude zřejmě výhodné pomocí elementárních řádkových úprav (které nemění hodnost) převést matici A na nějaký „jednoduchý tvar“, z něhož již hodnost okamžitě určíme. Tento „jednoduchý tvar“ popisuje následující definice.

Definice. Nechť A je matice typu m/n. Řekneme, že A je *matice ve schodovitém tvaru*, jestliže v matici A každý nenulový řádek začíná větším počtem nul než předchozí řádek.

Poznámka. Rozebereme-li si podrobněji předchozí definici, pak vidíme, že:

1. Libovolná matice typu $1/n$, tj. matice sestávající pouze z jednoho řádku, je vždy ve schodovitém tvaru.

2. Je-li matice A ve schodovitém tvaru, pak případné nulové řádky musí být v matici A umístěny „dole“. Specielně, nulová matice 0_{mn} je zřejmě zvláštním případem matice ve schodovitém tvaru.

3. Je-li nenulová matice A ve schodovitém tvaru, pak svým tvarem skutečně odpovídá tomuto názvu, neboť nuly v matici A tvoří jakési „schody“. Přitom první řádek může, ale nemusí začínat nulou (resp. nulami), druhý řádek však již musí začínat alespoň jednou nulou, třetí řádek musí začínat alespoň dvěma nulami, atd. Schématicky znázorněna vypadá nenulová matice A ve schodovitém tvaru takto:

$$A = \begin{pmatrix} 0 \cdot\cdot\, 0\ a_{1j_1} \cdots\cdots\cdots\cdots\cdots\cdots & a_{1n} \\ 0 \cdots\cdots\, 0\ a_{2j_2} \cdots\cdots\cdots\cdots\cdots & a_{2n} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & \\ 0 \cdots\cdots\cdots\cdots 0\ a_{kj_k} \cdots\cdots\cdots & a_{kn} \\ 0 \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & \\ 0 \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & 0 \end{pmatrix},$$

kde $1 \leq j_1 < j_2 < \cdots < j_k \leq n$, resp. $1 \leq k \leq \min\{m,n\}$, resp. $a_{ij_i} \neq 0$ pro $i = 1, 2, \ldots, k$.

Věta 5.2. *Každou matici lze konečným počtem elementárních řádkových úprav převést na schodovitý tvar.*

Důkaz. Nechť $A = (a_{ij})$ je matice typu m/n. Je-li A nulová matice, pak je již ve schodovitém tvaru a jsme hotovi. Nechť tedy A je nenulová matice. Důkaz nyní provedeme matematickou indukcí vzhledem k m (tj. vzhledem k počtu řádků matice A).

α) Pro $m = 1$ je matice A již ve schodovitém tvaru a tvrzení platí.

β) Předpokládejme, že každou matici o $1, 2, \ldots, m$ řádcích lze konečným počtem elementárních řádkových úprav převést na schodovitý tvar. Nechť nyní A je matice o $(m+1)$ řádcích. Nechť s-tý sloupec je prvním nenulovým sloupcem matice A. Pak případnou výměnou dvou řádků dostaneme z matice A matici $B = (b_{ij})$, která má v 1. řádku a s-tém sloupci nenulový prvek $b_{1s} \neq 0$. Nyní k i-tému řádku matice B přičteme $\left(-\frac{b_{is}}{b_{1s}}\right)$-násobek prvního řádku, postupně pro $i = 2, \ldots, m+1$. Dostaneme tak matici $C = (c_{ij})$, která má v prvních s sloupcích samé nuly s výjimkou prvku $c_{1s} \neq 0$. Aplikujeme-li nyní na matici sestávající z posledních m řádků matice C indukční předpoklad, dostáváme tvrzení věty (rozmyslete si podrobně proč!). $\square$

Věta 5.3. *Hodnost matice ve schodovitém tvaru je rovna počtu jejích nenulových řádků.*

Důkaz. Nechť A je matice typu m/n ve schodovitém tvaru. Je-li A nulová matice, pak $h(A) = 0$ a tvrzení platí.

Nechť tedy A je nenulová matice ve schodovitém tvaru, která obsahuje k nenulových řádků. Těchto k řádků musí být lineárně nezávislých (plyne rozepsáním přímo z definice matice ve schodovitém tvaru) a všechny ostatní řádky (pokud existují) jsou nulové. To znamená, že maximální počet lineárně nezávislých řádků matice A je roven k, a tedy podle věty 4.1. je $h(A) = k$. $\square$

Pomocí posledních dvou vět a důsledku věty 5.1. můžeme nyní poměrně jednoduše zjišťovat hodnost dané matice A. Matici A nejprve převedeme pomocí elementárních řádkových úprav na schodovitý tvar (algoritmus je popsán v důkazu věty 5.2., který byl konstruktivní), v němž pak jen spočítáme počet nenulových řádků. Celý postup si ukážeme na následujícím příkladu.

Příklad 5.1. Určete hodnost matice A (nad tělesem $\mathbb{R}$) tvaru:

$$A = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 2 & 0 & 0 & -1 & -2 \\ -1 & 1 & 3 & 0 & 0 & -4 \\ 2 & 1 & -3 & 0 & -1 & 2 \end{pmatrix}.$$

Řešení: Nejprve záměnou 1. a 2. řádku dosáhneme toho, že v levém horním rohu matice bude nenulový prvek. Potom vynásobením 1. řádku vhodným číslem (zde reálným) a jeho přičtením k 2., 3., resp. 4. řádku dosáhneme toho, že pod tímto nenulovým prvkem v 1. sloupci budou samé nuly. Analogickým způsobem pak upravujeme submatici sestávající z 2., 3. a 4. řádku, atd., až nakonec dostaneme matici ve schodovitém tvaru.

Poznamenejme, že po úpravě budeme mezi jednotlivými maticemi psát symbol $\to$. Z úsporných důvodů provádíme obvykle vždy několik elementárních řádkových úprav typu (3) najednou. Tedy pak:

$$A \to \begin{pmatrix} 1 & 2 & 0 & 0 & -1 & -2 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ -1 & 1 & 3 & 0 & 0 & -4 \\ 2 & 1 & -3 & 0 & -1 & 2 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 0 & 0 & -1 & -2 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 3 & 3 & 0 & -1 & -6 \\ 0 & -3 & -3 & 0 & 1 & 6 \end{pmatrix} \to$$
$$\begin{pmatrix} 1 & 2 & 0 & 0 & -1 & -2 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & -4 & -9 \\ 0 & 0 & 0 & 0 & 4 & 9 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 0 & 0 & -1 & -2 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & -4 & -9 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Vidíme, že poslední matice (která je ve schodovitém tvaru) má 3 nenulové řádky, a tedy $h(A) = 3$.

Předchozí metodu (která je samozřejmě jen jednou z mnoha známých metod určování hodnosti matice) můžeme s výhodou použít při řešení celé řady úloh o vektorovém prostoru T^n. Chceme-li například v T^n zjistit dimenzi a bázi nějakého podprostoru W generovaného konečným počtem zadaných vektorů, pak tyto vektory napíšeme jako řádky do matice, kterou elementárními řádkovými úpravami převedeme na schodovitý tvar. Nenulové řádky takto získané matice ve schodovitém tvaru jsou pak bází podprostoru W (jak plyne z vět 5.1. a 5.3.). Podobným způsobem lze postupovat například při zjišťování dimenze a báze součtu dvou podprostorů v T^n, atd.

Příklad 5.2. Ve vektorovém prostoru $\mathbb{R}^5$ jsou dány podprostory $W_1 = [\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3]$ a $W_2 = [\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3]$, kde $\boldsymbol{u}_1 = (1, -1, 2, 4, 0)$, $\boldsymbol{u}_2 = (0, 0, 1, 3, 2)$, $\boldsymbol{u}_3 = (1, -1, 1, 1, -2)$, resp. $\boldsymbol{v}_1 = (0, 1, 0, 2, -2)$, $\boldsymbol{v}_2 = (-1, 2, 1, 3, -2)$, $\boldsymbol{v}_3 = (-1, 0, 1, -1, 2)$. Určete dimenzi a bázi podprostoru $W_1 + W_2$.

Řešení: Vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3$ generují $W_1 + W_2$ (proč?), tzn. $W_1 + W_2 = [\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3, \boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3]$. Stačí tedy napsat uvedených šest vektorů do řádků matice a tuto matici převést elementárními řádkovými úpravami na schodovitý tvar, Tedy:

$$\begin{pmatrix} 1 & -1 & 2 & 4 & 0 \\ 0 & 0 & 1 & 3 & 2 \\ 1 & -1 & 1 & 1 & -2 \\ 0 & 1 & 0 & 2 & -2 \\ -1 & 2 & 1 & 3 & -2 \\ -1 & 0 & 1 & -1 & 2 \end{pmatrix} \to \begin{pmatrix} 1 & -1 & 2 & 4 & 0 \\ 0 & 1 & 0 & 2 & -2 \\ 0 & 0 & 1 & 3 & 2 \\ 0 & 0 & -1 & -3 & -2 \\ 0 & 1 & 3 & 7 & -2 \\ 0 & -1 & 3 & 3 & 2 \end{pmatrix} \to \begin{pmatrix} 1 & -1 & 2 & 4 & 0 \\ 0 & 1 & 0 & 2 & -2 \\ 0 & 0 & 1 & 3 & 2 \\ 0 & 0 & -1 & -3 & -2 \\ 0 & 0 & 3 & 5 & 0 \\ 0 & 0 & 3 & 5 & 0 \end{pmatrix} \to$$

$$\begin{pmatrix} 1 & -1 & 2 & 4 & 0 \\ 0 & 1 & 0 & 2 & -2 \\ 0 & 0 & 1 & 3 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -4 & -6 \\ 0 & 0 & 0 & -4 & -6 \end{pmatrix} \to \begin{pmatrix} 1 & -1 & 2 & 4 & 0 \\ 0 & 1 & 0 & 2 & -2 \\ 0 & 0 & 1 & 3 & 2 \\ 0 & 0 & 0 & 4 & 6 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Tedy $\dim(W_1 + W_2) = 4$, přičemž bázi $W_1 + W_2$ tvoří například nenulové řádky poslední matice, tj. vektory $\boldsymbol{w}_1 = (1, -1, 2, 4, 0)$, $\boldsymbol{w}_2 = (0, 1, 0, 2, -2)$, $\boldsymbol{w}_3 = (0, 0, 1, 3, 2)$, $\boldsymbol{w}_4 = (0, 0, 0, 4, 6)$.

Jednou z dalších základních úloh lineární algebry je hledání inverzní matice k dané čtvercové regulární matici A řádu n. Z důsledku věty 3.8. víme, že:

$$A^{-1} = \frac{1}{|A|} \cdot A^*,$$

kde A^* je adjungovaná matice k matici A, a podle tohoto vzorce můžeme též inverzní matici A^{-1} přímo spočítat. Je však vidět, že pro větší n bude výpočet příliš pracný (je třeba vypočítat jeden determinant matice řádu n a dále n^2 determinantů matic řádu $n-1$). Proto si nyní odvodíme jednu poměrně jednoduchou a pro ruční výpočet celkem vhodnou metodu nalezení inverzní matice.

Věta 5.4. *Nechť A je regulární matice řádu n nad T. Pak platí:*

(1) *matici A lze konečným počtem elementárních řádkových úprav převést na jednotkovou matici E_n,*

(2) *provedení řádkové elementární úpravy matice A je ekvivalentní vynásobení matice A zleva jistou regulární maticí řádu n.*

Důkaz. (1): Podle předpokladu je $h(A) = n$, a tedy (podle vět 5.2. a 5.3.) matici A lze konečným počtem elementárních řádkových úprav převést na tvar, v němž v hlavní diagonále jsou nenulové prvky a pod ní jsou samé nuly. Vynásobením jednotlivých řádků vhodnými nenulovými čísly z T dostaneme v hlavní diagonále samé jedničky a pak konečným počtem elementárních řádkových úprav typu (3) nad diagonálou samé nuly. Tedy dostaneme jednotkovou matici E_n.

(2): Rozepsáním se bezprostředně ověří, že:

α) Záměna dvou řádků (i-tého a j-tého) matice A je ekvivalentní vynásobení matice A zleva maticí F, kde F je matice vzniklá z jednotkové matice E_n (řádu n) záměnou i-tého a j-tého řádku. Zřejmě ale $|F| = -1$, tzn. matice F je regulární.

β) Vynásobení i-tého řádku matice A nenulovým číslem $t \in T$ je ekvivalentní vynásobení matice A zleva maticí G, kde G je matice vzniklá z jednotkové matice E_n vynásobením i-tého řádku číslem t. Ale $|G| = t \neq 0$, tzn. matice G je regulární.

γ) Přičtení t-násobku j-tého řádku k i-tému řádku matice A (kde $i \neq j$ a $t \in T$ libovolný) je ekvivalentní vynásobení matice A zleva maticí H, kde H je matice vzniklá z jednotkové matice E_n přičtením t-násobku j-tého řádku k i-tému řádku. Podle věty 2.5. (1) však $|H| = 1$, tzn. H je regulární matice. □

Z předchozí věty už nyní přímo plyne metoda výpočtu inverzní matice k matici A. Spočívá v tom, že elementárními řádkovými úpravami převedeme matici A na jednotkovou matici E_n a tytéž elementární řádkové úpravy paralelně aplikujeme na jednotkovou matici E_n, která nám nakonec přejde v hledanou inverzní matici A^{-1}, neboť podle předchozí věty existují regulární matice $R_1, \dots, R_s$ takové, že:

$$(R_s \cdot \dots \cdot R_2 \cdot R_1) \cdot A = E_n,$$

což znamená, že $(R_s \cdot \dots \cdot R_2 \cdot R_1) = A^{-1}$. Současně však:

$$(R_s \cdot \dots \cdot R_2 \cdot R_1) \cdot E_n = (R_s \cdot \dots \cdot R_2 \cdot R_1),$$

odkud tedy jako výsledek dostáváme matici $(R_s \cdot \dots \cdot R_2 \cdot R_1) = A^{-1}$.

Prakticky provádíme výpočet tak, že obě matice, tj. A a E_n, napíšeme vedle sebe a oddělíme svislou čarou. Pak provádíme zvolené elementární řádkové úpravy, a to současně pro obě matice najednou. Výsledné matice budeme mezi sebou oddělovat symbolem $\sim$.

Příklad 5.3. K dané regulární matici A (nad tělesem $\mathbb{R}$) nalezněte inverzní matici A^{-1}. Přitom:

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 1 & 0 \end{pmatrix}.$$

Řešení:

$$\left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 3 & 2 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 2 & 1 & -1 & 1 & 0 \\ 0 & 0 & -1 & -1 & 0 & 1 \end{array}\right) \sim$$
$$\left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 1 & 1 & 0 & -1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 & \frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 1 & 1 & 0 & -1 \end{array}\right) \sim$$
$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & -\frac{1}{2} & \frac{1}{2} \\ 0 & 1 & 0 & -1 & \frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 1 & 1 & 0 & -1 \end{array}\right).$$

Hledanou inverzní maticí je tedy matice:

$$A^{-1} = \begin{pmatrix} 1 & -\frac{1}{2} & \frac{1}{2} \\ -1 & \frac{1}{2} & \frac{1}{2} \\ 1 & 0 & -1 \end{pmatrix}.$$

V našich předchozích úvahách o vektorových prostorech jsme doposud vystačili vždy s jednou pevnou bází daného vektorového prostoru, vzhledem k níž jsme vyjadřovali například souřadnice vektoru, atd. Na závěr tohoto paragrafu budeme nyní vyšetřovat vzájemný vztah mezi dvěma bázemi daného vektorového prostoru, resp. vztah mezi souřadnicemi téhož vektoru v různých bázích daného prostoru. Ukážeme si, že v obou případech lze s výhodou použít maticového způsobu zápisu, čímž se formálně značně zjednoduší naše vyjadřování.

Definice. Nechť V je vektorový prostor nad T a nechť:

$$\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n \tag{1}$$

$$\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \tag{2}$$

jsou dvě jeho báze. Nechť dále je:

$$\begin{aligned}
\boldsymbol{v}_1 &= a_{11} \cdot \boldsymbol{u}_1 + a_{21} \cdot \boldsymbol{u}_2 + \cdots + a_{n1} \cdot \boldsymbol{u}_n \\
\boldsymbol{v}_2 &= a_{12} \cdot \boldsymbol{u}_1 + a_{22} \cdot \boldsymbol{u}_2 + \cdots + a_{n2} \cdot \boldsymbol{u}_n \\
&\vdots \\
\boldsymbol{v}_n &= a_{1n} \cdot \boldsymbol{u}_1 + a_{2n} \cdot \boldsymbol{u}_2 + \cdots + a_{nn} \cdot \boldsymbol{u}_n
\end{aligned} \tag{3}$$

Pak matice A tvaru:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

se nazývá *matice přechodu od báze* (1) *k bázi* (2).

Poznámka. 1. Rozebereme-li si předchozí definici, pak vidíme, že matici A přechodu od jedné báze ke druhé bázi prostoru V zkonstruujeme tak, že j-tý vektor druhé báze vyjádříme jako lineární kombinaci vektorů první báze a její koeficienty pak zapíšeme do j-tého sloupce matice A (pro $j = 1, 2, \ldots, n$). Přitom je samozřejmé, že jak pořadí obou bází, tak i pořadí vektorů v těchto bázích je podstatné a nelze je nijak zaměňovat.

2. Matice přechodu od jedné báze k druhé bázi prostoru V je vždy regulární (plyne z (3) a z lineární nezávislosti vektorů druhé báze).

Příklad 5.4. Ve vektorovém prostoru $\mathbb{R}^3$ mějme dány dvě báze:

$$\boldsymbol{u}_1 = (1,1,1), \quad \boldsymbol{u}_2 = (1,1,0), \quad \boldsymbol{u}_3 = (1,0,0), \tag{4}$$

$$\boldsymbol{v}_1 = (2,3,2), \quad \boldsymbol{v}_2 = (3,1,2), \quad \boldsymbol{v}_3 = (4,3,3). \tag{5}$$

Lehce se ověří, že platí:

$$\begin{aligned}
\boldsymbol{v}_1 &= 2 \cdot \boldsymbol{u}_1 + \boldsymbol{u}_2 - \boldsymbol{u}_3, \\
\boldsymbol{v}_2 &= 2 \cdot \boldsymbol{u}_1 - \boldsymbol{u}_2 + 2 \cdot \boldsymbol{u}_3, \\
\boldsymbol{v}_3 &= 3 \cdot \boldsymbol{u}_1 + \boldsymbol{u}_3,
\end{aligned}$$

resp.

$$\begin{aligned}
\boldsymbol{u}_1 &= \boldsymbol{v}_1 + \boldsymbol{v}_2 - \boldsymbol{v}_3, \\
\boldsymbol{u}_2 &= -4 \cdot \boldsymbol{v}_1 - 5 \cdot \boldsymbol{v}_2 + 6 \cdot \boldsymbol{v}_3, \\
\boldsymbol{u}_3 &= -3 \cdot \boldsymbol{v}_1 - 3 \cdot \boldsymbol{v}_2 + 4 \cdot \boldsymbol{v}_3,
\end{aligned}$$

odkud již plyne, že matice A přechodu od báze (4) k bázi (5), resp. matice B přechodu od báze (5) k bázi (4) mají tvar:

$$A = \begin{pmatrix} 2 & 2 & 3 \\ 1 & -1 & 0 \\ -1 & 2 & 1 \end{pmatrix}, \text{ resp. } B = \begin{pmatrix} 1 & -4 & -3 \\ 1 & -5 & -3 \\ -1 & 6 & 4 \end{pmatrix}.$$

Vidíme tedy, že především je $A \neq B$, ale na druhé straně se výpočtem lehce zjistí, že $A \cdot B = E_3$, a tedy $B = A^{-1}$. Tedy, zaměněním pořadí bází (4) a (5) jsme dostali matici přechodu, která je k původní matici přechodu inverzní. Následující věta ukáže, že tomu tak musí být vždycky.

Věta 5.5. *Nechť* (1), *resp.* (2) *jsou dvě báze vektorového prostoru* V *nad* T. *Nechť* A *je matice přechodu od báze* (1) *k bázi* (2). *Potom* A^{-1} *je maticí přechodu od báze* (2) *k bázi* (1).

Důkaz. Nechť $A = (a_{ij})$. Pak podle definice matice přechodu od (1) k (2) je:

$$\boldsymbol{v}_j = \sum_{k=1}^{n} a_{kj} \cdot \boldsymbol{u}_k, \ \ j = 1, \ldots, n.$$

Nechť dále $B = (b_{ij})$ je matice přechodu od báze (2) k bázi (1). Pak je:

$$\boldsymbol{u}_k = \sum_{r=1}^{n} b_{rk} \cdot \boldsymbol{v}_r, \ \ k = 1, \ldots, n.$$

Po dosazení dostáváme:

$$\boldsymbol{v}_j = \sum_{k=1}^{n} a_{kj} \cdot \sum_{r=1}^{n} b_{rk} \cdot \boldsymbol{v}_r = \sum_{r=1}^{n} \left(\sum_{k=1}^{n} b_{rk} \cdot a_{kj} \right) \cdot \boldsymbol{v}_r, \quad j = 1, \ldots, n.$$

Podle věty 4.2., kap. I., se každý vektor z V dá napsat pouze jediným způsobem jako lineární kombinace vektorů dané báze. Zřejmě však je:

$$\boldsymbol{v}_j = 0 \cdot \boldsymbol{v}_1 + \cdots + 0 \cdot \boldsymbol{v}_{j-1} + 1 \cdot \boldsymbol{v}_j + 0 \cdot \boldsymbol{v}_{j+1} + \cdots + 0 \cdot \boldsymbol{v}_n, \quad j = 1, \ldots, n.$$

Porovnáním posledních dvou rovností pak dostáváme:

$$\sum_{k=1}^{n} b_{rk} \cdot a_{kj} = \begin{cases} 0 & \text{pro } r \neq j \\ 1 & \text{pro } r = j \end{cases}$$

což maticově vyjádřeno říká, že $B \cdot A = E_n$, odkud již plyne, že $B = A^{-1}$.

□

Poznámka. Z definice matice přechodu plyne, že zadáním bází (1) a (2) je jednoznačně určena matice přechodu od (1) k (2), tj. jistá regulární matice A. Podobně však, máme-li dánu bázi (1) a nějakou regulární matici A, pak je těmito dvěma údaji (pomocí vztahů (3)) jednoznačně určena báze (2) taková, že matice A je maticí přechodu od (1) k (2). Stejně tak, zadáním báze (2) a regulární matice A je jednoznačně určena báze (1) taková, že A je maticí přechodu od (1) k (2). Bázi (1) můžeme v tomto případě zkonstruovat např. užitím věty 5.5. (tzn. ze vztahů (3), pomocí báze (2) a inverzní matice A^{-1}).

Zcela na závěr nyní ještě odvodíme, jaký je vzájemný vztah mezi souřadnicemi jednoho vektoru ve dvou různých bázích prostoru V. Je samozřejmé, že při změně báze se změní i souřadnice vektoru vzhledem k bázi. Poněvadž mnohdy pro jednoduchost výpočtů je vhodná speciální volba báze, je důležité znát pravidla, podle nichž se mění souřadnice vektoru při změně báze. Touto otázkou, nazývanou *transformace souřadnic vektoru*, se nyní budeme zabývat.

Nechť tedy (1) a (2) jsou dvě báze vektorového prostoru V a nechť $A = (a_{ij})$ je matice přechodu od báze (1) k bázi (2). Dále nechť $\boldsymbol{w} \in V$ je pevný vektor, přičemž $\boldsymbol{w}$ má v bázi (1), resp. v bázi (2), souřadnice:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad \text{resp.} \quad \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

To ale znamená, že platí:

$$\boldsymbol{w} = x_1 \cdot \boldsymbol{u}_1 + \cdots + x_n \cdot \boldsymbol{u}_n \tag{6}$$

$$\boldsymbol{w} = y_1 \cdot \boldsymbol{v}_1 + \cdots + y_n \cdot \boldsymbol{v}_n \tag{7}$$

Dosadíme-li do (7) vztahy (3), dostáváme:

$$\boldsymbol{w} = \sum_{j=1}^{n} y_j \cdot \boldsymbol{v}_j = \sum_{j=1}^{n} y_j \cdot \sum_{k=1}^{n} a_{kj} \cdot \boldsymbol{u}_k = \sum_{k=1}^{n} \left(\sum_{j=1}^{n} a_{kj} \cdot y_j \right) \cdot \boldsymbol{u}_k. \tag{8}$$

Nyní však porovnáním pravých stran (6) a (8) dostáváme:

$$x_1 \cdot \boldsymbol{u}_1 + \cdots + x_n \cdot \boldsymbol{u}_n = (a_{11} y_1 + \cdots + a_{1n} y_n) \cdot \boldsymbol{u}_1 + \cdots + (a_{n1} y_1 + \cdots + a_{nn} y_n) \cdot \boldsymbol{u}_n,$$

odkud z jednoznačnosti obou vyjádření plyne rovnost odpovídajících si koeficientů, tj.:

$$\begin{aligned} x_1 &= a_{11} y_1 + \cdots + a_{1n} y_n \\ x_2 &= a_{21} y_1 + \cdots + a_{2n} y_n \\ &\vdots \\ x_n &= a_{n1} y_1 + \cdots + a_{nn} y_n \end{aligned}$$

což však můžeme zapsat v maticovém tvaru:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = A \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

Tímto jsme tedy dostali souřadnice vektoru $\boldsymbol{w}$ v bázi (1) vyjádřené pomocí souřadnic téhož vektoru v bázi (2). Kdybychom chtěli naopak vyjádřit souřadnice vektoru $\boldsymbol{w}$ v bázi (2) pomocí jeho souřadnic v bázi (1), pak stačí obě strany poslední maticové rovnice vynásobit zleva maticí A^{-1} (která existuje, neboť matice A je regulární). Dostaneme pak:

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = A^{-1} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Kapitola 3

Soustavy lineárních rovnic

§1. Gaussova metoda řešení soustav lineárních rovnic

Se soustavami lineárních rovnic a jejich řešením je možné se v určitých jednoduchých, resp. speciálních případech setkat již na střední škole. V tomto paragrafu ukážeme jednu z mnoha známých metod praktického řešení obecných soustav lineárních rovnic. Výklad je veden tak, že je možno tento paragraf studovat nezávisle na jeho zařazení do III. kapitoly (z předchozí látky se používá pouze pojem matice, matice ve schodovitém tvaru, elementární řádková úprava matice a některé jednoduché vlastnosti vektorového prostoru T^n) a je pak možno jej použít při řešení konkrétních příkladů vztahujících se k problematice probírané dříve.

Definice. Nechť T je číselné těleso. Pak soustava rovnic:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{k1}x_1 + a_{k2}x_2 + \cdots + a_{kn}x_n &= b_k \end{aligned} \tag{1}$$

kde $a_{ij} \in T$, $b_i \in T$, se nazývá *soustava k lineárních rovnic o n neznámých* (nad tělesem T).

Řešení soustavy (1) je každá uspořádaná n-tice $(t_1, \ldots, t_n)$ prvků z T taková, že po dosazení t_i za x_i $(i = 1, \ldots, n)$ všechny rovnice v (1) přejdou v identity, tj. platí:

$$\begin{aligned} a_{11}t_1 + a_{12}t_2 + \cdots + a_{1n}t_n &= b_1 \\ a_{21}t_1 + a_{22}t_2 + \cdots + a_{2n}t_n &= b_2 \\ &\vdots \\ a_{k1}t_1 + a_{k2}t_2 + \cdots + a_{kn}t_n &= b_k \end{aligned}$$

Poznámka. 1. Pro lepší vyjadřování zaveďme ještě následující označení a názvy: číslo a_{ij} v soustavě (1) budeme nazývat *koeficient* (v i-té rovnici u j-té neznámě), resp. číslo b_i budeme nazývat *absolutní člen* i-té rovnice. Dále, matice:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \end{pmatrix}, \text{ resp. } \overline{A} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} & b_k \end{pmatrix}$$

se nazývá *matice soustavy* (1), resp. *rozšířená matice soustavy* (1). Abychom opticky odlišili absolutní členy od koeficientů soustavy (1), budeme obvykle v rozšířené matici soustavy $\overline{A}$ psát před sloupcem absolutních členů svislou čáru.

2. Každé řešení soustavy (1) je, jak bylo v definici řečeno, uspořádaná n-tice prvků z tělesa T, tzn. může být považováno za vektor z vektorového prostoru T^n. Množinu všech řešení soustavy (1) lze pak chápat jako jistou podmnožinu prostoru T^n (která může být případně i prázdná, nemá-li soustava (1) žádné řešení).

3. Označíme-li:

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \text{ resp. } B = \begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix},$$

pak můžeme zřejmě soustavu (1) zapsat krátce maticovou rovnicí:

$$A \cdot X = B.$$

Tento maticový způsob zápisu soustav lineárních rovnic nám pak v dalším často umožní přehledné a stručné vyjadřování.

Definice. Soustava lineárních rovnic se nazývá *řešitelná soustava* (resp. *neřešitelná soustava*), jestliže existuje alespoň jedno (resp. neexistuje žádné) její řešení.

Dvě soustavy lineárních rovnic o n neznámých (nad týmž tělesem T) se nazývají *ekvivalentní soustavy*, jestliže množiny jejich řešení si jsou rovny. Jakákoliv úprava dané soustavy lineárních rovnic, po níž vznikne soustava ekvivalentní, se nazývá *ekvivalentní úprava* dané soustavy lineárních rovnic.

Uvědomme si, že „řešit“ danou soustavu lineárních rovnic znamená buď najít všechna její řešení, nebo zjistit, že je neřešitelná. Pokud jde o počet řešení soustavy lineárních rovnic, nastane zřejmě vždycky právě jeden z následujících tří případů:

(1) soustava nemá žádné řešení (tj. je neřešitelná),
(2) soustava má jediné řešení,
(3) soustava má více než jedno řešení (ukážeme, že nekonečně mnoho).

Věta 1.1. *Nechť je dána soustava lineárních rovnic* (1)*. Pak následující úpravy jsou ekvivalentními úpravami soustavy* (1)*:*

(1) *libovolná záměna pořadí rovnic,*
(2) *vynásobení libovolné rovnice nenulovým číslem z T,*
(3) *k jedné rovnici přičtení jiné rovnice vynásobené libovolným číslem z T,*
(4) *vypuštění z* (1) *rovnice, která je lineární kombinací ostatních rovnic.*

Důkaz. (1), (2): Zřejmé.

(3): Vzhledem k (1) můžeme předpokládat, že k první rovnici soustavy (1) přičteme druhou rovnici vynásobenou číslem $p \in T$. Dostáváme tak soustavu (2) tvaru:

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n + p \cdot (a_{21}x_1 + \cdots + a_{2n}x_n) &= b_1 + p \cdot b_2 \\ a_{21}x_1 + \cdots + a_{2n}x_n &= b_2 \\ &\;\vdots \\ a_{k1}x_1 + \cdots + a_{kn}x_n &= b_k \end{aligned} \tag{2}$$

Nyní, je-li $(t_1, \ldots, t_n)$ řešením soustavy (1), pak zřejmě je $(t_1, \ldots, t_n)$ řešením soustavy (2).

Naopak, nechť $(t_1, \ldots, t_n)$ je řešením soustavy (2). Pak po dosazení do první rovnice soustavy (2) dostáváme:

$$a_{11}t_1 + \cdots + a_{1n}t_n + p \cdot (a_{21}t_1 + \cdots + a_{2n}t_n) = b_1 + p \cdot b_2.$$

Podle předpokladu však $a_{21}t_1 + \cdots + a_{2n}t_n = b_2$, tzn. po dosazení a odečtení dostáváme:

$$a_{11}t_1 + \cdots + a_{1n}t_n = b_1,$$

odkud již ihned plyne, že $(t_1, \ldots, t_n)$ je řešením soustavy (1) (poněvadž druhá až k-tá rovnice v (2) a v (1) jsou stejné).

Dokázali jsme tedy, že soustavy (1) a (2) jsou ekvivalentní.

(4): Vzhledem k (1) předpokládejme, že v soustavě (1) je první rovnice lineární kombinací ostatních rovnic, tj. soustava (1) je tvaru:

$$\begin{aligned} p_2 \cdot (a_{21}x_1 + \cdots + a_{2n}x_n) + \cdots + p_k \cdot (a_{k1}x_1 + \cdots + a_{kn}x_n) &= p_2 \cdot b_2 + \cdots + p_k \cdot b_k \\ a_{21}x_1 + \cdots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{k1}x_1 + \cdots + a_{kn}x_n &= b_k \end{aligned} \tag{3}$$

kde $p_2, \ldots, p_k \in T$. Uvažme dále soustavu (4), která vznikne ze soustavy (3) vypuštěním první rovnice, tj.:

$$\begin{aligned} a_{21}x_1 + \cdots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{k1}x_1 + \cdots + a_{kn}x_n &= b_k \end{aligned} \tag{4}$$

Nyní je však bezprostředně vidět, že $(t_1, \ldots, t_n)$ je řešením (3), právě když $(t_1, \ldots, t_n)$ je řešením (4), neboli že soustavy (3) a (4) jsou ekvivalentní. □

Při provádění ekvivalentních úprav dané soustavy lineárních rovnic není nutné stále opisovat celou soustavu i s neznámými, ale zřejmě stačí pracovat s její rozšířenou maticí soustavy. Uvědomme si, že pak provádění úprav (1) – (4) na dané soustavě je ekvivalentní provádění elementárních řádkových úprav na její rozšířené matici soustavy doplněnému o vypouštění řádků matice, které jsou lineárními kombinacemi ostatních řádků.

Na této úvaze je pak založena metoda řešení soustav lineárních rovnic, kterou nyní popíšeme. Její princip spočívá v tom, že danou soustavu lineárních rovnic převedeme na ekvivalentní, ale „jednodušší" soustavu, jejíž řešení (která jsou zároveň i řešeními původní soustavy) bude možno víceméně ihned vypsat.

Gaussova metoda řešení soustavy lineárních rovnic

Nechť je dána soustava lineárních rovnic (1). Pak ekvivalentními úpravami z věty 1.1. převedeme soustavu (1) na soustavu (1'), jejíž rozšířená matice soustavy je ve schodovitém tvaru, přičemž vždy vypustíme každou rovnici, která je lineární kombinací ostatních rovnic (z předchozí úvahy a z věty 5.2., kap. II., plyne, že toho lze po konečném počtu kroků vždy dosáhnout). Nechť soustava (1') má s rovnic. Potom:

1. Vyskytne-li se v (1') rovnice, v níž všechny koeficienty jsou nulové a absolutní člen je různý od nuly, pak zřejmě soustava (1'), a tedy i soustava (1) je neřešitelná.

V opačném případě je soustava (1) řešitelná, a sice:

2. Má jediné řešení, je-li $s = n$. Toto řešení lehce spočítáme postupným dosazováním ze soustavy (1').

3. Má nekonečně mnoho řešení, je-li $s < n$. V tomto případě (opět postupným dosazováním z (1')) vyjádříme jistých s neznámých pomocí zbývajících $(n - s)$ neznámých (které se nazývají *volné neznámé*). Dosazujeme-li za volné neznámé libovolně čísla z T (kterých je nekonečně mnoho), dostáváme pak jednotlivá konkrétní řešení soustavy (1) (kterých je tedy také nekonečně mnoho).

Ilustrujme si nyní Gaussovu metodu řešení soustavy lineárních rovnic na několika typických příkladech.

Příklad 1.1. Řešte soustavu lineárních rovnic (nad $\mathbb{R}$):

$$\begin{aligned} x_1 + 2x_2 - x_3 + x_4 &= 1 \\ -2x_1 - 3x_2 + 2x_3 - 3x_4 &= 2 \\ x_1 + x_2 - x_3 + 2x_4 &= -1 \\ x_2 + 2x_4 &= 3 \end{aligned}$$

Řešení: Napíšeme rozšířenou matici této soustavy a pomocí elementárních řádkových úprav ji převedeme na schodovitý tvar. Navíc vypouštíme řádky, které jsou lineární kombinací ostatních řádků (pokud se takové vyskytnou).

$$\left(\begin{array}{rrrr|r} 1 & 2 & -1 & 1 & 1 \\ -2 & -3 & 2 & -3 & 2 \\ 1 & 1 & -1 & 2 & -1 \\ 0 & 1 & 0 & 2 & 3 \end{array}\right) \to \left(\begin{array}{rrrr|r} 1 & 2 & -1 & 1 & 1 \\ 0 & 1 & 0 & -1 & 4 \\ 0 & -1 & 0 & 1 & -2 \\ 0 & 1 & 0 & 2 & 3 \end{array}\right) \to$$

$$\left(\begin{array}{rrrr|r} 1 & 2 & -1 & 1 & 1 \\ 0 & 1 & 0 & -1 & 4 \\ 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 3 & -1 \end{array}\right).$$

I když poslední matice ještě není formálně upravena na schodovitý tvar, vidíme, že daná soustava je neřešitelná, neboť ve třetím řádku poslední matice, tj. ve třetí rovnici poslední soustavy jsou všechny koeficienty u neznámých nulové, kdežto absolutní člen je od nuly různý.

Příklad 1.2. Řešte soustavu lineárních rovnic (nad $\mathbb{R}$):

$$\begin{aligned} x_1 - 2x_2 + x_3 &= -1 \\ x_1 \phantom{{}- 2x_2} + x_3 &= 1 \\ 2x_1 - 5x_2 + 4x_3 &= 0 \\ 2x_1 - 3x_2 \phantom{{}+ 4x_3} &= -4 \end{aligned}$$

Řešení:

$$\left(\begin{array}{ccc|c} 1 & -2 & 1 & -1 \\ 1 & 0 & 1 & 1 \\ 2 & -5 & 4 & 0 \\ 2 & -3 & 0 & -4 \end{array}\right) \to \left(\begin{array}{ccc|c} 1 & -2 & 1 & -1 \\ 0 & 2 & 0 & 2 \\ 0 & -1 & 2 & 2 \\ 0 & 1 & -2 & -2 \end{array}\right) \to \left(\begin{array}{ccc|c} 1 & -2 & 1 & -1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 2 & 3 \end{array}\right).$$

Tedy z poslední rovnice: $2x_3 = 3$, neboli $x_3 = \frac{3}{2}$. Dále z předposlední rovnice dostáváme přímo: $x_2 = 1$ a konečně z první rovnice: $x_1 = -1 + 2x_2 - x_3$, tj. po dosazení: $x_1 = -\frac{1}{2}$.

Daná soustava má tedy jediné řešení $\left(-\frac{1}{2}, 1, \frac{3}{2}\right)$.

Příklad 1.3. Řešte soustavu lineárních rovnic (nad $\mathbb{R}$):

$$\begin{aligned} x_1 - 2x_2 + x_3 + x_4 &= 2 \\ x_1 - 2x_2 - x_3 + x_4 &= -2 \\ x_1 - 2x_2 + 3x_3 + x_4 &= 6 \end{aligned}$$

Řešení:

$$\left(\begin{array}{cccc|c} 1 & -2 & 1 & 1 & 2 \\ 1 & -2 & -1 & 1 & -2 \\ 1 & -2 & 3 & 1 & 6 \end{array}\right) \to \left(\begin{array}{cccc|c} 1 & -2 & 1 & 1 & 2 \\ 0 & 0 & -2 & 0 & -4 \\ 0 & 0 & 2 & 0 & 4 \end{array}\right) \to \left(\begin{array}{cccc|c} 1 & -2 & 1 & 1 & 2 \\ 0 & 0 & 1 & 0 & 2 \end{array}\right).$$

Tedy dostáváme soustavu, v níž budou dvě volné neznámé (zřejmě kterékoliv dvě z neznámých x_1, x_2, x_4, nikoliv však neznámá x_3). Zvolíme-li za volné neznámé např. neznámé x_2, x_4, pak lehce vypočteme: $x_3 = 2$, $x_1 = 2x_2 - x_4$.

Tedy (položíme-li $x_2 = t$, $x_4 = s$) daná soustava má nekonečně mnoho řešení tvaru $(2t - s, t, 2, s)$, kde t, s jsou libovolná reálná čísla.

Poznámka. Jestliže má soustava lineárních rovnic nekonečně mnoho řešení, pak z Gaussovy metody vyplývá pouze to, kolik neznámých volíme za volné neznámé, nikoliv však, které neznámé to jsou. Může se totiž stát, že některou neznámou nesmíme volit za volnou neznámou (např. neznámou x_3 v příkladu 1.3.) nebo naopak, některou neznámou musíme volit za volnou neznámou (např. v soustavě dvou rovnic o čtyřech neznámých tvaru:

$$\begin{aligned} x_1 \qquad + 2x_3 + x_4 &= 1 \\ x_3 - x_4 &= 0 \end{aligned}$$

musíme zřejmě za jednu ze dvou volných neznámých zvolit neznámou x_2).

§2. Základní vlastnosti soustav lineárních rovnic

Mějme dánu soustavu k lineárních rovnic o n neznámých nad T, tj. soustavu:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{k1}x_1 + a_{k2}x_2 + \cdots + a_{kn}x_n &= b_k \end{aligned} \tag{1}$$

kde A, resp. $\overline{A}$ bude značit matici této soustavy, resp. rozšířenou matici této soustavy. Zajímáme-li se o hodnost matic A a $\overline{A}$, pak ihned vidíme, že zřejmě mohou dva případy: buď je $h(\overline{A}) = h(A)$, nebo je $h(\overline{A}) = h(A) + 1$. Přitom $h(\overline{A}) = h(A)$ nastane právě tehdy, když sloupec absolutních členů je lineární kombinací sloupců matice A (rozmyslete si podrobně proč).

Nyní si uvedeme důležitou větu, která nám umožní rozhodnout o řešitelnosti či neřešitelnosti soustavy lineárních rovnic, aniž bychom hledali její řešení.

Věta 2.1. (Frobeniova věta, resp. Kronecker-Capelliho věta**)** *Soustava lineárních rovnic (nad T) je řešitelná, právě když hodnost matice této soustavy je rovna hodnosti rozšířené matice této soustavy.*

Důkaz. Uvažujme soustavu (1), kde A, resp. $\overline{A}$ značí matici soustavy (1), resp. rozšířenou matici soustavy (1).

„$\Rightarrow$“: Nechť (1) je řešitelná soustava a nechť $(t_1, \ldots, t_n)$ je řešení (1). Pak platí:

$$\begin{aligned} a_{11}t_1 + a_{12}t_2 + \cdots + a_{1n}t_n &= b_1 \\ a_{21}t_1 + a_{22}t_2 + \cdots + a_{2n}t_n &= b_2 \\ &\vdots \\ a_{k1}t_1 + a_{k2}t_2 + \cdots + a_{kn}t_n &= b_k \end{aligned}$$

neboli:

$$\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_k \end{pmatrix} = t_1 \cdot \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{k1} \end{pmatrix} + t_2 \cdot \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{k2} \end{pmatrix} + \cdots + t_n \cdot \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{kn} \end{pmatrix},$$

což znamená, že sloupec absolutních členů je lineární kombinací sloupců matice A, a tedy $h(\overline{A}) = h(A)$.

„$\Leftarrow$“: Nechť $h(\overline{A}) = h(A)$. Potom (jak bylo řečeno v úvodu tohoto paragrafu) sloupec absolutních členů je lineární kombinací sloupců matice A. Označíme-li koeficienty v této lineární kombinaci $t_1, \ldots, t_n$, pak stejným obratem jako v 1. části důkazu dostaneme, že $(t_1, \ldots, t_n)$ je řešením soustavy (1). Tedy soustava (1) je řešitelná. $\square$

Frobeniova věta je jednoduchým a elegantním kriteriem řešitelnosti soustav lineárních rovnic, ovšem v případě řešitelné soustavy neříká nic o počtu řešení ani o tom, jak všechna řešení vypadají. Takové úvahy budou nyní obsahem zbytku tohoto paragrafu. Nejprve vyšetříme specielní případ soustavy (1), kdy $k = n$ (tzn. rovnic je tolik jako neznámých) a navíc matice soustavy je regulární.

Věta 2.2. (Cramerovo pravidlo) *Nechť je dána soustava n lineárních rovnic o n neznámých, jejíž matice soustavy A je regulární. Pak soustava má jediné řešení $(x_1, \ldots, x_n)$, přičemž:*

$$x_j = \tfrac{|A_j|}{|A|}, \quad j = 1, 2, \ldots, n,$$

kde A_j je matice vzniklá z matice A nahrazením j-tého sloupce sloupcem absolutních členů.

Důkaz. Uvažme soustavu (1), v níž $k = n$, a kterou tedy můžeme maticově zapsat ve tvaru:

$$A \cdot X = B, \quad \text{kde } X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}. \tag{2}$$

Matice A je však podle předpokladu regulární, tzn. existuje inverzní matice A^{-1}. Potom vynásobením rovnosti (2) zleva maticí A^{-1} dostaneme $A^{-1} \cdot (A \cdot X) = A^{-1} \cdot B$, odkud:

$$X = A^{-1} \cdot B, \tag{3}$$

což je tedy řešení dané soustavy, které (jak plyne z odvození) je jediné.

Pokusme se nyní nalezené řešení explicitně vyjádřit. Podle důsledku věty 3.8., kap. II., je:

$$A^{-1} = \frac{1}{|A|} \cdot \begin{pmatrix} A_{11} & A_{21} & \cdots & A_{n1} \\ \vdots & \vdots & \vdots & \vdots \\ A_{1j} & A_{2j} & \cdots & A_{nj} \\ \vdots & \vdots & \vdots & \vdots \\ A_{1n} & A_{2n} & \cdots & A_{nn} \end{pmatrix},$$

kde A_{ij} je algebraický doplněk prvku a_{ij} v matici A. Z (3) pak dostáváme:

$$x_j = \frac{1}{|A|} \cdot (A_{1j} \cdot b_1 + A_{2j} \cdot b_2 + \cdots + A_{nj} \cdot b_n) =$$
$$\frac{1}{|A|} \cdot \begin{vmatrix} a_{11} & \cdots & a_{1,j-1} & b_1 & a_{1,j+1} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & \cdots & a_{n,j-1} & b_n & a_{n,j+1} & \cdots & a_{nn} \end{vmatrix}$$

užitím důsledku Laplaceovy věty. Tedy skutečně $x_j = \frac{|A_j|}{|A|}$ pro $j = 1, \ldots, n$. □

Nyní vyřešíme obecný případ, tzn. popíšeme řešení obecné soustavy k lineárních rovnic o n neznámých, o níž víme, že je řešitelná.

Věta 2.3. (Obecné Cramerovo pravidlo) *Nechť* (1) *je řešitelná soustava lineárních rovnic a nechť $h(A) = r$. Dále:*

- *Vybereme z matice A r lineárně nezávislých řádků a dále uvažujeme pouze ty rovnice, jejichž koeficienty se nacházejí ve vybraných řádcích.*
- *Ponecháme na levé straně takových r neznámých, že matice sestavená z koeficientů u těchto neznámých je regulární. Ostatní neznámé (pokud existují) převedeme na pravé strany a nazveme je volné neznámé.*

Potom, zvolíme-li za volné neznámé libovolně pevné prvky z T a vypočítáme-li Cramerovým pravidlem zbývající neznámé, dostaneme tímto způsobem právě všechna řešení soustavy (1).

Důkaz. Podle předpokladu je $h(\overline{A}) = h(A) = r$. Vzhledem k větě 1.1. (1) můžeme předpokládat, že prvních r řádků matice $\overline{A}$ je lineárně nezávislých a ostatní řádky jsou lineární kombinací prvních r řádků. Potom podle věty 1.1. (4) je soustava (1) ekvivalentní soustavě:

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= b_1 \\ &\vdots \\ a_{r1}x_1 + \cdots + a_{rn}x_n &= b_r \end{aligned} \tag{4}$$

Nyní mohou nastat dva případy:

I. Je-li $r = n$, pak $|A| \neq 0$ a podle věty 2.2. existuje jediné řešení soustavy (4), a tedy i soustavy (1), které spočteme Cramerovým pravidlem, tzn. tvrzení platí.

II. Nechť $r < n$ a nechť pro přehlednost zápisu je nenulový minor řádu r matice soustavy (4) tvořen prvními r sloupci. Převedením zbývajících neznámých na pravé strany a dosazením $x_j = c_j$, kde $c_j \in T$, $j = r{+}1, \dots, n$ dostáváme:

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1r}x_r &= b_1 - a_{1,r+1}c_{r+1} - \cdots - a_{1n}c_n \\ &\vdots \\ a_{r1}x_1 + \cdots + a_{rr}x_r &= b_r - a_{r,r+1}c_{r+1} - \cdots - a_{rn}c_n \end{aligned} \tag{5}$$

Na soustavu (5) můžeme použít Cramerovo pravidlo, čímž dostaneme jediné řešení $(c_1, \dots, c_r)$ soustavy (5). Potom však $(c_1, \dots, c_r, c_{r+1}, \dots, c_n)$ je zřejmě řešením (4), tzn. i řešením (1).

Naopak, musíme ukázat, že každé řešení soustavy (1) lze obdržet popsaným způsobem. Nechť tedy $(d_1, \dots, d_n)$ je libovolné řešení soustavy (1). Pak $(d_1, \dots, d_n)$ je řešením soustavy (4). Dosadíme-li d_j za x_j pro $j = r + 1, \dots, n$, pak $(d_1, \dots, d_r)$ je řešením soustavy (5), a musí tedy být rovno tomu jedinému řešení, které dostaneme použitím Cramerova pravidla. Tedy řešení $(d_1, \dots, d_n)$ jsme dostali postupem uvedeným ve větě. □

Důsledek. *Nechť je dána soustava lineárních rovnic* (1). *Potom:*

(1) *soustava* (1) *má jediné řešení* $\iff h(A) = h(\overline{A}) = n$,

(2) *soustava* (1) *má nekonečně mnoho řešení* $\iff h(A) = h(\overline{A}) < n$.

Důkaz. Obě tvrzení plynou přímo z Frobeniovy věty a z důkazu obecného Cramerova pravidla, podle něhož má soustava (1) jediné řešení, právě když neexistuje žádná volná neznámá, tzn. právě když $h(A) = n$. □

Poznámka. Poznamenejme, že řešení soustav lineárních rovnic pomocí Cramerova pravidla, resp. obecného Cramerova pravidla má spíše teoretický význam, protože je numericky poměrně náročné (např. rozhodně náročnější než Gaussova metoda popsaná v §1). Na druhé straně nám ale Cramerovo pravidlo umožňuje přímý výpočet jednotlivých neznámých, což může být někdy výhodné (např. jsme-li v situaci, kdy nás zajímá pouze hodnota jedné neznámé).

§3. Homogenní soustavy lineárních rovnic

Definice. Soustava:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= 0 \\ &\vdots \\ a_{k1}x_1 + a_{k2}x_2 + \cdots + a_{kn}x_n &= 0 \end{aligned} \tag{1}$$

kde $a_{ij} \in T$, se nazývá *homogenní soustava* k lineárních rovnic o n neznámých nad T.

Poznámka. Matici soustavy (1), resp. rozšířenou matici soustavy (1) budeme opět značit A, resp. $\overline{A}$. Protože matice $\overline{A}$ vznikla z matice A přidáním sloupce skládajícího se ze samých nul, je zřejmě $h(\overline{A}) = h(A)$, a tedy (podle Frobeniovy věty) homogenní soustava (1) je vždy řešitelná.

Evidentně, uspořádaná n-tice $(0, 0, \ldots, 0)$ je řešením soustavy (1). Toto řešení se nazývá *nulové řešení*. Vidíme tedy, že homogenní soustava má buď jediné řešení (a sice nulové), anebo má nekonečně mnoho řešení (tj. kromě nulového i nenulová řešení).

Kriterium pro oba případy udává následující věta.

Věta 3.1. *Nechť* (1) *je homogenní soustava s maticí soustavy A. Potom:*
(1) *soustava* (1) *má pouze nulové řešení* $\iff$ $h(A) = n$,
(2) *soustava* (1) *má též nenulová řešení* $\iff$ $h(A) < n$.

Důkaz. Tvrzení plyne přímo z důsledku věty 2.3., neboť v (1) je $h(\overline{A}) = h(A)$. □

Poznámka. Z předchozí věty a z věty 4.4., kap. II., plyne, že ve specielním případě, kdy počet rovnic je roven počtu neznámých (tj. $k = n$), má homogenní soustava pouze nulové řešení (resp. má též nenulová řešení), právě když $|A| \neq 0$ (resp. $|A| = 0$).

Jak již bylo dříve řečeno, každé řešení soustavy lineárních rovnic o n neznámých nad T je možno považovat za vektor z vektorového prostoru T^n. Množina W všech řešení této soustavy je pak podmnožinou v T^n, která v případě nehomogenní soustavy zřejmě není nikdy podprostorem v T^n (neboť zcela jistě neobsahuje nulový vektor). V případě homogenních soustav je však situace jiná, jak ukazuje následující věta.

Věta 3.2. *Množina W všech řešení homogenní soustavy* (1) *je podprostorem ve vektorovém prostoru T^n a platí:* $\dim W = n - h(A)$.

Důkaz. I. Dokážeme, že W je podprostor v T^n. Zřejmě je $(0, 0, \ldots, 0) \in W$, tzn. $W \neq \emptyset$. Dále, nechť $(c_1, \ldots, c_n), (d_1, \ldots, d_n) \in W$, $t, s \in T$ libovolné, tzn. je: $\sum\limits_{j=1}^{n} a_{ij}c_j = 0$, $\sum\limits_{j=1}^{n} a_{ij}d_j = 0$ pro $i = 1, \ldots, k$. Pak ale:

$$\sum_{j=1}^{n} a_{ij}(t \cdot c_j + s \cdot d_j) = t \cdot \sum_{j=1}^{n} a_{ij}c_j + s \cdot \sum_{j=1}^{n} a_{ij}d_j = t \cdot 0 + s \cdot 0 = 0$$

pro $i = 1, \ldots, k$. To znamená, že $t \cdot (c_1, \ldots, c_n) + s \cdot (d_1, \ldots, d_n) \in W$, a tedy W je podprostor v T^n.

II. Dokážeme, že $\dim W = n - r$, kde $r = h(A)$. Zřejmě musí být $0 \leq r \leq n$. Je-li $r = 0$, pak $W = T^n$, resp. je-li $r = n$, pak $W = \{(0, 0, \ldots, 0)\}$, a v obou případech je $\dim W = n - r$.

Předpokládejme tedy, že $1 \leq r \leq n - 1$. Protože $h(A) = r$, lze v matici A soustavy (1) najít nenulový minor řádu r. Bez újmy na obecnosti můžeme předpokládat, že:

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1r} \\ a_{21} & a_{22} & \cdots & a_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ a_{r1} & a_{r2} & \cdots & a_{rr} \end{vmatrix} \neq 0.$$

Podle obecného Cramerova pravidla je pak W rovno množině všech řešení soustavy:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1r}x_r + a_{1,r+1}x_{r+1} + \cdots + a_{1n}x_n &= 0 \\ &\vdots \\ a_{r1}x_1 + a_{r2}x_2 + \cdots + a_{rr}x_r + a_{r,r+1}x_{r+1} + \cdots + a_{rn}x_n &= 0 \end{aligned} \qquad (2)$$

v níž za neznámé $x_{r+1}, \ldots, x_n$ volíme libovolně jisté prvky z T.

Označme $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{n-r}$ následující řešení soustavy (2), a tedy i soustavy (1):

$$\begin{aligned}
\boldsymbol{w}_1 &= (c_{11}, \quad \dots, c_{1r}, \quad 1, 0, 0, \dots, 0, 0) \\
\boldsymbol{w}_2 &= (c_{21}, \quad \dots, c_{2r}, \quad 0, 1, 0, \dots, 0, 0) \\
&\vdots \\
\boldsymbol{w}_{n-r} &= (c_{n-r,1}, \dots, c_{n-r,r}, 0, 0, 0, \dots, 0, 1)
\end{aligned}$$

a ukážeme, že tvoří bázi podprostoru W.

α) Vektory $\boldsymbol{w}_1, \dots, \boldsymbol{w}_{n-r}$ jsou zřejmě lineárně nezávislé (rozmyslete si podrobně proč).

β) Nechť $\boldsymbol{u} = (u_1, \dots, u_n) \in W$ libovolný, tzn. $\boldsymbol{u}$ je řešením soustavy (1). Uvažme vektor $\boldsymbol{w} = u_{r+1} \cdot \boldsymbol{w}_1 + \dots + u_n \cdot \boldsymbol{w}_{n-r}$. Zřejmě je $\boldsymbol{w} \in W$ a platí $\boldsymbol{w} = (y_1, \dots, y_r, u_{r+1}, \dots, u_n)$, kde $y_1, \dots, y_r$ jsou nějaká čísla z T. Vidíme, že vektory $\boldsymbol{u}$ a $\boldsymbol{w}$ mají posledních $(n-r)$ složek shodných a oba jsou z W, tzn. oba jsou řešeními (2). Pak ovšem podle obecného Cramerova pravidla musí být $y_1 = u_1, \dots, y_r = u_r$, odkud plyne, že $\boldsymbol{u} = \boldsymbol{w}$, tzn. vektor $\boldsymbol{u}$ je lineární kombinací vektorů $\boldsymbol{w}_1, \dots, \boldsymbol{w}_{n-r}$, které tedy generují podprostor W. Dohromady dostáváme, že $\dim W = n - r = n - h(A)$. □

Poznámka. 1. Na základě předchozí věty jsme u homogenní soustavy oprávněni hovořit o podprostoru všech řešení místo o množině všech řešení. Dále je dobré si uvědomit, že číslo $n - h(A)$ udává počet volných neznámých, a tedy dimenze podprostoru řešení dané homogenní soustavy je rovna počtu volných neznámých v této soustavě.

2. Při praktickém hledání báze podprostoru řešení W je nejvýhodnější postupovat tak, že si nejprve obecně vyjádříme řešení dané soustavy, potom $(n-r)$ volných neznámých zvolíme $(n-r)$ lineárně nezávislými způsoby a spočítáme vektory báze W. Je zřejmé, že bází W je nekonečně mnoho, přičemž početně nejjednodušší volbou bude volba provedená v důkazu předchozí věty (tj. volba vždy jedné jedničky a ostatních nul).

Příklad 3.1. Nalezněte dvě báze podprostoru řešení W homogenní soustavy lineárních rovnic (nad $\mathbb{R}$):

$$\begin{aligned}
x_1 + x_2 + x_3 - x_4 &= 0 \\
x_3 + x_4 &= 0
\end{aligned}$$

Řešení: Soustavu zřejmě není nutné upravovat, volné neznámé budou dvě, např. x_2 a x_4, přičemž pak je $x_3 = -x_4$, $x_1 = -x_2 + 2x_4$. Obecné řešení soustavy je tedy tvaru $(-t + 2s, t, -s, s)$, kde $t, s \in \mathbb{R}$.

Volíme-li např. $t = 1$, $s = 0$, resp. $t = 0$, $s = 1$, dostáváme bázi podprostoru řešení W ve tvaru $(-1, 1, 0, 0), (2, 0, -1, 1)$.

Podobně, volíme-li např. $t = 1$, $s = 1$, resp. $t = -1$, $s = \sqrt{2}$ (uvědomme si, že se jedná o dvě lineárně nezávislé volby!), dostáváme bázi podprostoru řešení W ve tvaru $(1, 1, -1, 1), (1 + 2\sqrt{2}, -1, -\sqrt{2}, \sqrt{2})$.

Předchozí věta v podstatě říká, že homogenní soustavou lineárních rovnic o n neznámých je určen jistý podprostor vektorového prostoru T^n. Toto tvrzení lze však také obrátit, jak ukazuje následující věta.

Věta 3.3. *Nechť W je libovolný podprostor vektorového prostoru T^n. Pak existuje homogenní soustava lineárních rovnic (o n neznámých, nad T), jejíž množina řešení je rovna právě W.*

Důkaz. Je-li $W = \{(0, \dots, 0)\}$, resp. $W = T^n$, pak věta zřejmě platí (hledanou soustavou je pak např. soustava s maticí soustavy E_n, resp. 0_{nn}).

Nechť tedy $\{(0, \dots, 0)\} \subsetneqq W \subsetneqq T^n$ a nechť vektory:

$$\begin{aligned} \boldsymbol{w}_1 &= (w_{11}, w_{12}, \dots, w_{1n}) \\ &\vdots \\ \boldsymbol{w}_k &= (w_{k1}, w_{k2}, \dots, w_{kn}) \end{aligned}$$

tvoří bázi podprostoru W. Uvažme následující homogenní soustavu:

$$\begin{aligned} w_{11}x_1 + w_{12}x_2 + \dots + w_{1n}x_n &= 0 \\ &\vdots \\ w_{k1}x_1 + w_{k2}x_2 + \dots + w_{kn}x_n &= 0 \end{aligned} \tag{3}$$

Hodnost matice soustavy (3) je rovna k, neboť její řádky jsou lineárně nezávislé. Označme písmenem U podprostor řešení soustavy (3). Podle věty 3.2. je pak $\dim U = n - k$ (> 0). Nechť:

$$\begin{aligned} \boldsymbol{u}_1 &= (u_{11}, \quad u_{12}, \quad \dots, u_{1n} \quad), \\ &\vdots \\ \boldsymbol{u}_{n-k} &= (u_{n-k,1}, u_{n-k,2}, \dots, u_{n-k,n}) \end{aligned}$$

je pevná báze podprostoru U. Uvažme další homogenní soustavu:

$$\begin{aligned} u_{11}x_1 + \quad u_{12}x_2 + \dots + \quad u_{1n}x_n &= 0 \\ &\vdots \\ u_{n-k,1}x_1 + u_{n-k,2}x_2 + \dots + u_{n-k,n}x_n &= 0 \end{aligned} \tag{4}$$

o níž dokážeme, že je hledanou soustavou, tzn. označíme-li podprostor řešení soustavy (4) jako $\overline{W}$, musíme dokázat, že $\overline{W} = W$.

Ale $\boldsymbol{w}_j$ je řešením soustavy (4) (což plyne z toho, že $\boldsymbol{u}_1, \dots, \boldsymbol{u}_{n-k}$ jsou řešeními soustavy (3)) pro $j = 1, \dots, k$, a tedy $\boldsymbol{w}_1, \dots, \boldsymbol{w}_k \in \overline{W}$, odkud dostáváme, že $W = L(\boldsymbol{w}_1, \dots, \boldsymbol{w}_k) \subseteq \overline{W}$.

Dále, hodnost matice soustavy (4) je zřejmě $n - k$, tzn. podle věty 3.2. je pak $\dim \overline{W} = n - (n - k) = k = \dim W$.

Dohromady je tedy $W \subseteq \overline{W} \wedge \dim W = \dim \overline{W}$, odkud podle věty 4.5. (2), kap. I., dostáváme, že $W = \overline{W}$. □

Poznámka. Je třeba si uvědomit, že homogenní soustava, jejíž existenci předchozí věta zaručuje, není zřejmě určena jednoznačně. Dále, obratů uvedených v důkazu předchozí věty se používá při řešení konkrétních příkladů, a je proto nutné je znát.

Příklad 3.2. Nalezněte soustavu lineárních rovnic (nad $\mathbb{R}$), jejíž množina řešení je rovna podprostoru W vektorového prostoru $\mathbb{R}^4$, kde W je generován vektory:

$$\boldsymbol{w}_1 = (1, 2, 1, 1), \quad \boldsymbol{w}_2 = (0, 1, -1, 1), \quad \boldsymbol{w}_3 = (1, 3, 0, 2).$$

Řešení: Nejprve si napíšeme soustavu (3) (přitom není nutné z generátorů W předem vybrat bázi W, neboť eventuelní nadbytečné rovnice v (3) během výpočtu stejně vypadnou), pak najdeme bázi jejího podprostoru řešení U a nakonec pak složky vektorů báze U budou vystupovat jako koeficienty v hledané soustavě (4).

Nejprve tedy řešíme soustavu:

$$\begin{aligned} x_1 + 2x_2 + x_3 + x_4 &= 0 \\ x_2 - x_3 + x_4 &= 0 \\ x_1 + 3x_2 \qquad + 2x_4 &= 0 \end{aligned} \Rightarrow \left(\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 0 \\ 0 & 1 & -1 & 1 & 0 \\ 1 & 3 & 0 & 2 & 0 \end{array}\right) \to \cdots \to$$

$$\left(\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 0 \\ 0 & 1 & -1 & 1 & 0 \end{array}\right),$$

odkud dostáváme $x_2 = x_3 - x_4$, $x_1 = -3x_3 + x_4$, tzn. báze podprostoru řešení této soustavy je například $\boldsymbol{u}_1 = (-3, 1, 1, 0), \boldsymbol{u}_2 = (1, -1, 0, 1)$.

Hledaná soustava lineárních rovnic je pak například:

$$\begin{aligned} -3x_1 + x_2 + x_3 \qquad &= 0 \\ x_1 - x_2 \qquad + x_4 &= 0 \end{aligned}$$

Na závěr celé kapitoly se vrátíme ještě k obecným soustavám lineárních rovnic (nad T) a budeme se snažit říci něco více o množině řešení takové soustavy. Hlavní význam následujících úvah a tvrzení se však ukáže a využije později v geometrii.

Definice. Nechť je dána soustava lineárních rovnic nad T:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ &\vdots \\ a_{k1}x_1 + a_{k2}x_2 + \cdots + a_{kn}x_n &= b_k \end{aligned} \tag{5}$$

Pak homogenní soustava lineárních rovnic s týmiž koeficienty u neznámých, tj.:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= 0 \\ &\vdots \\ a_{k1}x_1 + a_{k2}x_2 + \cdots + a_{kn}x_n &= 0 \end{aligned} \tag{6}$$

se nazývá *zhomogenizovaná soustava* k soustavě (5).

Věta 3.4. *Nechť je dána soustava lineárních rovnic* (5). *Pak platí:*

(1) *součet libovolného řešení soustavy* (5) *s libovolným řešením k ní zhomogenizované soustavy je řešením soustavy* (5),

(2) *rozdíl libovolných dvou řešení soustavy* (5) *je řešením k ní zhomogenizované soustavy.*

Důkaz. (1): Nechť $\boldsymbol{u} = (u_1, \dots, u_n)$ je řešení soustavy (5) a nechť $\boldsymbol{v}' = (v_1', \dots, v_n')$ je řešení k ní zhomogenizované soustavy (6), tzn. platí:

$$\sum_{j=1}^{n} a_{ij}u_j = b_i, \ \text{ resp. } \sum_{j=1}^{n} a_{ij}v_j' = 0$$

pro $i = 1, \dots, k$. Pak $\boldsymbol{u} + \boldsymbol{v}' = (u_1 + v_1', \dots, u_n + v_n')$ a platí:

$$\sum_{j=1}^{n} a_{ij}(u_j + v_j') = \sum_{j=1}^{n} a_{ij}u_j + \sum_{j=1}^{n} a_{ij}v_j' = b_i + 0 = b_i$$

pro $i = 1, \dots, k$, a tedy $\boldsymbol{u} + \boldsymbol{v}'$ je řešením soustavy (5).

(2): Nechť $\boldsymbol{u} = (u_1, \dots, u_n)$, resp. $\boldsymbol{v} = (v_1, \dots, v_n)$ jsou dvě řešení soustavy (5), tzn. platí:

$$\sum_{j=1}^{n} a_{ij}u_j = b_i, \ \text{ resp. } \sum_{j=1}^{n} a_{ij}v_j = b_i$$

pro $i = 1, \dots, k$. Pak $\boldsymbol{u} - \boldsymbol{v} = (u_1 - v_1, \dots, u_n - v_n)$ a platí:

$$\sum_{j=1}^{n} a_{ij}(u_j - v_j) = \sum_{j=1}^{n} a_{ij}u_j - \sum_{j=1}^{n} a_{ij}v_j = b_i - b_i = 0$$

pro $i = 1, \dots, k$, a tedy $\boldsymbol{u} - \boldsymbol{v}$ je řešením zhomogenizované soustavy (6). $\square$

Věta 3.5. *Nechť* (5) *je řešitelná soustava lineárních rovnic. Pak všechna řešení soustavy* (5) *obdržíme přičtením všech řešení zhomogenizované soustavy* (6) *k jednomu pevnému řešení soustavy* (5).

Důkaz. Označme M množinu všech řešení soustavy (5). Podle předpokladu je $M \neq \emptyset$. Nechť $\boldsymbol{u}_0 \in M$ je pevné řešení soustavy (5). Označme dále:

$$\overline{M} = \{\boldsymbol{u}_0 + \boldsymbol{v}' \mid \boldsymbol{v}' \text{ je řešení (6)}\}.$$

Dokážeme, že $M = \overline{M}$.

„$\subseteq$“: Nechť $\boldsymbol{u} \in M$ je libovolné řešení soustavy (5). Podle věty 3.4. (2) je $\boldsymbol{u} - \boldsymbol{u}_0$ řešením zhomogenizované soustavy (6). Ale pak je: $\boldsymbol{u} = \boldsymbol{u}_0 + (\boldsymbol{u} - \boldsymbol{u}_0) \in \overline{M}$.

„$\supseteq$“: Plyne ihned z věty 3.4. (1). $\square$

Kapitola 4

Euklidovské vektorové prostory

§1. Skalární součin, velikost a odchylka vektorů

Při našich dosavadních úvahách o vektorových prostorech jsme pomocí operací sčítání vektorů a násobení čísla s vektorem vyšetřovali pojmy jako byla lineární závislost a nezávislost vektorů, generovatelnost, souřadnice vektoru, atd. Prozatím jsme však neměli možnost ve vektorových prostorech „měřit", tzn. zjišťovat a porovnávat délky vektorů, resp. odchylky (tj. velikosti úhlů), což jsou pojmy, které hrají podstatnou roli např. v geometrii. Jejich definice jsou založeny na pojmu skalárního součinu, který nyní zavedeme. Omezíme se přitom však pouze na vektorové prostory nad tělesem reálných čísel.

Úmluva. Všude v dalším v této kapitole budeme vektorovým prostorem rozumět *reálný vektorový prostor*, tj. (konečnědimenzionální) vektorový prostor nad tělesem $\mathbb{R}$ reálných čísel.

Definice. Nechť V je vektorový prostor (nad $\mathbb{R}$) a nechť každé dvojici vektorů $\boldsymbol{u}, \boldsymbol{v} \in V$ je přiřazeno reálné číslo $\boldsymbol{u} \cdot \boldsymbol{v}$ tak, že pro libovolné $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in V$, $r \in \mathbb{R}$ platí:

(1) $\boldsymbol{u} \cdot \boldsymbol{v} = \boldsymbol{v} \cdot \boldsymbol{u}$,
(2) $(\boldsymbol{u} + \boldsymbol{v}) \cdot \boldsymbol{w} = (\boldsymbol{u} \cdot \boldsymbol{w}) + (\boldsymbol{v} \cdot \boldsymbol{w})$,
(3) $(r \cdot \boldsymbol{u}) \cdot \boldsymbol{v} = r \cdot (\boldsymbol{u} \cdot \boldsymbol{v})$,
(4) je-li $\boldsymbol{u} \neq \boldsymbol{o}$, pak $\boldsymbol{u} \cdot \boldsymbol{u} > 0$.

Potom reálné číslo $\boldsymbol{u} \cdot \boldsymbol{v}$ se nazývá *skalární součin* vektorů $\boldsymbol{u}, \boldsymbol{v}$.

Vektorový prostor, v němž je definován skalární součin, se nazývá euklidovský vektorový prostor nebo krátce *euklidovský prostor*.

Poznámka. 1. Z definice plyne, že euklidovský prostor je vlastně uspořádaná dvojice $(V, \cdot)$ sestávající z vektorového prostoru V a ze skalárního součinu $\cdot$ definovaného ve V. Z důvodů stručnosti však budeme obvykle říkat pouze „euklidovský prostor V“ (tzn. zavedeme podobnou úmluvu jako u grup nebo těles, u nichž při označování vynecháváme symboly operací, pokud není nebezpečí nedorozumění).

2. Z kapitoly I. víme, že každý podprostor vektorového prostoru V nad T je sám vektorovým prostorem nad T. Je-li specielně V euklidovským prostorem, tzn. je reálný s definovaným skalárním součinem, pak zřejmě axiomy skalárního součinu budou jistě splněny i v jeho libovolném (vektorovém) podprostoru. To znamená, že každý (vektorový) podprostor euklidovského prostoru V je sám euklidovským prostorem. Budeme jej stručně nazývat *podprostor euklidovského prostoru.*

Předchozí definice nic neříká o tom, zda v libovolném vektorovém prostoru (nad $\mathbb{R}$) lze definovat skalární součin, resp. kolika způsoby. Odpověď na tyto otázky nám dá následující příklad a věta.

Příklad 1.1. Nechť $V = \mathbb{R}^2$ a nechť $\boldsymbol{u} = (u_1, u_2), \boldsymbol{v} = (v_1, v_2) \in \mathbb{R}^2$. Pak:

1. Položíme-li $\boldsymbol{u} \cdot \boldsymbol{v} = u_1v_1 + u_2v_2$,
jsou zřejmě splněny axiomy skalárního součinu a $\mathbb{R}^2$ s tímto skalárním součinem je euklidovským prostorem.

2. Položíme-li $\boldsymbol{u} \cdot \boldsymbol{v} = 4u_1v_1 + 2u_1v_2 + 2u_2v_1 + 3u_2v_2$,
pak jsou opět splněny axiomy skalárního součinu (ověřte si sami podrobným rozepsáním!), tzn. $\mathbb{R}^2$ s tímto skalárním součinem je euklidovským prostorem.

Je vidět, že i když se v obou případech jedná o tentýž vektorový prostor $\mathbb{R}^2$, jsou definované skalární součiny různé, a tedy různé jsou pak i pomocí nich získané euklidovské prostory.

Příklad 1.2. Nechť $V = \mathbb{R}_n[x]$ a nechť $\boldsymbol{f} = f(x), \boldsymbol{g} = g(x) \in \mathbb{R}_n[x]$ jsou libovolné vektory – polynomy. Položíme-li $\boldsymbol{f} \cdot \boldsymbol{g} = \int_0^1 f(x) \cdot g(x)\, \boldsymbol{dx}$, pak rozepsáním (užitím základních vět o integrování známých z analýzy) se ověří platnost axiomů skalárního součinu. Tedy $\mathbb{R}_n[x]$ s tímto skalárním součinem je euklidovský prostor.

Věta 1.1. *V každém reálném vektorovém prostoru V lze definovat skalární součin.*

Důkaz. Pro nulový vektorový prostor věta zřejmě platí (stačí položit $\boldsymbol{o} \cdot \boldsymbol{o} = 0$). Nechť tedy $\dim V = n > 0$ a nechť $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ je pevná báze prostoru V. Pak libovolné vektory $\boldsymbol{u}, \boldsymbol{v} \in V$ lze (jednoznačně) vyjádřit ve tvaru:

$$\boldsymbol{u} = x_1 \cdot \boldsymbol{e}_1 + \cdots + x_n \cdot \boldsymbol{e}_n,$$

resp.

$$\boldsymbol{v} = y_1 \cdot \boldsymbol{e}_1 + \cdots + y_n \cdot \boldsymbol{e}_n.$$

Položíme-li:

$$\boldsymbol{u} \cdot \boldsymbol{v} = x_1 y_1 + \cdots + x_n y_n,$$

pak zřejmě $\boldsymbol{u} \cdot \boldsymbol{v} \in \mathbb{R}$ a lehce se ověří, že jsou splněny axiomy (1) – (4) skalárního součinu. □

Shrneme-li naše dosavadní úvahy, můžeme říct, že z každého reálného vektorového prostoru lze utvořit euklidovský prostor, obecně však nikoliv jediným způsobem.

Věta 1.2. *Nechť V je euklidovský vektorový prostor. Pak platí:*
(1) $\boldsymbol{u} \cdot (\boldsymbol{v} + \boldsymbol{w}) = (\boldsymbol{u} \cdot \boldsymbol{v}) + (\boldsymbol{u} \cdot \boldsymbol{w})$,
(2) $\boldsymbol{u} \cdot (r \cdot \boldsymbol{v}) = r \cdot (\boldsymbol{u} \cdot \boldsymbol{v})$,
(3) $\left(\sum\limits_{i=1}^{m} p_i \cdot \boldsymbol{u}_i\right) \cdot \left(\sum\limits_{j=1}^{n} r_j \cdot \boldsymbol{v}_j\right) = \sum\limits_{i=1}^{m}\sum\limits_{j=1}^{n} p_i r_j \cdot (\boldsymbol{u}_i \cdot \boldsymbol{v}_j)$,
(4) $\boldsymbol{o} \cdot \boldsymbol{u} = \boldsymbol{u} \cdot \boldsymbol{o} = 0$,
(4) $\boldsymbol{u} \cdot \boldsymbol{u} = 0 \iff \boldsymbol{u} = \boldsymbol{o}$
pro $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}, \boldsymbol{u}_i, \boldsymbol{v}_j \in V$, $r, p_i, r_j \in \mathbb{R}$ lib.

Důkaz. (1) a (2): Jsou zřejmé důsledky definice skalárního součinu.
(3): Dokážeme lehce matematickou indukcí.
(4): $\boldsymbol{o} \cdot \boldsymbol{u} = (0 \cdot \boldsymbol{o}) \cdot \boldsymbol{u} = 0 \cdot (\boldsymbol{o} \cdot \boldsymbol{u}) = 0$. Zbytek analogicky.
(5): „$\Rightarrow$“: Plyne z axiomu (4) skalárního součinu.
„$\Leftarrow$“: Plyne z (4). □

Definice. Nechť V je euklidovský prostor, $\boldsymbol{u} \in V$. Pak nezáporné reálné číslo:

$$\|\boldsymbol{u}\| = \sqrt{\boldsymbol{u} \cdot \boldsymbol{u}}$$

se nazývá délka nebo též *velikost vektoru* $\boldsymbol{u}$.

Je-li $\|\boldsymbol{u}\| = 1$, pak říkáme, že *vektor* $\boldsymbol{u}$ *je normovaný.*

Věta 1.3. (Schwarzova nerovnost) *Nechť V je euklidovský prostor, $\boldsymbol{u}, \boldsymbol{v} \in V$ libovolné. Pak platí:*

$$|\boldsymbol{u} \cdot \boldsymbol{v}| \leq \|\boldsymbol{u}\| \cdot \|\boldsymbol{v}\|, \tag{1}$$

tzn. absolutní hodnota skalárního součinu dvou vektorů je menší nebo rovna součinu velikostí těchto vektorů.

Důkaz. Je-li $\boldsymbol{v} = \boldsymbol{o}$, pak $|\boldsymbol{u} \cdot \boldsymbol{o}| = 0 = \|\boldsymbol{u}\| \cdot \|\boldsymbol{o}\|$ a věta platí. Předpokládejme tedy, že $\boldsymbol{v} \neq \boldsymbol{o}$ a uvažme vektor $\boldsymbol{u} - r \cdot \boldsymbol{v}$, kde $r \in \mathbb{R}$ je libovolné. Pak je:

$$0 \leq (\boldsymbol{u} - r \cdot \boldsymbol{v}) \cdot (\boldsymbol{u} - r \cdot \boldsymbol{v}) = \boldsymbol{u} \cdot \boldsymbol{u} - 2r \cdot (\boldsymbol{u} \cdot \boldsymbol{v}) + r^2 \cdot (\boldsymbol{v} \cdot \boldsymbol{v}).$$

Zvolíme-li nyní $r = \frac{\boldsymbol{u} \cdot \boldsymbol{v}}{\boldsymbol{v} \cdot \boldsymbol{v}}$ (což lze, neboť podle předpokladu $\boldsymbol{v} \cdot \boldsymbol{v} > 0$), dostaneme:

$$0 \leq \boldsymbol{u} \cdot \boldsymbol{u} - 2 \cdot \frac{(\boldsymbol{u} \cdot \boldsymbol{v})}{(\boldsymbol{v} \cdot \boldsymbol{v})} \cdot (\boldsymbol{u} \cdot \boldsymbol{v}) + \frac{(\boldsymbol{u} \cdot \boldsymbol{v})^2}{(\boldsymbol{v} \cdot \boldsymbol{v})^2} \cdot (\boldsymbol{v} \cdot \boldsymbol{v}),$$

odkud po vykrácení a pak vynásobení číslem $\boldsymbol{v} \cdot \boldsymbol{v}$ (> 0) dostáváme:

$$0 \leq (\boldsymbol{u} \cdot \boldsymbol{u}) \cdot (\boldsymbol{v} \cdot \boldsymbol{v}) - (\boldsymbol{u} \cdot \boldsymbol{v})^2,$$

neboli:

$$(\boldsymbol{u} \cdot \boldsymbol{v})^2 \leq (\boldsymbol{u} \cdot \boldsymbol{u}) \cdot (\boldsymbol{v} \cdot \boldsymbol{v}),$$

což po odmocnění dává dokazovanou nerovnost (1). □

Důsledek. *Ve Schwarzově nerovnosti* (1) *nastane rovnost, právě když vektory $\boldsymbol{u}, \boldsymbol{v}$ jsou lineárně závislé.*

Důkaz. Z důkazu předchozí věty plyne, že v (1) nastane rovnost, právě když $\boldsymbol{v} = \boldsymbol{o}$ nebo $\boldsymbol{u} - r \cdot \boldsymbol{v} = \boldsymbol{o}$, tzn. právě když $\boldsymbol{u}, \boldsymbol{v}$ jsou lineárně závislé.

□

Poznámka. Schwarzovu nerovnost (1) často zapisujeme v ekvivalentním tvaru:

$$(\boldsymbol{u} \cdot \boldsymbol{v})^2 \le \|\boldsymbol{u}\|^2 \cdot \|\boldsymbol{v}\|^2.$$

Poznamenejme ještě, že pro nerovnost (1) se v literatuře používá též pojmenování „Cauchyova nerovnost“, resp. „Cauchy-Bunjakovského nerovnost“, event. „Cauchy-Schwarzova nerovnost“.

Věta 1.4. *Nechť V je euklidovský prostor, $\boldsymbol{u}, \boldsymbol{v} \in V$, $r \in \mathbb{R}$. Pak platí:*
(1) $\|\boldsymbol{u}\| \ge 0$, *přičemž* $\|\boldsymbol{u}\| = 0$, *právě když* $\boldsymbol{u} = \boldsymbol{o}$,
(2) $\|r \cdot \boldsymbol{u}\| = |r| \cdot \|\boldsymbol{u}\|$,
(3) $\|\boldsymbol{u} + \boldsymbol{v}\| \le \|\boldsymbol{u}\| + \|\boldsymbol{v}\|$,
(4) *je-li* $\boldsymbol{u} \ne \boldsymbol{o}$, *pak* $\frac{1}{\|\boldsymbol{u}\|} \cdot \boldsymbol{u}$ *je normovaný vektor.*

Důkaz. (1) a (4): Jsou bezprostředními důsledky definice velikosti vektoru.
(2): $\|r \cdot \boldsymbol{u}\|^2 = (r \cdot \boldsymbol{u}) \cdot (r \cdot \boldsymbol{u}) = r^2 \cdot (\boldsymbol{u} \cdot \boldsymbol{u})$, odkud po odmocnění dostáváme:

$$\|r \cdot \boldsymbol{u}\| = \sqrt{r^2 \cdot (\boldsymbol{u} \cdot \boldsymbol{u})} = |r| \cdot \|\boldsymbol{u}\|.$$

(3): Z definice velikosti vektoru a Schwarzovy nerovnosti plyne: $\|\boldsymbol{u} + \boldsymbol{v}\|^2 = (\boldsymbol{u} + \boldsymbol{v}) \cdot (\boldsymbol{u} + \boldsymbol{v}) = (\boldsymbol{u} \cdot \boldsymbol{u}) + 2 \cdot (\boldsymbol{u} \cdot \boldsymbol{v}) + (\boldsymbol{v} \cdot \boldsymbol{v}) \le (\boldsymbol{u} \cdot \boldsymbol{u}) + 2 \cdot \|\boldsymbol{u}\| \cdot \|\boldsymbol{v}\| + (\boldsymbol{v} \cdot \boldsymbol{v}) = \|\boldsymbol{u}\|^2 + 2 \cdot \|\boldsymbol{u}\| \cdot \|\boldsymbol{v}\| + \|\boldsymbol{v}\|^2 = \big(\|\boldsymbol{u}\| + \|\boldsymbol{v}\|\big)^2$. Protože však $\|\boldsymbol{u} + \boldsymbol{v}\|$ i $\big(\|\boldsymbol{u}\| + \|\boldsymbol{v}\|\big)$ jsou nezáporná čísla, dostáváme po odmocnění žádané tvrzení. $\square$

Poznámka. 1. Nerovnost uvedená ve 3. části věty se obvykle nazývá „trojúhelníková nerovnost“.

2. Použijeme-li obratu provedeného ve 4. části věty (tzn. vektor $\boldsymbol{u}$ násobíme číslem $\frac{1}{\|\boldsymbol{u}\|}$), pak říkáme, že jsme vektor $\boldsymbol{u}$ „normovali“.

Definice. Nechť $\boldsymbol{u}, \boldsymbol{v}$ jsou *nenulové* vektory z euklidovského prostoru V. Pak reálné číslo φ splňující vztahy:

$$\cos\varphi = \frac{\boldsymbol{u} \cdot \boldsymbol{v}}{\|\boldsymbol{u}\| \cdot \|\boldsymbol{v}\|} \quad \wedge \quad 0 \le \varphi \le \pi \tag{2}$$

se nazývá *odchylka vektorů* $\boldsymbol{u}, \boldsymbol{v}$.

Poznámka. Je potřeba si rozmyslet, že uvedená definice odchylky je korektní, tzn. že číslo φ splňující (2) existuje, a to jediné. Ale Schwarzovu nerovnost můžeme pro nenulové vektory $\boldsymbol{u}, \boldsymbol{v}$ přepsat ve tvaru:

$$\frac{|\boldsymbol{u}\cdot\boldsymbol{v}|}{\|\boldsymbol{u}\|\cdot\|\boldsymbol{v}\|} \le 1, \text{ tzn. } \left|\frac{\boldsymbol{u}\cdot\boldsymbol{v}}{\|\boldsymbol{u}\|\cdot\|\boldsymbol{v}\|}\right| \le 1, \text{ odkud } -1 \le \frac{\boldsymbol{u}\cdot\boldsymbol{v}}{\|\boldsymbol{u}\|\cdot\|\boldsymbol{v}\|} \le 1.$$

Vidíme tedy (na základě našich znalostí o goniometrických funkcích), že existuje právě jedno reálné číslo φ splňující podmínky (2).

Poznamenejme ještě, že odchylka vektorů není definována pro případ, kdy některý z těchto vektorů je nulovým vektorem.

§2. Ortogonálnost

Definice. Nechť V je euklidovský prostor a nechť:

$$\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k \tag{1}$$

je konečná posloupnost vektorů z V. Řekneme, že:

(1) posloupnost (1) je ortogonální (nebo stručně, že *vektory* $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ *jsou ortogonální*), jestliže je:

$$\boldsymbol{u}_i \cdot \boldsymbol{u}_j = 0 \text{ pro každé } i, j = 1, \ldots, k \ \wedge\ i \neq j,$$

(2) posloupnost (1) je ortonormální (nebo stručně, že *vektory* $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ *jsou ortonormální*), je-li ortogonální a každý její vektor je normovaný,

(3) posloupnost (1) je *ortogonální báze* (resp. *ortonormální báze*) euklidovského prostoru V, jestliže je ortogonální (resp. ortonormální) a navíc je bází prostoru V.

Poznámka. Rozebereme-li si definici ortogonálnosti pro nejjednodušší případy, pak ihned vidíme, že:

pro $k = 1$: Posloupnost sestávající z jednoho vektoru je vždy ortogonální (bez ohledu na to, zda např. daný vektor je nulový či nikoliv).

pro $k = 2$: Vektory $\boldsymbol{u}_1, \boldsymbol{u}_2$ jsou ortogonální, právě když $\boldsymbol{u}_1 \cdot \boldsymbol{u}_2 = 0$. V tomto případě budeme psát $\boldsymbol{u}_1 \perp \boldsymbol{u}_2$ nebo $\boldsymbol{u}_2 \perp \boldsymbol{u}_1$ (zřejmě zde nezáleží na pořadí vektorů). Dále, jsou-li oba vektory $\boldsymbol{u}_1, \boldsymbol{u}_2$ nenulové, pak zřejmě jsou ortogonální, právě když jejich odchylka je $\frac{\pi}{2}$ (plyne z definice odchylky). Na druhé straně, dva vektory, z nichž alespoň jeden je nulový, jsou vždycky ortogonální (přičemž jejich odchylka samozřejmě není definována).

Další vlastnosti ortogonálních vektorů popisují následující tvrzení.

Věta 2.1. *Nechť V je euklidovský prostor. Pak pro vektory z V platí:*

(1) $\boldsymbol{u} \perp \boldsymbol{u} \iff \boldsymbol{u} = \boldsymbol{o}$,

(2) $\boldsymbol{u} \perp \boldsymbol{x}$ *pro každé* $\boldsymbol{x} \in V \iff \boldsymbol{u} = \boldsymbol{o}$,

(3) $\boldsymbol{u} \perp \boldsymbol{w}_i$ *pro* $i = 1, \dots, k \iff \boldsymbol{u} \perp \left(\sum_{i=1}^{k} r_i \cdot \boldsymbol{w}_i\right)$ *pro každé* $r_i \in \mathbb{R}$.

Důkaz. (1), (2): Ihned plyne z předchozí definice a z definice skalárního součinu.

(3): „$\Rightarrow$“: Nechť $\boldsymbol{u} \perp \boldsymbol{w}_i$, tzn. $\boldsymbol{u} \cdot \boldsymbol{w}_i = 0$ pro $i = 1, \dots, k$. Pak pro libovolná $r_i \in \mathbb{R}$ je:

$$\boldsymbol{u} \cdot \left(\sum_{i=1}^{k} r_i \cdot \boldsymbol{w}_i\right) = \sum_{i=1}^{k} r_i \cdot (\boldsymbol{u} \cdot \boldsymbol{w}_i) = 0,$$

a tedy $\boldsymbol{u} \perp \left(\sum_{i=1}^{k} r_i \cdot \boldsymbol{w}_i\right)$.

„$\Leftarrow$“: Zvolíme-li $r_i = 1$ a $r_j = 0$ pro $j \neq i$, pak $\boldsymbol{u} \perp \boldsymbol{w}_i$, $i = 1, \dots, k$.

□

Věta 2.2. *Nenulové ortogonální vektory euklidovského prostoru* V *jsou lineárně nezávislé.*

Důkaz. Nechť $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k \in V$ jsou nenulové ortogonální vektory. Nechť $r_1 \cdot \boldsymbol{u}_1 + \cdots + r_k \cdot \boldsymbol{u}_k = \boldsymbol{o}$.

Provedeme-li (pro libovolné $i = 1, \dots, k$) skalární součin vektoru $\boldsymbol{u}_i$ s oběma stranami této rovnosti, dostaneme:

$$(r_1 \cdot \boldsymbol{u}_1 + \cdots + r_k \cdot \boldsymbol{u}_k) \cdot \boldsymbol{u}_i = \boldsymbol{o} \cdot \boldsymbol{u}_i,$$

odkud po rozepsání a s využitím ortogonálnosti zadaných vektorů dostáváme $r_i \cdot (\boldsymbol{u}_i \cdot \boldsymbol{u}_i) = 0$.

Protože však $\boldsymbol{u}_i \neq \boldsymbol{o}$, je $\boldsymbol{u}_i \cdot \boldsymbol{u}_i \neq 0$, a musí tedy být $r_i = 0$ (pro každé $i = 1, \dots, k$). To však znamená, že vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ jsou lineárně nezávislé.

□

Poznamenejme, že předpoklad nenulovosti všech vektorů je v předchozí větě podstatný a bez něj věta neplatí. Jinak řečeno, jsou-li ortogonální vektory z V lineárně závislé, znamená to, že alespoň jeden z nich musí být nulový.

Věta 2.3. *Nechť* V *je euklidovský prostor,* $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k \in V$ *libovolné. Pak existují ve* V *ortogonální vektory* $\boldsymbol{e}_1, \dots, \boldsymbol{e}_k$*, které generují tentýž podprostor jako vektory* $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$*, tzn. platí:*

$$L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k) = L(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k).$$

Důkaz. Provedeme matematickou indukcí vzhledem ke k.

α) Pro $k = 1$ tvrzení platí (stačí položit $\boldsymbol{e}_1 = \boldsymbol{u}_1$).

β) Předpokládejme, že tvrzení věty platí pro $i = 1, 2, \ldots, k-1$ ($k \geq 2$). Tedy existují ortogonální vektory $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_{k-1}$ tak, že platí:

$$L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{k-1}) = L(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_{k-1}). \tag{2}$$

Položme:

$$\boldsymbol{e}_k = p_1 \cdot \boldsymbol{e}_1 + \cdots + p_{k-1} \cdot \boldsymbol{e}_{k-1} + \boldsymbol{u}_k, \tag{3}$$

kde $p_i \in \mathbb{R}$, a určíme koeficienty p_i tak, aby $\boldsymbol{e}_k \cdot \boldsymbol{e}_i = 0$ pro $i = 1, \ldots, k-1$. Ale po provedení skalárního součinu vektoru $\boldsymbol{e}_i$ s oběma stranami (3) dostaneme:

$$\boldsymbol{e}_k \cdot \boldsymbol{e}_i = 0 = p_i \cdot (\boldsymbol{e}_i \cdot \boldsymbol{e}_i) + (\boldsymbol{u}_k \cdot \boldsymbol{e}_i),$$

odkud:

$$p_i = \begin{cases} -\frac{\boldsymbol{u}_k \cdot \boldsymbol{e}_i}{\boldsymbol{e}_i \cdot \boldsymbol{e}_i} & \text{je-li } \boldsymbol{e}_i \neq \boldsymbol{o} \\ \text{libovolné} & \text{je-li } \boldsymbol{e}_i = \boldsymbol{o} \end{cases}$$

Potom tedy vektory $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k$ jsou ortogonální.

Zbývá nám ještě dokázat rovnost $L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k) = L(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k)$. Ale z (2) a (3) plyne jednak, že $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k \in L(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k)$, tzn. $L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k) \subseteq L(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k)$, a také, že $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k \in L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k)$, tzn. $L(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k) \subseteq L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k)$. Dohromady pak dostáváme žádanou rovnost. □

Poznámka. 1. Důkaz předchozí věty byl konstruktivní a jeho algoritmus se nazývá *Gram-Schmidtův ortogonalizační proces* (používá se při řešení konkrétních příkladů!).

2. V předchozí větě se nic nepředpokládá o lineární závislosti nebo nezávislosti vektorů $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$. Proto výsledné ortogonální vektory $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k$ mohou, ale nemusí být všechny nenulové. Přesněji řečeno, je-li $\dim L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k) = r$ ($\leq k$), pak tedy i $\dim L(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k) = r$, což znamená, že právě $(k - r)$ z vektorů $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k$ je nulových a zbývajících r vektorů je nenulových a tvoří ortogonální bázi podprostoru $L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k)$, tj. podprostoru generovaného vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$.

Specielně tedy, jsou-li vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ lineárně nezávislé, tzn. tvoří bázi podprostoru $L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k)$, pak vektory $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k$ tvoří ortogonální bázi tohoto podprostoru.

Věta 2.4. *V každém nenulovém euklidovském prostoru V existuje ortogonální báze (resp. ortonormální báze).*

Důkaz. Nechť $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ je libovolná báze V. Pak podle předchozí věty a poznámky existuje ortogonální báze $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ prostoru V. Normováním každého z vektorů $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ pak dostaneme ortonormální bázi $\frac{1}{\|\boldsymbol{e}_1\|} \cdot \boldsymbol{e}_1, \ldots, \frac{1}{\|\boldsymbol{e}_n\|} \cdot \boldsymbol{e}_n$ prostoru V. □

Příklad 2.1. V euklidovském prostoru $\mathbb{R}^4$ se skalárním součinem definovaným:

$$(x_1, x_2, x_3, x_4) \cdot (y_1, y_2, y_3, y_4) = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$$

nalezněte ortogonální bázi podprostoru W generovaného vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3$. Přitom:

$$\boldsymbol{u}_1 = (0, 1, 2, 1), \;\; \boldsymbol{u}_2 = (-1, 1, 1, 1), \;\; \boldsymbol{u}_3 = (1, 0, 1, 0).$$

Řešení: Platí $W = L(\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3)$, tzn. použijeme Gram-Schmidtova ortogonalizačního procesu:

$\boldsymbol{e}_1 = \boldsymbol{u}_1 = (0, 1, 2, 1)$.

$\boldsymbol{e}_2 = p \cdot \boldsymbol{e}_1 + \boldsymbol{u}_2$, kde $p = -\frac{\boldsymbol{u}_2 \cdot \boldsymbol{e}_1}{\boldsymbol{e}_1 \cdot \boldsymbol{e}_1} = -\frac{2}{3}$. Tedy $\boldsymbol{e}_2 = (-1, \frac{1}{3}, -\frac{1}{3}, \frac{1}{3})$.

$\boldsymbol{e}_3 = p_1 \cdot \boldsymbol{e}_1 + p_2 \cdot \boldsymbol{e}_2 + \boldsymbol{u}_3$, kde $p_1 = -\frac{\boldsymbol{u}_3 \cdot \boldsymbol{e}_1}{\boldsymbol{e}_1 \cdot \boldsymbol{e}_1} = -\frac{1}{3}$, $p_2 = -\frac{\boldsymbol{u}_3 \cdot \boldsymbol{e}_2}{\boldsymbol{e}_2 \cdot \boldsymbol{e}_2} = 1$. Tedy $\boldsymbol{e}_3 = -\frac{1}{3} \cdot \boldsymbol{e}_1 + \boldsymbol{e}_2 + \boldsymbol{u}_3 = (0, 0, 0, 0) = \boldsymbol{o}$.

Výsledek: ortogonální bázi podprostoru W tvoří např. vektory $\boldsymbol{e}_1, \boldsymbol{e}_2$.

Definice. Nechť A, B jsou libovolné podmnožiny euklidovského prostoru V. Je-li:

$$\boldsymbol{a} \cdot \boldsymbol{b} = 0 \;\text{ pro každé } \boldsymbol{a} \in A, \, \boldsymbol{b} \in B,$$

pak říkáme, že A, B jsou *ortogonální množiny* a píšeme $A \perp B$ nebo $B \perp A$.

Poznámka. Jinak řečeno, A, B jsou ortogonální množiny, právě když $\boldsymbol{a}, \boldsymbol{b}$ jsou ortogonální vektory pro každé $\boldsymbol{a} \in A$, $\boldsymbol{b} \in B$.

Ve specielních případech: prázdná množina, resp. množina $\{\boldsymbol{o}\}$ jsou zřejmě ortogonální ke každé podmnožině ve V. Dále z definice plyne, že:

$$A \perp B \implies A \cap B = \emptyset \text{ nebo } A \cap B = \{\boldsymbol{o}\}.$$

Následující věta pak ukáže, že při studiu ortogonálních množin bude mít smysl omezit se pouze na podprostory euklidovského prostoru V.

Věta 2.5. *Nechť A, B jsou podmnožiny euklidovského prostoru V. Pak platí:*

$$A \perp B \iff [A] \perp [B],$$

tzn. dvě množiny jsou ortogonální, právě když jsou ortogonální podprostory generované těmito množinami.

Důkaz. „$\Leftarrow$“: Plyne z definice, uvědomíme-li si, že $A \subseteq [A]$, $B \subseteq [B]$.

„$\Rightarrow$“: Pro $A = \emptyset$ nebo $B = \emptyset$ tvrzení zřejmě platí (neboť $[\emptyset] = \{\boldsymbol{o}\}$). Předpokládejme tedy $A \neq \emptyset$, $B \neq \emptyset$ a $A \perp B$. Nechť dále $\boldsymbol{u} \in [A]$, $\boldsymbol{v} \in [B]$ libovolné. Ale podprostor $[A]$ je roven množině všech lineárních kombinací konečně mnoha vektorů z A (plyne z věty 2.3. (2), kap. I. – rozepište si podrobně sami!), tzn. $\boldsymbol{u} = p_1 \cdot \boldsymbol{a}_1 + \cdots + p_k \cdot \boldsymbol{a}_k$, kde $\boldsymbol{a}_i \in A$, a podobně $\boldsymbol{v} = r_1 \cdot \boldsymbol{b}_1 + \cdots + r_m \cdot \boldsymbol{b}_m$, kde $\boldsymbol{b}_j \in B$. Potom však:

$$\boldsymbol{u} \cdot \boldsymbol{v} = \left(\sum_{i=1}^{k} p_i \cdot \boldsymbol{a}_i\right) \cdot \left(\sum_{j=1}^{m} r_j \cdot \boldsymbol{b}_j\right) = \sum_{i=1}^{k}\sum_{j=1}^{m} p_i r_j \cdot (\boldsymbol{a}_i \cdot \boldsymbol{b}_j) = 0,$$

neboť $\boldsymbol{a}_i \cdot \boldsymbol{b}_j = 0$. Tedy platí $[A] \perp [B]$, což jsme měli dokázat. □

Definice. Nechť W je podprostor euklidovského prostoru V. Pak množina:

$$W^{\perp} = \{\boldsymbol{x} \in V \mid \boldsymbol{x} \cdot \boldsymbol{w} = 0 \text{ pro každé } \boldsymbol{w} \in W\}$$

se nazývá *ortogonální doplněk podprostoru W* (ve V).

Poznámka. Zřejmě platí $W \perp W^{\perp}$ a ve specielních případech přímo z definice dostáváme, že $V^{\perp} = \{\boldsymbol{o}\}$, resp. $\{\boldsymbol{o}\}^{\perp} = V$.

Základní obecné vlastnosti ortogonálního doplňku pak popisují následující věty.

Věta 2.6. *Nechť W je podprostor euklidovského prostoru V. Pak platí:*
(1) *$W^{\perp}$ je podprostor ve V,*
(2) *$V = W \dot{+} W^{\perp}$, tzn. prostor V je přímým součtem podprostorů W a $W^{\perp}$.*

Důkaz. (1): Zřejmě $\boldsymbol{o} \in W^{\perp}$, a tedy $W^{\perp} \neq \emptyset$. Dále nechť $\boldsymbol{x}, \boldsymbol{y} \in W^{\perp}$, $r \in \mathbb{R}$ libovolné. Pak pro libovolný vektor $\boldsymbol{w} \in W$ je:

$$(\boldsymbol{x} + \boldsymbol{y}) \cdot \boldsymbol{w} = (\boldsymbol{x} \cdot \boldsymbol{w}) + (\boldsymbol{y} \cdot \boldsymbol{w}) = 0 + 0 = 0,$$

resp.

$$(r \cdot \boldsymbol{x}) \cdot \boldsymbol{w} = r \cdot (\boldsymbol{x} \cdot \boldsymbol{w}) = r \cdot 0 = 0,$$

a tedy $W^\perp$ je podprostor ve V.

(2): Je-li $W = \{\boldsymbol{o}\}$, pak $W^\perp = V$ a tvrzení platí. Nechť tedy $W \neq \{\boldsymbol{o}\}$ a nechť $\boldsymbol{e}_1, \dots, \boldsymbol{e}_k$ je ortonormální báze W (její existence je zaručena větou 2.4.).

a) Dokážeme, že $W + W^\perp = V$. Zřejmě stačí dokázat inkluzi „$\supseteq$“. Nechť tedy $\boldsymbol{u} \in V$ libovolný. Označme:

$$\boldsymbol{x} = (\boldsymbol{u} \cdot \boldsymbol{e}_1) \cdot \boldsymbol{e}_1 + \dots + (\boldsymbol{u} \cdot \boldsymbol{e}_k) \cdot \boldsymbol{e}_k.$$

Pak zřejmě $\boldsymbol{x} \in W$. Dále vezměme vektor $(-\boldsymbol{x} + \boldsymbol{u})$ a spočtěme:

$$(-\boldsymbol{x} + \boldsymbol{u}) \cdot \boldsymbol{e}_i = -(\boldsymbol{x} \cdot \boldsymbol{e}_i) + (\boldsymbol{u} \cdot \boldsymbol{e}_i) = -(\boldsymbol{u} \cdot \boldsymbol{e}_i) + (\boldsymbol{u} \cdot \boldsymbol{e}_i) = 0$$

pro $i = 1, \dots, k$, odkud plyne, že $(-\boldsymbol{x} + \boldsymbol{u}) \in W^\perp$. Potom však $\boldsymbol{u} = \boldsymbol{x} + (-\boldsymbol{x} + \boldsymbol{u}) \in W + W^\perp$.

b) Platí $W \cap W^\perp = \{\boldsymbol{o}\}$, neboť $\boldsymbol{w} \in W \cap W^\perp \implies \boldsymbol{w} \cdot \boldsymbol{w} = 0 \implies \boldsymbol{w} = \boldsymbol{o}$. Dohromady pak dostáváme, že $V = W \dot{+} W^\perp$. □

Poznámka. Je-li W libovolný podprostor ve V, pak (podle 2. části předchozí věty a podle definice přímého součtu podprostorů) se libovolný vektor $\boldsymbol{u} \in V$ dá napsat, a to jediným způsobem, ve tvaru:

$$\boldsymbol{u} = \boldsymbol{x} + \boldsymbol{y},$$

kde $\boldsymbol{x} \in W$, $\boldsymbol{y} \in W^\perp$.

Poznamenejme, že vektor $\boldsymbol{x}$ z tohoto vyjádření se nazývá *ortogonální projekce vektoru $\boldsymbol{u}$ do podprostoru W*. Následující věta ukáže, že ortogonální projekce součtu dvou vektorů je rovna součtu jejich ortogonálních projekcí a podobně tomu je pro násobek vektoru.

Věta 2.7. *Nechť W je podprostor euklidovského prostoru V, nechť $\boldsymbol{x}$ (resp. $\boldsymbol{x}'$) je ortogonální projekce vektoru $\boldsymbol{u}$ (resp. $\boldsymbol{u}'$) do podprostoru W a nechť $r \in \mathbb{R}$ libovolné. Pak platí:*

(1) *$(\boldsymbol{x} + \boldsymbol{x}')$ je ortogonální projekce vektoru $(\boldsymbol{u} + \boldsymbol{u}')$ do W,*

(2) *$r \cdot \boldsymbol{x}$ je ortogonální projekce vektoru $r \cdot \boldsymbol{u}$ do W.*

Důkaz. Podle předpokladu je $\boldsymbol{u} = \boldsymbol{x} + \boldsymbol{y}$, $\boldsymbol{u}' = \boldsymbol{x}' + \boldsymbol{y}'$, kde $\boldsymbol{x}, \boldsymbol{x}' \in W$, $\boldsymbol{y}, \boldsymbol{y}' \in W^{\perp}$. Potom:

(1): $(\boldsymbol{u} + \boldsymbol{u}') = (\boldsymbol{x} + \boldsymbol{y}) + (\boldsymbol{x}' + \boldsymbol{y}') = (\boldsymbol{x} + \boldsymbol{x}') + (\boldsymbol{y} + \boldsymbol{y}')$, kde $\boldsymbol{x} + \boldsymbol{x}' \in W$, $\boldsymbol{y} + \boldsymbol{y}' \in W^{\perp}$,

(2): $r \cdot \boldsymbol{u} = r \cdot (\boldsymbol{x} + \boldsymbol{y}) = r \cdot \boldsymbol{x} + r \cdot \boldsymbol{y}$, kde $r \cdot \boldsymbol{x} \in W$, $r \cdot \boldsymbol{y} \in W^{\perp}$,
odkud již podle předchozí poznámky plyne tvrzení. □

Věta 2.8. *Nechť W, S jsou podprostory euklidovského prostoru V. Pak platí:*
(1) $(W^{\perp})^{\perp} = W$,
(2) $(W + S)^{\perp} = W^{\perp} \cap S^{\perp}$,
(3) $(W \cap S)^{\perp} = W^{\perp} + S^{\perp}$.

Důkaz. (1): Podle věty 2.6. je $W \dot{+} W^{\perp} = V$ a také $W^{\perp} \dot{+} (W^{\perp})^{\perp} = V$, odkud plyne, že $\dim W = \dim V - \dim W^{\perp} = \dim (W^{\perp})^{\perp}$. Je tedy $\dim W = \dim (W^{\perp})^{\perp}$, přičemž zřejmě $W \subseteq (W^{\perp})^{\perp}$, tzn. pak (podle věty 4.5. (2), kap. I.) je $W = (W^{\perp})^{\perp}$.

(2): Inkluze „$\subseteq$“ je zřejmá. Dokážeme inkluzi „$\supseteq$“. Nechť $\boldsymbol{x} \in W^{\perp} \cap S^{\perp}$ a nechť $\boldsymbol{u} \in (W + S)$ je libovolný, tzn. $\boldsymbol{u} = \boldsymbol{w} + \boldsymbol{s}$, kde $\boldsymbol{w} \in W$, $\boldsymbol{s} \in S$. Potom:

$$\boldsymbol{x} \cdot \boldsymbol{u} = \boldsymbol{x} \cdot (\boldsymbol{w} + \boldsymbol{s}) = \boldsymbol{x} \cdot \boldsymbol{w} + \boldsymbol{x} \cdot \boldsymbol{s} = 0 + 0 = 0,$$

a tedy je $\boldsymbol{x} \in (W + S)^{\perp}$. Je tedy $W^{\perp} \cap S^{\perp} \subseteq (W + S)^{\perp}$ a dohromady platí žádaná rovnost.

(3): Užitím (1) a (2) dostáváme:

$$(W \cap S) = (W^{\perp})^{\perp} \cap (S^{\perp})^{\perp} = (W^{\perp} + S^{\perp})^{\perp},$$

odkud:

$$(W \cap S)^{\perp} = \big((W^{\perp} + S^{\perp})^{\perp}\big)^{\perp} = W^{\perp} + S^{\perp}.$$

□

Kapitola 5

Lineární zobrazení vektorových prostorů

§1. Základní vlastnosti lineárního zobrazení

V našich předchozích úvahách o vektorových prostorech jsme vždy vyšetřovali vlastnosti jednoho vektorového prostoru (pro úplnost připomeňme, že vektorovým prostorem rozumíme vždy konečnědimenzionální vektorový prostor). V této kapitole se naopak budeme zabývat vzájemnými vztahy mezi dvěma (případně i více) vektorovými prostory. Tyto „vzájemné vztahy" budeme studovat pomocí zobrazení jednoho vektorového prostoru do druhého. Aby naše úvahy měly praktický smysl, bude zřejmě nutné pracovat s takovými zobrazeními, která nějakým způsobem „zachovávají" operace, s nimiž se ve vektorových prostorech setkáváme, tj. zachovávají jednak součet vektorů a jednak násobek čísla s vektorem. Přitom zřejmě druhý požadavek bude moci být splněn jen tehdy, když uvažované vektorové prostory budou nad stejným číselným tělesem.

Definice. Nechť V, V' jsou vektorové prostory nad týmž číselným tělesem T. Zobrazení $\varphi : V \to V'$ splňující:
(1) $\varphi(\boldsymbol{u} + \boldsymbol{v}) = \varphi(\boldsymbol{u}) + \varphi(\boldsymbol{v})$,
(2) $\varphi(t \cdot \boldsymbol{u}) = t \cdot \varphi(\boldsymbol{u})$
pro $\boldsymbol{u}, \boldsymbol{v} \in V$, $t \in T$ libovolné se nazývá *lineární zobrazení* vektorového prostoru V do V'.

Je-li navíc φ bijektivní, pak se nazývá *izomorfismus vektorového prostoru V na V'*.

Poznámka. 1. Je nutné si uvědomit, že vektorové prostory V a V' jsou obecně různé, a tedy i operace sčítání vektorů (resp. násobení čísla s vektorem) ve V a ve V' jsou pak samozřejmě také různé. Přesto však je budeme pro jednoduchost označovat stejným symbolem $+$ (resp. $\cdot$). Nebude moci dojít k nedorozumění, poněvadž ze souvislosti a z ostatní symboliky bude vždy zřejmé, o kterou operaci se jedná. Pro ulehčení orientace budeme vektory z V' obvykle označovat čárkovaně, kdežto vektory z V nečárkovaně. Specielně tedy $\boldsymbol{o}'$ bude značit nulový vektor z V', kdežto $\boldsymbol{o}$ bude značit nulový vektor z V.

2. Lehce se ukáže, že podmínky (1) a (2) z předchozí definice jsou ekvivalentní jediné podmínce:

(3) $\varphi(t \cdot \boldsymbol{u} + s \cdot \boldsymbol{v}) = t \cdot \varphi(\boldsymbol{u}) + s \cdot \varphi(\boldsymbol{v})$ pro $\boldsymbol{u}, \boldsymbol{v} \in V$, $t, s \in T$ libovolné.

Ověřujeme-li tedy, že zobrazení $\varphi : V \to V'$ je lineární zobrazení, pak ověřujeme buď podmínky (1) a (2), nebo jedinou podmínku (3).

Dále, matematickou indukcí lze (3) rozšířit na libovolný konečný počet sčítanců, tzn. pro lineární zobrazení φ platí:

$$\varphi(t_1 \cdot \boldsymbol{u}_1 + \cdots + t_k \cdot \boldsymbol{u}_k) = t_1 \cdot \varphi(\boldsymbol{u}_1) + \cdots + t_k \cdot \varphi(\boldsymbol{u}_k).$$

Příklad 1.1. Nechť V, V' jsou vektorové prostory nad T, nechť $t \in T$. Pak:

1. Zobrazení $\varphi : V \to V$ definované:

$$\varphi(\boldsymbol{u}) = t \cdot \boldsymbol{u} \quad \text{pro každé } \boldsymbol{u} \in V$$

je lineární zobrazení. Je-li $t \neq 0$, pak φ je dokonce izomorfismus (ověřte si obojí rozepsáním!). Specielně, pro $t = 1$ dostáváme identické zobrazení id_V, které je tedy izomorfismem vektorového prostoru V na V.

2. Zobrazení $\omega : V \to V'$ definované:

$$\omega(\boldsymbol{u}) = \boldsymbol{o}' \quad \text{pro každé } \boldsymbol{u} \in V$$

je lineární zobrazení, které budeme nazývat *nulové lineární zobrazení.*

Příklad 1.2. Zobrazení $\varphi : \mathbb{R}^3 \to \mathbb{R}^2$ definované:

$$\varphi\big((x_1, x_2, x_3)\big) = (2x_1 + x_3, x_1 - x_2 - x_3) \quad \text{pro } \forall (x_1, x_2, x_3) \in \mathbb{R}^3$$

je lineární zobrazení, které není izomorfismem.

Dále, např. zobrazení $\psi : \mathbb{R}^3 \to \mathbb{R}^2$ definované:

$$\psi\big((x_1, x_2, x_3)\big) = (2x_1 + 1, x_1 - x_2 - x_3) \quad \text{pro } \forall (x_1, x_2, x_3) \in \mathbb{R}^3$$

není lineární zobrazení (zřejmě neplatí (1) ani (2)).

Příklad 1.3. Zobrazení $\delta : \mathbb{R}_n[x] \to \mathbb{R}_n[x]$ definované:

$$\delta\big(f(x)\big) = f'(x) \quad \text{pro } \forall f(x) \in \mathbb{R}_n[x],$$

tj. zobrazení přiřazující polynomu $f(x)$ jeho derivaci $f'(x)$, je lineární zobrazení (při ověřování podmínek (1) a (2) se využije některých vět o derivování funkcí známých z analýzy). Zřejmě δ není bijektivní zobrazení, a tedy není izomorfismem.

Věta 1.1. *Nechť $\varphi : V \to V'$ je lineární zobrazení. Pak platí:*

(1) $\varphi(\boldsymbol{o}) = \boldsymbol{o}'$, *tj. nulový vektor se musí zobrazit na nulový vektor,*

(2) $\varphi(-\boldsymbol{u}) = -\varphi(\boldsymbol{u})$ *pro* $\forall \boldsymbol{u} \in V$,

(3) $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k \in V$ *jsou lineárně závislé vektory* $\implies$ $\varphi(\boldsymbol{u}_1), \dots, \varphi(\boldsymbol{u}_k)$ *jsou lineárně závislé vektory (ve V').*

Důkaz. (1): Zřejmě je $\boldsymbol{o} = 0 \cdot \boldsymbol{o}$, tzn. pak $\varphi(\boldsymbol{o}) = \varphi(0 \cdot \boldsymbol{o}) = 0 \cdot \varphi(\boldsymbol{o}) = \boldsymbol{o}'$.

(2): $\varphi(-\boldsymbol{u}) = \varphi\big((-1) \cdot \boldsymbol{u}\big) = (-1) \cdot \varphi(\boldsymbol{u}) = -\varphi(\boldsymbol{u})$ podle věty 1.1. (4), kap. I.

(3): $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ jsou lineárně závislé $\implies$ existují $t_1, \dots, t_n \in T$, z nichž alespoň jedno je různé od nuly, tak, že $t_1 \cdot \boldsymbol{u}_1 + \dots + t_k \cdot \boldsymbol{u}_k = \boldsymbol{o}$. Pak ale $\varphi(t_1 \cdot \boldsymbol{u}_1 + \dots + t_k \cdot \boldsymbol{u}_k) = \varphi(\boldsymbol{o})$, tzn. $t_1 \cdot \varphi(\boldsymbol{u}_1) + \dots + t_k \cdot \varphi(\boldsymbol{u}_k) = \boldsymbol{o}'$, a tedy $\varphi(\boldsymbol{u}_1), \dots, \varphi(\boldsymbol{u}_k)$ jsou lineárně závislé. $\square$

Další věta si všímá toho, jak se lineární zobrazení chová vůči podprostorům. Připomeňme, že je-li $\varphi : V \to V'$ zobrazení a W je podmnožina ve V, pak symbolem $\varphi(W)$ označujeme množinu obrazů všech prvků z W, tj.:

$$\varphi(W) = \{\boldsymbol{x}' \in V' \mid \exists \boldsymbol{w} \in W \text{ tak, že } \varphi(\boldsymbol{w}) = \boldsymbol{x}'\}.$$

Věta 1.2. *Nechť $\varphi : V \to V'$ je lineární zobrazení, W podprostor ve V. Pak:*

(1) $\varphi(W)$ *je podprostor ve* V',

(2) $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ *jsou generátory podprostoru* W $\implies$ $\varphi(\boldsymbol{u}_1), \dots, \varphi(\boldsymbol{u}_k)$ *jsou generátory podprostoru* $\varphi(W)$,

(3) $\dim W \geq \dim \varphi(W)$.

Důkaz. (1): Provede se přímým ověřením definice podprostoru.

(2): Nechť $\boldsymbol{x}' \in \varphi(W)$ libovolný, tzn. existuje $\boldsymbol{w} \in W$ tak, že $\varphi(\boldsymbol{w}) = \boldsymbol{x}'$. Ale podle předpokladu $\boldsymbol{w} = t_1 \cdot \boldsymbol{u}_1 + \cdots + t_k \cdot \boldsymbol{u}_k$, a tedy $\boldsymbol{x}' = \varphi(t_1 \cdot \boldsymbol{u}_1 + \cdots + t_k \cdot \boldsymbol{u}_k) = t_1 \cdot \varphi(\boldsymbol{u}_1) + \cdots + t_k \cdot \varphi(\boldsymbol{u}_k)$, odkud plyne, že $\varphi(\boldsymbol{u}_1), \ldots, \varphi(\boldsymbol{u}_k)$ jsou generátory $\varphi(W)$.

(3): Je-li $W = \{\boldsymbol{o}\}$, pak tvrzení zřejmě platí. Nechť tedy $W \neq \{\boldsymbol{o}\}$ a nechť $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m$ je báze W. Pak podle (2) jsou vektory $\varphi(\boldsymbol{u}_1), \ldots, \varphi(\boldsymbol{u}_m)$ generátory $\varphi(W)$, a tedy $\dim \varphi(W) \leq m = \dim W$. □

Věta 1.3. *Složením lineárních zobrazení dostaneme opět lineární zobrazení, tj. jsou-li $\varphi : V \to V'$, $\psi : V' \to V''$ lineární zobrazení, pak $\psi \circ \varphi : V \to V''$ je lineární zobrazení.*

Důkaz. Ověříme podmínku (3). Pro $\boldsymbol{u}, \boldsymbol{v} \in V$, $t, s \in T$ je:

$$(\psi \circ \varphi)(t \cdot \boldsymbol{u} + s \cdot \boldsymbol{v}) = \psi\big(\varphi(t \cdot \boldsymbol{u} + s \cdot \boldsymbol{v})\big) = \psi\big(t \cdot \varphi(\boldsymbol{u}) + s \cdot \varphi(\boldsymbol{v})\big) = \\ t \cdot \big((\psi \circ \varphi)(\boldsymbol{u})\big) + s \cdot \big((\psi \circ \varphi)(\boldsymbol{v})\big),$$

a tedy $(\psi \circ \varphi)$ je lineární zobrazení. □

Následující důležitá věta ukáže, že k úplnému zadání lineárního zobrazení $V \to V'$ stačí zadat pouze obrazy vektorů pevné báze prostoru V a obrazy zbývajících vektorů z V jsou pak již jednoznačně vynuceny. Na druhé straně, takovýto výsledek se dá celkem očekávat, uvědomíme-li si, že každý vektor z V je jistou lineární kombinací vektorů báze a že lineární zobrazení „zachovává lineární kombinace vektorů“.

Věta 1.4. (Základní věta o lineárních zobrazeních) *Nechť V, V' jsou vektorové prostory nad T, nechť $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ je báze prostoru V a nechť $\boldsymbol{v}'_1, \ldots, \boldsymbol{v}'_n$ jsou libovolné vektory z V'. Pak existuje jediné lineární zobrazení $\varphi : V \to V'$ takové, že $\varphi(\boldsymbol{u}_1) = \boldsymbol{v}'_1$, …, $\varphi(\boldsymbol{u}_n) = \boldsymbol{v}'_n$.*

Důkaz. I. existence: Nechť $\boldsymbol{x} \in V$ libovolný, přičemž $\boldsymbol{x} = x_1 \cdot \boldsymbol{u}_1 + \cdots + x_n \cdot \boldsymbol{u}_n$. Položme $\varphi(\boldsymbol{x}) = x_1 \cdot \boldsymbol{v}'_1 + \cdots + x_n \cdot \boldsymbol{v}'_n$. Potom φ je zobrazení V do V', které je lineární zobrazení (obojí si podrobně rozmyslete, resp. dokažte!). Dále, zřejmě $\varphi(\boldsymbol{u}_i) = \boldsymbol{v}'_i$ pro $i = 1, \ldots, n$.

II. jednoznačnost: Nechť φ je výše zkonstruované lineární zobrazení a nechť dále $\psi : V \to V'$ je lineární zobrazení takové, že $\psi(\boldsymbol{u}_1) = \boldsymbol{v}'_1$, …, $\psi(\boldsymbol{u}_n) = \boldsymbol{v}'_n$. Pak pro libovolný vektor $\boldsymbol{x} \in V$ (pro nějž $\boldsymbol{x} = x_1 \cdot \boldsymbol{u}_1 + \cdots + x_n \cdot \boldsymbol{u}_n$) je:

$$\psi(\boldsymbol{x}) = \psi(x_1 \cdot \boldsymbol{u}_1 + \cdots + x_n \cdot \boldsymbol{u}_n) = x_1 \cdot \psi(\boldsymbol{u}_1) + \cdots + x_n \cdot \psi(\boldsymbol{u}_n) = \\ x_1 \cdot \boldsymbol{v}'_1 + \cdots + x_n \cdot \boldsymbol{v}'_n = \varphi(\boldsymbol{x}),$$

což však znamená, že $\psi = \varphi$. □

Definice. Nechť $\varphi : V \to V'$ je lineární zobrazení. Pak:
(1) množina $\operatorname{Ker}\varphi = \{\boldsymbol{u} \in V \mid \varphi(\boldsymbol{u}) = \boldsymbol{o}'\}$ se nazývá *jádro lineárního zobrazení* φ,
(2) množina $\operatorname{Im}\varphi = \varphi(V)$ se nazývá *obraz lineárního zobrazení* φ.

Poznámka. Označení $\operatorname{Ker}\varphi$, resp. $\operatorname{Im}\varphi$ jsou v literatuře běžně používané zkratky pro anglické názvy „kernel“ = jádro, resp. „image“ = obraz.

Následující tvrzení ukáží, že obě podmnožiny jsou podprostory a popíší jejich základní vlastnosti.

Věta 1.5. *Nechť $\varphi : V \to V'$ je lineární zobrazení. Pak:*
(1) *jádro* $\operatorname{Ker}\varphi$ *je podprostorem ve V,*
(2) *obraz* $\operatorname{Im}\varphi$ *je podprostorem ve V'.*

Důkaz. (1): Zřejmě $\boldsymbol{o} \in \operatorname{Ker}\varphi$, a tedy $\operatorname{Ker}\varphi \neq \emptyset$. Dále, nechť $\boldsymbol{u}, \boldsymbol{v} \in \operatorname{Ker}\varphi$, tzn. je $\varphi(\boldsymbol{u}) = \boldsymbol{o}'$, $\varphi(\boldsymbol{v}) = \boldsymbol{o}'$. Pak $\varphi(\boldsymbol{u} + \boldsymbol{v}) = \varphi(\boldsymbol{u}) + \varphi(\boldsymbol{v}) = \boldsymbol{o}' + \boldsymbol{o}' = \boldsymbol{o}'$, a tedy $\boldsymbol{u} + \boldsymbol{v} \in \operatorname{Ker}\varphi$. Podobně pro $\boldsymbol{u} \in \operatorname{Ker}\varphi$ a $t \in T$ je $t \cdot \boldsymbol{u} \in \operatorname{Ker}\varphi$. Dohromady tedy $\operatorname{Ker}\varphi$ je podprostor ve V.

(2): Jde o speciální případ věty 1.2. (1). □

Věta 1.6. *Lineární zobrazení φ je injektivní* $\iff$ $\operatorname{Ker}\varphi = \{\boldsymbol{o}\}$.

Důkaz. „$\Rightarrow$“: Nechť $\boldsymbol{x} \in \operatorname{Ker}\varphi$ libovolný. Pak $\varphi(\boldsymbol{x}) = \boldsymbol{o}' = \varphi(\boldsymbol{o})$ užitím věty 1.1. (1). Z injektivnosti zobrazení φ pak dostáváme $\boldsymbol{x} = \boldsymbol{o}$, tzn. $\operatorname{Ker}\varphi = \{\boldsymbol{o}\}$,

„$\Leftarrow$“: Nechť $\varphi(\boldsymbol{u}) = \varphi(\boldsymbol{v})$. Potom $\varphi(\boldsymbol{u} - \boldsymbol{v}) = \boldsymbol{o}'$, neboli $\boldsymbol{u} - \boldsymbol{v} \in \operatorname{Ker}\varphi = \{\boldsymbol{o}\}$. Tedy $\boldsymbol{u} - \boldsymbol{v} = \boldsymbol{o}$, neboli $\boldsymbol{u} = \boldsymbol{v}$, což znamená, že φ je injektivní zobrazení. □

Definice. Nechť $\varphi : V \to V'$ je lineární zobrazení. Pak dimenze jádra $\operatorname{Ker}\varphi$ se nazývá *defekt lineárního zobrazení* φ a dimenze obrazu $\operatorname{Im}\varphi$ se nazývá *hodnost lineárního zobrazení* φ.

Věta 1.7. *Nechť $\varphi : V \to V'$ je lineární zobrazení. Pak součet defektu a hodnosti lineárního zobrazení φ je roven dimenzi prostoru V, tj.:*

$$\dim(\operatorname{Ker}\varphi) + \dim(\operatorname{Im}\varphi) = \dim V.$$

Důkaz. Je-li $\operatorname{Im}\varphi = \{\boldsymbol{o}'\}$, pak $\operatorname{Ker}\varphi = V$ a věta zřejmě platí. Nechť je tedy $\operatorname{Im}\varphi \neq \{\boldsymbol{o}'\}$ a nechť $\boldsymbol{w}'_1, \dots, \boldsymbol{w}'_r$ je báze $\operatorname{Im}\varphi$. Pak existují vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_r \in V$ tak, že $\varphi(\boldsymbol{u}_1) = \boldsymbol{w}'_1, \dots, \varphi(\boldsymbol{u}_r) = \boldsymbol{w}'_r$. Z věty 1.1. (3) plyne, že $\boldsymbol{u}_1, \dots, \boldsymbol{u}_r$ jsou lineárně nezávislé, tzn. je pak:

$$\dim L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_r) = r = \dim(\operatorname{Im}\varphi). \tag{1}$$

Dále:

I. Ukážeme, že $\operatorname{Ker}\varphi + L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_r) = V$.
Ale inkluze „$\subseteq$“ je zřejmá a naopak, je-li $\boldsymbol{x} \in V$ libovolný, pak $\varphi(\boldsymbol{x}) \in \operatorname{Im}\varphi$, tzn. $\varphi(\boldsymbol{x}) = c_1 \cdot \boldsymbol{w}'_1 + \dots + c_r \cdot \boldsymbol{w}'_r$, kde $c_i \in T$. Uvažme nyní vektor $\boldsymbol{u} = c_1 \cdot \boldsymbol{u}_1 + \dots + c_r \cdot \boldsymbol{u}_r$. Zřejmě je $\boldsymbol{u} \in L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_r)$ a dále:

$$\begin{gathered}\varphi(\boldsymbol{u}) = \varphi(c_1 \cdot \boldsymbol{u}_1 + \dots + c_r \cdot \boldsymbol{u}_r) = c_1 \cdot \varphi(\boldsymbol{u}_1) + \dots + c_r \cdot \varphi(\boldsymbol{u}_r) = \\ c_1 \cdot \boldsymbol{w}'_1 + \dots + c_r \cdot \boldsymbol{w}'_r = \varphi(\boldsymbol{x}),\end{gathered}$$

odkud $\varphi(\boldsymbol{x} - \boldsymbol{u}) = \boldsymbol{o}'$, neboli $\boldsymbol{x} - \boldsymbol{u} \in \operatorname{Ker}\varphi$. Potom však:

$$\boldsymbol{x} = (\boldsymbol{x} - \boldsymbol{u}) + \boldsymbol{u} \in \operatorname{Ker}\varphi + L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_r),$$

což jsme potřebovali dokázat.

II. Ukážeme, že $\operatorname{Ker}\varphi \cap L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_r) = \{\boldsymbol{o}\}$.
Nechť $\boldsymbol{x} \in \operatorname{Ker}\varphi \cap L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_r)$. Pak $\varphi(\boldsymbol{x}) = \boldsymbol{o}'$ a současně $\boldsymbol{x} = t_1 \cdot \boldsymbol{u}_1 + \dots + t_r \cdot \boldsymbol{u}_r$, odkud:

$$\boldsymbol{o}' = \varphi(\boldsymbol{x}) = t_1 \cdot \varphi(\boldsymbol{u}_1) + \dots + t_r \cdot \varphi(\boldsymbol{u}_r) = t_1 \cdot \boldsymbol{w}'_1 + \dots + t_r \cdot \boldsymbol{w}'_r.$$

Ale z lineární nezávislosti vektorů $\boldsymbol{w}'_1, \dots, \boldsymbol{w}'_r$ plyne, že $t_1 = \dots = t_r = 0$, a tedy po dosazení dostáváme $\boldsymbol{x} = \boldsymbol{o}$.

Nyní, z I. a II. užitím věty o součtu a průniku podprostorů a vztahu (1) dostáváme:

$$\begin{gathered}\dim V = \dim\big(\operatorname{Ker}\varphi + L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_r)\big) = \\ \dim\operatorname{Ker}\varphi + \dim L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_r) - \dim\big(\operatorname{Ker}\varphi \cap L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_r)\big) = \\ \dim\operatorname{Ker}\varphi + \dim\operatorname{Im}\varphi - 0 = \dim\operatorname{Ker}\varphi + \dim\operatorname{Im}\varphi.\end{gathered}$$

□

Definice. Nechť V, V' jsou vektorové prostory nad T a nechť existuje izomorfismus vektorového prostoru V na V'. Pak říkáme, že V a V' jsou *izomorfní vektorové prostory* a píšeme $V \cong V'$.

Věta 1.8. *Relace $\cong$ je relací ekvivalence na množině všech (konečnědimenzionálních) vektorových prostorů nad tělesem T.*

Důkaz. reflexivita: Je zřejmá (neboť id_V je izomorfismus V na V).

symetrie: Nechť $V \cong V'$, tzn. existuje izomorfismus $\varphi : V \to V'$. Pak zobrazení $\varphi^{-1} : V' \to V$ je bijektivní a ukážeme, že je lineární zobrazení. Nechť $\boldsymbol{u}', \boldsymbol{v}' \in V'$, $t, s \in T$ libovolné a označme $\varphi^{-1}(\boldsymbol{u}') = \boldsymbol{u}$, $\varphi^{-1}(\boldsymbol{v}') = \boldsymbol{v}$. Potom je $\varphi(\boldsymbol{u}) = \boldsymbol{u}'$, $\varphi(\boldsymbol{v}) = \boldsymbol{v}'$. Nyní:

$$\varphi^{-1}(t \cdot \boldsymbol{u}' + s \cdot \boldsymbol{v}') = \varphi^{-1}\big(t \cdot \varphi(\boldsymbol{u}) + s \cdot \varphi(\boldsymbol{v})\big) = \varphi^{-1}\big(\varphi(t \cdot \boldsymbol{u} + s \cdot \boldsymbol{v})\big) = \\ t \cdot \boldsymbol{u} + s \cdot \boldsymbol{v} = t \cdot \varphi^{-1}(\boldsymbol{u}') + s \cdot \varphi^{-1}(\boldsymbol{v}').$$

Je tedy $V' \cong V$.

tranzitivita: Plyne z vlastností bijekce a z věty 1.3. □

Věta 1.9. *Nechť $\varphi : V \to V'$ je izomorfismus. Pak platí:*

(1) $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k \in V$ *jsou lineárně závislé* $\iff$ $\varphi(\boldsymbol{u}_1), \dots, \varphi(\boldsymbol{u}_k)$ *jsou lineárně závislé,*

(2) $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k \in V$ *jsou lineárně nezávislé* $\iff$ $\varphi(\boldsymbol{u}_1), \dots, \varphi(\boldsymbol{u}_k)$ *jsou lineárně nezávislé,*

(3) $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ *je báze* V $\iff$ $\varphi(\boldsymbol{u}_1), \dots, \varphi(\boldsymbol{u}_n)$ *je báze* V',

(4) $\dim V = \dim V'$.

Důkaz. Podle předpokladu je $\varphi : V \to V'$ bijektivní lineární zobrazení a podle důkazu předchozí věty je $\varphi^{-1} : V' \to V$ také bijektivní lineární zobrazení. Potom:

(1): Plyne z věty 1.1. (3) aplikované na φ, resp. φ^{-1}.

(2): Je logickým důsledkem (1).

(3): Plyne z (2) a z věty 1.2. (2), uvědomíme-li si, že $\varphi(V) = V'$ a $\varphi^{-1}(V') = V$.

(4): Je-li V nulovým prostorem, pak je tvrzení zřejmé. V ostatních případech plyne z (3). □

Poznámka. Utvoříme-li na množině všech (konečnědimenzionálních) vektorových prostorů nad T rozklad příslušný ekvivalenci $\cong$, pak v každé třídě tohoto rozkladu budou vždy všechny navzájem izomorfní vektorové prostory. Z věty 1.9. pak plyne, že tyto izomorfní vektorové prostory mají z algebraického hlediska naprosto stejné vlastnosti (jedná se tedy o pouze formálně různé exempláře shodných vlastností). V matematice se obvykle o takovýchto objektech říká, že jsou „stejné, až na izomorfismus“ a často se dokonce ztotožňují.

Následující věta pak podá velmi jednoduchou charakterizaci izomorfních vektorových prostorů, tj. vektorových prostorů patřících do jedné třídy zmíněného rozkladu.

Věta 1.10. (Věta o izomorfismu vektorových prostorů) *Nechť V, V' jsou vektorové prostory nad T. Pak:*

$$V \cong V' \iff \dim V = \dim V'.$$

Důkaz. „$\Rightarrow$“: Plyne přímo z věty 1.9. (4).

„$\Leftarrow$“: Je-li $\dim V = \dim V' = 0$, pak zřejmě $V \cong V'$. Nechť tedy $\dim V = \dim V' = n$ (≥ 1) a nechť $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ je báze V, resp. $\boldsymbol{u}'_1, \dots, \boldsymbol{u}'_n$ je báze V'. Nechť dále $\boldsymbol{x} \in V$ libovolný, přičemž $\boldsymbol{x} = x_1 \cdot \boldsymbol{u}_1 + \dots + x_n \cdot \boldsymbol{u}_n$ (víme, že toto vyjádření existuje, a to jediné). Položme:

$$\varphi(\boldsymbol{x}) = x_1 \cdot \boldsymbol{u}'_1 + \dots + x_n \cdot \boldsymbol{u}'_n.$$

Pak zřejmě $\varphi : V \to V'$ je zobrazení a rozepsáním se ukáže, že φ je bijektivní (proveďte si podrobně sami!). Dokažme, že φ je lineární zobrazení. Nechť $\boldsymbol{x}, \boldsymbol{y} \in V$, $t, s \in T$, přičemž $\boldsymbol{x} = x_1 \cdot \boldsymbol{u}_1 + \dots + x_n \cdot \boldsymbol{u}_n$, $\boldsymbol{y} = y_1 \cdot \boldsymbol{u}_1 + \dots + y_n \cdot \boldsymbol{u}_n$. Potom:

$$\begin{gathered} \varphi(t \cdot \boldsymbol{x} + s \cdot \boldsymbol{y}) = \varphi\big((tx_1 + sy_1) \cdot \boldsymbol{u}_1 + \dots + (tx_n + sy_n) \cdot \boldsymbol{u}_n\big) = \\ (tx_1 + sy_1) \cdot \boldsymbol{u}'_1 + \dots + (tx_n + sy_n) \cdot \boldsymbol{u}'_n = \\ t \cdot (x_1 \cdot \boldsymbol{u}'_1 + \dots + x_n \cdot \boldsymbol{u}'_n) + s \cdot (y_1 \cdot \boldsymbol{u}'_1 + \dots + y_n \cdot \boldsymbol{u}'_n) = t \cdot \varphi(\boldsymbol{x}) + s \cdot \varphi(\boldsymbol{y}). \end{gathered}$$

Dohromady pak φ je izomorfismus prostoru V na V', a tedy $V \cong V'$. □

Poznámka. Z předchozí věty plyne, že při zadaném číselném tělese T je každý vektorový prostor jednoznačně (až na izomorfismus) určen svojí dimenzí. Přitom např. zřejmě každý nenulový n-dimenzionální vektorový prostor nad T je izomorfní s prostorem T^n. Vidíme tedy, že vektorové prostory T^n pro $n = 1, 2, 3, \dots$ vyčerpávají (až na izomorfismus) všechny nenulové vektorové prostory nad T. Mohlo by se tedy na první pohled zdát, že při budování obecné teorie vektorových prostorů by vlastně stačilo omezit se pouze na prostory T^n. Je však ihned vidět, že bychom tímto nedosáhli žádného zjednodušení, neboť z důkazu předchozí věty plyne, že použitý izomorfismus závisí na volbě báze. Pokud bychom tedy chtěli nějaké tvrzení o prostoru T^n přenést na libovolný n-dimenzionální vektorový prostor, znamenalo by to vždy dokázat jeho nezávislost na volbě báze.

§2. Lineární transformace a její matice

Definice. Nechť V je vektorový prostor nad T. Lineární zobrazení $\varphi : V \to V$ se nazývá *lineární transformace* vektorového prostoru V.

Je-li navíc φ bijektivní, pak se nazývá *automorfismus* vektorového prostoru V.

Poznámka. Vidíme, že lineární transformace je pouze specielním případem lineárního zobrazení, a sice pro $V' = V$. Znamená to tedy, že všechny úvahy a tvrzení z předchozího paragrafu zůstávají v platnosti i pro lineární transformace, přičemž bude zřejmě platit ještě něco navíc.

Specielně zdůrazněme, že podle základní věty o lineárních zobrazeních je lineární transformace nenulového prostoru V jednoznačně určena zadáním obrazů pevné báze prostoru V.

Dále si všimněme toho, že je-li $V = \{\boldsymbol{o}\}$, pak existuje pouze jediná, a to identická lineární transformace prostoru V a všechny úvahy o ní jsou víceméně triviální. Proto se v dalším budeme zabývat pouze lineárními transformacemi nenulových vektorových prostorů.

Nejprve uvedeme větu, která nám podá řadu ekvivalentních podmínek pro to, aby lineární transformace byla automorfismem, tj. aby byla bijektivní.

Věta 2.1. *Nechť φ je lineární transformace prostoru V. Pak následující výroky jsou ekvivalentní:*
(1) *φ je automorfismus,*
(2) *φ je injektivní zobrazení,*
(3) *φ je surjektivní zobrazení,*
(4) *φ zobrazuje libovolnou bázi prostoru V na bázi prostoru V,*
(5) *φ zobrazuje libovolné lineárně nezávislé vektory opět na lineárně nezávislé vektory.*

Důkaz. „(1) $\Rightarrow$ (2)“: Zřejmé.

„(2) $\Rightarrow$ (3)“: Nechť φ je injektivní zobrazení. Pak podle věty 1.6. je $\operatorname{Ker}\varphi = \{\boldsymbol{o}\}$, a tedy podle věty 1.7. musí být $\dim \operatorname{Im}\varphi = \dim V$, neboli $\varphi(V) = V$. To však znamená, že φ je surjektivní zobrazení.

„(3) $\Rightarrow$ (4)“: Je-li φ surjektivní, pak $\varphi(V) = V$. Nechť nyní $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ je báze prostoru V. Podle věty 1.2. (2) jsou $\varphi(\boldsymbol{u}_1), \dots, \varphi(\boldsymbol{u}_n)$ generátory $\varphi(V) = V$. Ale z generátorů prostoru V lze vybrat bázi V, která však v našem případě musí sestávat z n vektorů, což znamená, že $\varphi(\boldsymbol{u}_1), \dots, \varphi(\boldsymbol{u}_n)$

je báze V.

„(4) $\Rightarrow$ (5)“: Nechť $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k \in V$ jsou lineárně nezávislé vektory. Ale lineárně nezávislé vektory z V lze doplnit na bázi V, odkud užitím (4) dostaneme, že $\varphi(\boldsymbol{u}_1), \dots, \varphi(\boldsymbol{u}_k)$ jsou lineárně nezávislé vektory.

„(5) $\Rightarrow$ (1)“: Z (5) plyne, že $\operatorname{Ker}\varphi = \{\boldsymbol{o}\}$ (neboť je-li $\boldsymbol{x} \neq \boldsymbol{o}$ libovolný, pak $\boldsymbol{x}$ je lineárně nezávislý, a tedy podle (5) je $\varphi(\boldsymbol{x})$ také lineárně nezávislý, neboli $\varphi(\boldsymbol{x}) \neq \boldsymbol{o}$). Ale je-li $\operatorname{Ker}\varphi = \{\boldsymbol{o}\}$, pak z věty 1.6. plyne, že φ je injektivní, a užitím věty 1.7. dostaneme, že φ je surjektivní. Dohromady tedy φ je automorfismus. □

Definice. Nechť φ je lineární transformace prostoru V. Nechť:

$$\boldsymbol{u}_1, \dots, \boldsymbol{u}_n \tag{1}$$

je pevná báze prostoru V a platí:

$$\begin{aligned}
\varphi(\boldsymbol{u}_1) &= a_{11} \cdot \boldsymbol{u}_1 + a_{21} \cdot \boldsymbol{u}_2 + \dots + a_{n1} \cdot \boldsymbol{u}_n \\
\varphi(\boldsymbol{u}_2) &= a_{12} \cdot \boldsymbol{u}_1 + a_{22} \cdot \boldsymbol{u}_2 + \dots + a_{n2} \cdot \boldsymbol{u}_n \\
&\vdots \\
\varphi(\boldsymbol{u}_n) &= a_{1n} \cdot \boldsymbol{u}_1 + a_{2n} \cdot \boldsymbol{u}_2 + \dots + a_{nn} \cdot \boldsymbol{u}_n
\end{aligned}$$

Pak matice:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

se nazývá *matice lineární transformace φ v bázi* (1).

Poznámka. 1. Vidíme, že matice A je čtvercová řádu n (kde $n = \dim V$) a je utvořena tak, že souřadnice vektoru $\varphi(\boldsymbol{u}_j)$ v bázi (1) jsou napsány do j-tého sloupce matice A ($j = 1, \dots, n$). Tyto souřadnice jsou určeny jednoznačně, a tedy i matice A je jednoznačně určena.

Uvědomme si dále, že pojem matice lineární transformace je vázán podstatným způsobem na pevnou bázi prostoru V. Zřejmě matice téže lineární transformace φ v různých bázích prostoru V budou obecně různé.

2. Všimněme si ještě vzájemného vztahu mezi pojmem „matice přechodu“ (definovaným v §5, kap. II.) a pojmem „matice lineární transformace“. Jsou-li $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ a $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$ dvě báze prostoru V a označíme-li symbolem φ lineární transformaci prostoru V zadanou určením obrazů báze tak, že vektory první báze se postupně zobrazují na vektory druhé báze, tzn.:

$$\begin{aligned} \varphi(\boldsymbol{u}_1) &= \boldsymbol{v}_1, \\ &\vdots \\ \varphi(\boldsymbol{u}_n) &= \boldsymbol{v}_n, \end{aligned}$$

pak ihned vidíme, že matice přechodu od báze $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ k bázi $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$ je rovna matici lineární transformace φ v bázi $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$.

Označení. Množinu všech lineárních transformací prostoru V budeme označovat symbolem $\mathcal{L}(V)$.

Prvky množiny $\mathcal{L}(V)$ jsou tedy lineární transformace vektorového prostoru V, tj. jistá zobrazení $V \to V$. Zřejmě je $\mathcal{L}(V) \neq \emptyset$, neboť například identické zobrazení $\mathrm{id}_V \in \mathcal{L}(V)$. Na množině $\mathcal{L}(V)$ nyní určitým přirozeným způsobem definujeme součet a součin, resp. násobek číslem a popíšeme základní vlastnosti takto vzniklých algebraických struktur.

Definice. Nechť $\varphi, \psi \in \mathcal{L}(V)$, $t \in T$ libovolné. Pak zobrazení:

(1) $\varphi + \psi : V \to V$ definované $(\varphi + \psi)(\boldsymbol{u}) = \varphi(\boldsymbol{u}) + \psi(\boldsymbol{u})$ pro $\forall \boldsymbol{u} \in V$ se nazývá *součet lineárních transformací* φ a ψ,

(2) $\varphi \circ \psi : V \to V$ definované $(\varphi \circ \psi)(\boldsymbol{u}) = \varphi\big(\psi(\boldsymbol{u})\big)$ pro $\forall \boldsymbol{u} \in V$ se nazývá *součin lineárních transformací* φ a ψ,

(3) $t \cdot \varphi : V \to V$ definované $(t \cdot \varphi)(\boldsymbol{u}) = t \cdot \big(\varphi(\boldsymbol{u})\big)$ pro $\forall \boldsymbol{u} \in V$ se nazývá *součin čísla t s lineární transformací φ.*

Věta 2.2. *Nechť φ, ψ jsou lineární transformace prostoru V, $t \in T$ libovolné. Pak:*

(1) *$\varphi + \psi$, $\varphi \circ \psi$, $t \cdot \varphi$ jsou lineární transformace prostoru V,*

(2) *$(\mathcal{L}(V), +)$ je komutativní grupa,*

(3) *$(\mathcal{L}(V), +, \circ)$ je okruh s jedničkou,*

(4) *$\mathcal{L}(V)$ je vektorový prostor nad tělesem T (vzhledem k $+$, resp. $\cdot$).*

Důkaz. (1): Zřejmě $\varphi + \psi$, $\varphi \circ \psi$, $t \cdot \varphi$ jsou zobrazení $V \to V$. Rozepsáním se bezprostředně ověří, že jsou to lineární zobrazení.

(2): Dokáže se rozepsáním. Přitom roli nulového prvku hraje nulová lineární transformace $\omega : V \to V$ (definovaná $\omega(\boldsymbol{u}) = \boldsymbol{o}$ pro $\forall \boldsymbol{u} \in V$), resp.

opačným prvkem k $\varphi \in \mathcal{L}(V)$ je lineární transformace $\varrho : V \to V$ definovaná $\varrho(\boldsymbol{u}) = -\varphi(\boldsymbol{u})$ pro $\forall \boldsymbol{u} \in V$.

(3): Dokáže se opět rozepsáním, s využitím (2). Jedničkou okruhu je zřejmě identická transformace id_V.

(4): Dokáže se užitím (2) a bezprostředním ověřením axiomů vektorového prostoru. $\square$

Věta 2.3. *Nechť φ, ψ jsou lineární transformace prostoru V, $\dim V = n \geq 1$ a nechť maticí φ (resp. ψ) v bázi* (1) *je matice A (resp. B). Potom:*

(1) *maticí lineární transformace $\varphi + \psi$ v bázi* (1) *je matice $A + B$,*

(2) *maticí lineární transformace $\varphi \circ \psi$ v bázi* (1) *je matice $A \cdot B$,*

(3) *maticí lineární transformace $t \cdot \varphi$ v bázi* (1) *je matice $t \cdot A$.*

Důkaz. Nechť $A = (a_{ij})$, $B = (b_{ij})$, $i, j = 1, \dots, n$. Při tomto označení pak platí:

$$\varphi(\boldsymbol{u}_j) = \sum_{r=1}^{n} a_{rj} \cdot \boldsymbol{u}_r, \quad \psi(\boldsymbol{u}_j) = \sum_{r=1}^{n} b_{rj} \cdot \boldsymbol{u}_r$$

pro $j = 1, \dots, n$. Pak:

(1): $(\varphi + \psi)(\boldsymbol{u}_j) = \varphi(\boldsymbol{u}_j) + \psi(\boldsymbol{u}_j) = \sum\limits_{r=1}^{n} a_{rj} \cdot \boldsymbol{u}_r + \sum\limits_{r=1}^{n} b_{rj} \cdot \boldsymbol{u}_r = \sum\limits_{r=1}^{n} (a_{rj} + b_{rj}) \cdot \boldsymbol{u}_r$ pro $j = 1, \dots, n$, a tedy maticí lineární transformace $\varphi + \psi$ v bázi (1) je matice $(a_{ij} + b_{ij}) = A + B$.

(2): Označme $A \cdot B = (c_{ij})$, tzn. $c_{ij} = \sum\limits_{k=1}^{n} a_{ik} \cdot b_{kj}$ pro $i, j = 1, \dots, n$. Ale $(\varphi \circ \psi)(\boldsymbol{u}_j) = \varphi\left(\sum\limits_{r=1}^{n} b_{rj} \cdot \boldsymbol{u}_r\right) = \sum\limits_{r=1}^{n} b_{rj} \cdot \varphi(\boldsymbol{u}_r) = \sum\limits_{r=1}^{n} b_{rj} \cdot \sum\limits_{s=1}^{n} a_{sr} \cdot \boldsymbol{u}_s = \sum\limits_{s=1}^{n} \left(\sum\limits_{r=1}^{n} a_{sr} b_{rj}\right) \cdot \boldsymbol{u}_s = \sum\limits_{s=1}^{n} c_{sj} \cdot \boldsymbol{u}_s$, odkud plyne, že maticí lineární transformace $\varphi \circ \psi$ v bázi (1) je matice $A \cdot B$.

(3): $(t \cdot \varphi)(\boldsymbol{u}_j) = t \cdot \varphi(\boldsymbol{u}_j) = t \cdot \sum\limits_{r=1}^{n} a_{rj} \cdot \boldsymbol{u}_r = \sum\limits_{r=1}^{n} (t \cdot a_{rj}) \cdot \boldsymbol{u}_r$, a tedy maticí lineární transformace $t \cdot \varphi$ v bázi (1) je matice $(t \cdot a_{ij}) = t \cdot A$. $\square$

Věta 2.4. *Nechť V je vektorový prostor nad T, $\dim V = n \geq 1$. Pak vektorový prostor $\mathcal{L}(V)$ je izomorfní vektorovému prostoru $\mathrm{Mat}_{nn}(T)$.*

Důkaz. Nechť (1) je pevná báze V. Definujme zobrazení $F : \mathcal{L}(V) \to \mathrm{Mat}_{nn}(T)$ takto: pro libovolné $\varphi \in \mathcal{L}(V)$ položme:

$$F(\varphi) = A,$$

kde A je matice lineární transformace φ v bázi (1). Nyní dokážeme, že:

I. F je bijektivní zobrazení.

Nechť $A \in \mathrm{Mat}_{nn}(T)$ libovolná. Označme $\boldsymbol{w}_1, \dots, \boldsymbol{w}_n$ vektory z V, jejichž souřadnicemi v bázi (1) (tj. bázi $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$) jsou po řadě sloupce matice A. Podle základní věty o lineárních zobrazeních existuje jediná lineární transformace φ prostoru V s vlastností $\varphi(\boldsymbol{u}_1) = \boldsymbol{w}_1, \dots, \varphi(\boldsymbol{u}_n) = \boldsymbol{w}_n$. Ale maticí φ v bázi (1) je pak právě matice A. Tedy existuje právě jedno $\varphi \in \mathcal{L}(V)$ tak, že $F(\varphi) = A$, neboli matice A má při zobrazení F právě jeden vzor, což znamená, že F je bijektivní zobrazení.

II. F je lineární zobrazení.

Nechť $\varphi, \psi \in \mathcal{L}(V)$, $t \in T$ libovolné, přičemž $F(\varphi) = A$, $F(\psi) = B$. Pak podle věty 2.3. (1) je $F(\varphi + \psi) = A + B = F(\varphi) + F(\psi)$ a podle věty 2.3. (3) je $F(t \cdot \varphi) = t \cdot A = t \cdot F(\varphi)$. Tedy F je lineární zobrazení.

Dohromady dostáváme, že F je izomorfismus, neboli $\mathcal{L}(V) \cong \mathrm{Mat}_{nn}(T)$.

$\square$

Poznamenejme, že z předchozí věty a z věty o izomorfismu vektorových prostorů plyne, že $\dim \mathcal{L}(V) = n^2$ (poněvadž, jak víme, $\dim \mathrm{Mat}_{nn}(T) = n^2$).

Na závěr paragrafu si ještě stručně všimneme toho, jak vypadají matice téže lineární transformace v různých bázích prostoru V a jaké jsou některé jejich základní vlastnosti.

Věta 2.5. *Nechť $A, B \in \mathrm{Mat}_{nn}(T)$, nechť $\dim V = n$ (≥ 1). Pak platí:*

A, B jsou maticemi téže lineární transformace prostoru V (ve vhodných bázích) $\iff$ existuje regulární matice S tak, že $B = S^{-1} \cdot A \cdot S$.

Důkaz. „$\Rightarrow$“: Nechť $A = (a_{ij})$, resp. $B = (b_{ij})$ je matice lineární transformace φ v bázi (1), resp. v bázi (1') (kde (1) je báze $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$, resp. (1') je báze $\boldsymbol{u}'_1, \dots, \boldsymbol{u}'_n$). Dále nechť $S = (s_{ij})$ je matice přechodu od báze (1) k bázi (1'), tzn. S je regulární matice a platí:

$$\boldsymbol{u}'_j = \sum_{i=1}^{n} s_{ij} \cdot \boldsymbol{u}_j$$

pro $j = 1, \dots, n$. Potom však:

$$\varphi(\boldsymbol{u}'_j) = \sum_{k=1}^{n} b_{kj} \cdot \boldsymbol{u}'_k = \sum_{k=1}^{n} b_{kj} \cdot \sum_{i=1}^{n} s_{ik} \cdot \boldsymbol{u}_i = \sum_{i=1}^{n} \left(\sum_{k=1}^{n} s_{ik} b_{kj} \right) \cdot \boldsymbol{u}_i$$

a také:

$$\varphi(\boldsymbol{u}'_j) = \varphi\left(\sum_{k=1}^{n} s_{kj} \cdot \boldsymbol{u}_k \right) = \sum_{k=1}^{n} s_{kj} \cdot \varphi(\boldsymbol{u}_k) = \sum_{k=1}^{n} s_{kj} \cdot \sum_{i=1}^{n} a_{ik} \cdot \boldsymbol{u}_i = \sum_{i=1}^{n} \left(\sum_{k=1}^{n} a_{ik} s_{kj} \right) \cdot \boldsymbol{u}_i,$$

odkud porovnáním pravých stran (na základě jednoznačnosti vyjádření vektoru $\varphi(\boldsymbol{u}_j)$ pomocí báze (1)) dostáváme, že:

$$\sum_{k=1}^{n} s_{ik} b_{kj} = \sum_{k=1}^{n} a_{ik} s_{kj}$$

pro $i, j = 1, \ldots, n$, což však znamená, že $S \cdot B = A \cdot S$, neboli $B = S^{-1} \cdot A \cdot S$.

„$\Leftarrow$“: Nechť $B = S^{-1} \cdot A \cdot S$ a nechť (1) je pevná báze prostoru V. Pak (podle důkazu věty 2.4.) existuje jediná lineární transformace φ prostoru V taková, že A je maticí φ v bázi (1). Dále, S je regulární matice, tzn. existuje (jediná) báze (1') prostoru V taková, že S je matice přechodu od báze (1) k (1'). Konečně, podle předpokladu je $S \cdot B = A \cdot S$, neboli $\sum_{k=1}^{n} s_{ik} b_{kj} = \sum_{k=1}^{n} a_{ik} s_{kj}$ pro $i, j = 1, \ldots, n$. Potom stejnými úpravami jako v první části důkazu dostáváme:

$$\varphi(\boldsymbol{u}'_j) = \sum_{i=1}^{n} \left(\sum_{k=1}^{n} a_{ik} s_{kj} \right) \cdot \boldsymbol{u}_i = \sum_{i=1}^{n} \left(\sum_{k=1}^{n} s_{ik} b_{kj} \right) \cdot \boldsymbol{u}_i = \sum_{k=1}^{n} b_{kj} \cdot \boldsymbol{u}'_k$$

pro $j = 1, \ldots, n$, což však znamená, že B je maticí lineární transformace φ v bázi (1'). Tedy matice A, B jsou maticemi téže lineární transformace prostoru V. $\square$

Definice. Nechť $A, B \in \mathrm{Mat}_{nn}(T)$ a nechť existuje regulární matice S taková, že $B = S^{-1} \cdot A \cdot S$. Pak říkáme, že matice A, B jsou *podobné matice* a píšeme $A \sim B$.

Věta 2.6. *Relace $\sim$ podobnosti matic je relací ekvivalence na množině* $\mathrm{Mat}_{nn}(T)$.

Důkaz. a) reflexivita: Pro libovolnou matici $A \in \mathrm{Mat}_{nn}(T)$ je zřejmě $A = E_n^{-1} \cdot A \cdot E_n$, kde E_n je jednotková matice řádu n. Je tedy $A \sim A$.

b) symetrie: Nechť $A \sim B$, tzn. existuje regulární matice S tak, že $B = S^{-1} \cdot A \cdot S$. Pak ale $A = S \cdot B \cdot S^{-1} = (S^{-1})^{-1} \cdot A \cdot (S^{-1})$, kde S^{-1} je zřejmě regulární. Tedy $B \sim A$.

c) tranzitivita: Nechť $A \sim B$ a $B \sim C$, tzn. existují regulární matice S, Q tak, že $B = S^{-1} \cdot A \cdot S$ a $C = Q^{-1} \cdot B \cdot Q$. Po dosazení dostáváme $C = Q^{-1} \cdot S^{-1} \cdot A \cdot S \cdot Q = (S \cdot Q)^{-1} \cdot A \cdot (S \cdot Q)$, přičemž matice $S \cdot Q$ je zřejmě regulární. Tedy je $A \sim C$. □

Definice. Nechť $A = (a_{ij})$ je čtvercová matice řádu n (nad T) a nechť λ je proměnná. Pak determinant:

$$|A - \lambda E_n| = \begin{vmatrix} a_{11}-\lambda & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22}-\lambda & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn}-\lambda \end{vmatrix}$$

se nazývá *charakteristický polynom matice* A.

Poznámka. Provedeme-li výpočet předchozího determinantu (např. užitím věty 2.2., kap. II.), dostaneme:

$$|A - \lambda E_n| = (-1)^n \cdot \lambda^n + (-1)^{n-1} \cdot (a_{11} + a_{22} + \cdots + a_{nn}) \cdot \lambda^{n-1} + \cdots + |A|.$$

Je tedy okamžitě vidět, že se skutečně jedná o polynom proměnné λ, který je stupně n a jeho koeficienty jsou z číselného tělesa T.

Konkrétně, například pro $n = 3$ dostaneme rozepsáním:

$$|A - \lambda E_3| = \begin{vmatrix} a_{11}-\lambda & a_{12} & a_{13} \\ a_{21} & a_{22}-\lambda & a_{23} \\ a_{31} & a_{32} & a_{33}-\lambda \end{vmatrix} =$$

$$-\lambda^3 + (a_{11}+a_{22}+a_{33}) \cdot \lambda^2 - \left(\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{vmatrix} + \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} \right) \cdot \lambda + |A|.$$

Věta 2.7. *Nechť A, B jsou podobné matice. Pak matice A, B mají:*
(1) *stejné determinanty, tj.* $|A| = |B|$,
(2) *stejnou hodnost, tj.* $h(A) = h(B)$,
(3) *stejné charakteristické polynomy, tj.* $|A - \lambda E_n| = |B - \lambda E_n|$.

Důkaz. Nechť $A, B \in \mathrm{Mat}_{nn}(T)$ jsou podobné matice, tzn. existuje regulární matice S tak, že $B = S^{-1} \cdot A \cdot S$. Potom:

(1): Užitím Cauchyovy věty a věty 3.9. (3), kap. II., dostáváme:

$$|B| = |S^{-1} \cdot A \cdot S| = \tfrac{1}{|S|} \cdot |A| \cdot |S| = |A|.$$

(2): Užitím věty 4.5. (2), kap. II., je:

$$h(B) = h(S^{-1} \cdot A \cdot S) = h(A \cdot S) = h(A).$$

(3): Užitím Cauchyovy věty a zřejmého faktu, že $\lambda E_n = S^{-1} \cdot (\lambda E_n) \cdot S$, dostáváme:

$$|B - \lambda E_n| = |S^{-1} \cdot A \cdot S - S^{-1} \cdot (\lambda E_n) \cdot S| = |S^{-1} \cdot (A - \lambda E_n) \cdot S| = \tfrac{1}{|S|} \cdot |A - \lambda E_n| \cdot |S| = |A - \lambda E_n|.$$

□

Poznámka. Připomeňme, že předchozí větu nelze obrátit, tzn. rovnost determinantů, rovnost hodností a rovnost charakteristických polynomů dvou matic jsou pouze nutné, nikoliv však dostatečné podmínky pro podobnost těchto matic. Vezmeme-li např. matice:

$$E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

pak zřejmě $|E_2| = |B|$, $h(E_2) = h(B)$ a $|E_2 - \lambda E_2| = |B - \lambda E_2|$, ale matice E_2 a B nejsou podobné (neboť pro každou regulární matici S řádu 2 je $S^{-1} \cdot E_2 \cdot S = E_2$, což znamená, že matice E_2 je podobná pouze sama sobě).

Jak již bylo řečeno, všechny matice dané lineární transformace φ jsou navzájem podobné. Z předchozí věty potom plyne, že determinant (resp. hodnost, resp. charakteristický polynom) všech matic dané lineární transformace φ je vždy stejný. Vidíme tedy, že tyto pojmy závisí pouze na lineární transformaci samotné, nikoliv na její konkrétní matici v jisté bázi. Z tohoto zjištění pak plyne korektnost následujícího pojmu a věty.

Definice. Nechť φ je lineární transformace vektorového prostoru V a nechť A je matice lineární transformace φ (v jisté bázi prostoru V). Pak charakteristický polynom matice A, tj. $|A - \lambda E_n|$, se nazývá *charakteristický polynom lineární transformace* φ.

Věta 2.8. *Nechť φ je lineární transformace vektorového prostoru V a nechť A je matice lineární transformace φ (v jisté bázi prostoru V). Pak:*

$$\dim \operatorname{Im} \varphi = h(A),$$

neboli hodnost lineární transformace φ je rovna hodnosti její matice A.

Důkaz. Nechť A je matice lineární transformace φ v bázi $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$, kterou označme (1). Podle věty 1.2. (2) vektory $\varphi(\boldsymbol{u}_1), \dots, \varphi(\boldsymbol{u}_n)$ jsou generátory podprostoru $\varphi(V) = \operatorname{Im}\varphi$, přičemž souřadnice těchto vektorů v bázi (1) tvoří po řadě řádky matice A', tj. transponované matice k matici A.

Přiřadíme-li nyní každému vektoru z V uspořádanou n-tici jeho souřadnic v bázi (1), dostaneme izomorfismus prostoru V na prostor T^n, pomocí něhož již lehce ukážeme, že $h(A') = \dim \operatorname{Im}\varphi$ (rozmyslete si podrobně sami!). Ale $h(A') = h(A)$, a tedy $\dim \operatorname{Im}\varphi = h(A)$. □

§3. Vlastní vektory a vlastní hodnoty lineární transformace

Definice. Nechť φ je lineární transformace vektorového prostoru V. Podprostor W vektorového prostoru V se nazývá *invariantní podprostor vzhledem k* φ, je-li:

$$\varphi(W) \subseteq W,$$

tzn. pro libovolný vektor $\boldsymbol{x} \in W$ platí $\varphi(\boldsymbol{x}) \in W$.

Příklad 3.1. Nechť V je libovolný pevný vektorový prostor nad T. Uvažme:

1. Identickou lineární transformaci $\mathrm{id}_V : V \to V$. Pak zřejmě každý podprostor W ve V je invariantní vzhledem k id_V.

2. Nulovou lineární transformaci $\omega : V \to V$ (definovanou $\omega(\boldsymbol{x}) = \boldsymbol{o}$ pro $\forall \boldsymbol{x} \in V$). Pak opět každý podprostor W ve V je invariantní vzhledem k ω.

3. Libovolnou lineární transformaci $\varphi : V \to V$. Pak triviální podprostory ve V (tzn. podprostory $\{\boldsymbol{o}\}$ a V) jsou invariantní vzhledem k φ.

Příklad 3.2. Ve vektorovém prostoru $\mathbb{R}^2$ uvažme podprostor $W = \{(x, 0) \mid x \in \mathbb{R}\}$ a dále uvažme dvě lineární transformace φ a ψ prostoru $\mathbb{R}^2$ definované:

$$\begin{aligned} \varphi\big((x_1, x_2)\big) &= (x_1 + x_2, 0), \\ \psi\big((x_1, x_2)\big) &= (x_2, x_1) \end{aligned}$$

pro každé $(x_1, x_2) \in \mathbb{R}^2$. Lehce se ověří, že W je invariantní podprostor vzhledem k φ, zatímco tentýž podprostor W není invariantním podprostorem vzhledem k ψ (neboť například $(1, 0) \in W$, ale $\psi\big((1, 0)\big) = (0, 1) \notin W$).

Poznámka. V příkladu 3.1. jsou uvedeny speciální, triviální případy. Uvědomme si, že obecně podprostor W může, ale nemusí být invariantní vzhledem k φ a dále, že podprostor, který je invariantní vzhledem k jedné lineární transformaci, nemusí být invariantní vzhledem k jiné lineární transformaci (viz příklad 3.2.). Vidíme tedy, že pojem invariantního podprostoru je vždy vázán na pevnou lineární transformaci.

Další příklady obecných konstrukcí invariantních podprostorů (vzhledem k φ) nám ukáží následující dvě věty.

Věta 3.1. *Nechť φ je lineární transformace prostoru V. Pak jádro* $\operatorname{Ker}\varphi$ *a obraz* $\operatorname{Im}\varphi$ *jsou invariantními podprostory vzhledem k φ.*

Důkaz. Podle věty 1.5. jsou $\operatorname{Ker}\varphi$ i $\operatorname{Im}\varphi$ podprostory ve V. Ukážeme jejich invariantnost vzhledem k φ. Nechť $\boldsymbol{u} \in \operatorname{Ker}\varphi$ libovolný. Pak $\varphi(\boldsymbol{u}) = \boldsymbol{o} \in \operatorname{Ker}\varphi$, a tedy $\operatorname{Ker}\varphi$ je invariantní vzhledem k φ. Dále nechť $\boldsymbol{u} \in \operatorname{Im}\varphi$ libovolný, tzn. zřejmě $\boldsymbol{u} \in V$. Pak ale $\varphi(\boldsymbol{u}) \in \varphi(V) = \operatorname{Im}\varphi$, a $\operatorname{Im}\varphi$ je tedy invariantní vzhledem k φ. □

Věta 3.2. *Nechť φ je lineární transformace prostoru V a nechť $W_1, \dots, W_k$ jsou podprostory ve V, které jsou invariantní vzhledem k φ. Pak průnik $(W_1 \cap \dots \cap W_k)$ a součet $(W_1 + \dots + W_k)$ jsou invariantní podprostory vzhledem k φ.*

Důkaz. Víme, že $(W_1 \cap \dots \cap W_k)$, resp. $(W_1 + \dots + W_k)$ jsou podprostory ve V. Dále:

a) Nechť $\boldsymbol{u} \in W_1 \cap \dots \cap W_k$ libovolný. Pak $\boldsymbol{u} \in W_i$ a podle předpokladu $\varphi(\boldsymbol{u}) \in W_i$ pro $i = 1, \dots, k$. Tedy $\varphi(\boldsymbol{u}) \in W_1 \cap \dots \cap W_k$, což znamená, že $W_1 \cap \dots \cap W_k$ je invariantní podprostor vzhledem k φ.

b) Označme $W = W_1 + \dots + W_k$. Nechť $\boldsymbol{u} \in W$, tzn. $\boldsymbol{u} = \boldsymbol{u}_1 + \dots + \boldsymbol{u}_k$, kde $\boldsymbol{u}_i \in W_i$. Pak ale $\varphi(\boldsymbol{u}) = \varphi(\boldsymbol{u}_1 + \dots + \boldsymbol{u}_k) = \varphi(\boldsymbol{u}_1) + \dots + \varphi(\boldsymbol{u}_k) \in W$, neboť podle předpokladu $\varphi(\boldsymbol{u}_i) \in W_i$. Tedy W je invariantní podprostor vzhledem k φ. □

Důležitou roli při studiu lineárních transformací hrají jednodimenzionální invariantní podprostory. Z kapitoly o vektorových prostorech víme, že jednodimenzionální podprostor W ve vektorovém prostoru V (nad T) je generován jedním nenulovým vektorem $\boldsymbol{u} \in V$, tzn. je pak:

$$W = L(\boldsymbol{u}) = \{t \cdot \boldsymbol{u} \mid t \in T\}.$$

Máme-li navíc dánu lineární transformaci φ prostoru V, pak zřejmě podprostor $W = L(\boldsymbol{u})$ je invariantní vzhledem k φ, právě když existuje číslo $\lambda \in T$ tak, že $\varphi(\boldsymbol{u}) = \lambda \cdot \boldsymbol{u}$, tzn. právě když se generátor $\boldsymbol{u}$ podprostoru W zobrazí na jistý svůj násobek (rozepište si podrobně sami!). A právě vektory tohoto typu se budeme v dalším zabývat.

Definice. Nechť φ je lineární transformace vektorového prostoru V (nad T). Nechť $\boldsymbol{u} \in V$, $\lambda \in T$ splňují:

$$\boldsymbol{u} \neq \boldsymbol{o} \quad \wedge \quad \varphi(\boldsymbol{u}) = \lambda \cdot \boldsymbol{u}.$$

Pak číslo λ se nazývá *vlastní hodnota lineární transformace* φ a vektor $\boldsymbol{u}$ se nazývá *vlastní vektor lineární transformace* φ *příslušný vlastní hodnotě* λ.

Poznámka. Z předchozí definice ihned plyne, že je-li $\boldsymbol{u}$ vlastním vektorem φ příslušným vlastní hodnotě λ, pak také každý nenulový vektor $\boldsymbol{w} \in L(\boldsymbol{u})$, tj. každý nenulový násobek vektoru $\boldsymbol{u}$, je rovněž vlastním vektorem φ příslušným téže vlastní hodnotě λ.

Příklad 3.3. Nechť V je vektorový prostor nad T. Dále:

1. Nechť $\mathrm{id}_V : V \to V$ je identická lineární transformace prostoru V. Pak zřejmě každý nenulový vektor z V je vlastním vektorem id_V příslušným vlastní hodnotě $\lambda = 1$ (což je jediná vlastní hodnota id_V).

2. Nechť $\omega : V \to V$ je nulová lineární transformace prostoru V. Pak podobně každý nenulový vektor z V je vlastním vektorem transformace ω příslušným vlastní hodnotě $\lambda = 0$ (což je opět jediná vlastní hodnota ω).

3. Nechť $\varphi : V \to V$ je libovolná lineární transformace. Pak všechny nenulové vektory z $\operatorname{Ker} \varphi$ (pokud existují) jsou vlastními vektory φ příslušnými vlastní hodnotě $\lambda = 0$. Přitom samozřejmě φ může obecně mít další vlastní hodnoty a jim odpovídající vlastní vektory.

Příklad 3.4. Nechť $\delta : \mathbb{R}_n[x] \to \mathbb{R}_n[x]$ je lineární transformace derivování (viz příklad 1.3.). Bezprostředně je vidět, že polynomy stupně nula (tj. nenulové reálné konstantní polynomy) jsou vlastními vektory transformace δ příslušnými vlastní hodnotě $\lambda = 0$ a že žádné jiné vlastní hodnoty a vlastní vektory δ neexistují.

Předchozí příklady vlastních hodnot a vektorů byly víceméně triviální. Úplný popis vlastních hodnot a vlastních vektorů lineární transformace v obecném případě podává následující věta.

Věta 3.3. *Nechť φ je lineární transformace vektorového prostoru V nad T. Pak:*

(1) *vlastními hodnotami φ jsou právě všechny kořeny (patřící do T) charakteristického polynomu transformace φ,*

(2) *je-li $\lambda \in T$ vlastní hodnota φ, pak vlastní vektory φ příslušné λ jsou právě všechny nenulové vektory z podprostoru* $\mathrm{Ker}(\varphi - \lambda \cdot \mathrm{id}_V)$.

Důkaz. (2): Nechť $\lambda \in T$ je vlastní hodnota φ. Pak $\boldsymbol{u} \in V$ je vlastní vektor φ příslušný vlastní hodnotě λ, právě když:

$$\boldsymbol{u} \neq \boldsymbol{o} \quad \wedge \quad \varphi(\boldsymbol{u}) = \lambda \cdot \boldsymbol{u}. \tag{1}$$

Ale $\lambda \cdot \boldsymbol{u} = \lambda \cdot \mathrm{id}_V(\boldsymbol{u})$, a tedy po dosazení a úpravě (1) dostáváme ekvivalentní podmínku:

$$\boldsymbol{u} \neq \boldsymbol{o} \quad \wedge \quad (\varphi - \lambda \cdot \mathrm{id}_V)(\boldsymbol{u}) = \boldsymbol{o}. \tag{2}$$

Ale množina vektorů splňujících (2) je rovna množině všech nenulových vektorů z podprostoru $\mathrm{Ker}(\varphi - \lambda \cdot \mathrm{id}_V)$ vektorového prostoru V.

(1): Z právě dokázaného a z vět 2.8. a 1.7. plyne: λ je vlastní hodnota $\varphi \iff \lambda \in T$ a $\mathrm{Ker}(\varphi - \lambda \cdot \mathrm{id}_V) \neq \{\boldsymbol{o}\} \iff \lambda \in T$ a matice lineární transformace $\varphi - \lambda \cdot \mathrm{id}_V$ (v pevné bázi prostoru V) je singulární. Ale je-li A maticí lineární transformace φ (v pevné bázi V), pak $(A - \lambda \cdot E_n)$ je maticí lineární transformace $\varphi - \lambda \cdot \mathrm{id}_V$ (v téže bázi). Tedy pak λ je vlastní hodnota $\varphi \iff \lambda \in T$ a $|A - \lambda \cdot E_n| = 0$, neboli $\lambda \in T$ je kořenem charakteristického polynomu lineární transformace φ. □

Důsledek. *Nechť φ je lineární transformace prostoru V, nechť $A = (a_{ij})$, $1 \leq i, j \leq n$, je matice φ (v dané bázi prostoru V) a nechť λ je vlastní hodnota φ. Pak vlastní vektory transformace φ příslušné λ (vyjádřené v dané bázi) jsou právě všechna nenulová řešení soustavy lineárních rovnic:*

$$\begin{array}{rcrcccr} (a_{11} - \lambda)x_1 & + & a_{12}x_2 & + \cdots + & a_{1n}x_n & = & 0 \\ a_{21}x_1 & + & (a_{22} - \lambda)x_2 & + \cdots + & a_{2n}x_n & = & 0 \\ & & & & & \vdots & \\ a_{n1}x_1 & + & a_{n2}x_2 & + \cdots + & (a_{nn} - \lambda)x_n & = & 0 \end{array} \tag{3}$$

Důkaz. Nechť $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ je daná báze V a nechť vektor $\boldsymbol{u}$ má v této bázi souřadnice $(x_1, \dots, x_n)$, tj. $\boldsymbol{u} = x_1 \cdot \boldsymbol{u}_1 + \dots + x_n \cdot \boldsymbol{u}_n$. Pak po dosazení a úpravě dostáváme:

$$(\varphi - \lambda \cdot \mathrm{id}_V)(\boldsymbol{u}) = \varphi(\boldsymbol{u}) - \lambda \cdot \boldsymbol{u} =$$
$$\big((a_{11} - \lambda)x_1 + a_{12}x_2 + \dots + a_{1n}x_n\big) \cdot \boldsymbol{u}_1 + \big(a_{21}x_1 + (a_{22} - \lambda)x_2 + \dots +$$
$$a_{2n}x_n\big) \cdot \boldsymbol{u}_2 + \dots + \big(a_{n1}x_1 + a_{n2}x_2 + \dots + (a_{nn} - \lambda)x_n\big) \cdot \boldsymbol{u}_n.$$

Podle předchozí věty je však $\boldsymbol{u}$ vlastním vektorem transformace φ příslušným vlastní hodnotě λ, právě když $\boldsymbol{u} \neq \boldsymbol{o}$ a $\boldsymbol{u} \in \mathrm{Ker}(\varphi - \lambda \cdot \mathrm{id}_V)$. Ale to vzhledem k předchozímu vyjádření nastane, právě když $\boldsymbol{u}$ je nenulový a jeho souřadnice splňují (3). $\square$

Poznámka. 1. S problémem nalezení vlastních hodnot a vlastních vektorů se velmi často setkáváme při řešení praktických úloh, a to nejen v matematice, ale i v různých technických aplikacích. Uvědomme si však, že předchozí věta nám dává odpověď pouze na teoretické úrovni, neboť hledání vlastních hodnot převádí na hledání kořenů polynomu n-tého stupně, což je úloha, která obecně není algoritmicky řešitelná. Samozřejmě existuje pro hledání vlastních hodnot a vlastních vektorů řada numerických metod, které však zde nebudeme uvádět, neboť přesahují rámec tohoto kurzu.

2. Poznamenejme ještě, že z hlediska aplikací bývá výhodné sestavit z vlastních vektorů bázi prostoru V (pokud samozřejmě taková báze vůbec existuje), neboť potom se celá situace početně velmi zjednoduší. Důvodem je, že daná lineární transformace má pak v takové bázi diagonální matici. (*Diagonální matice* je čtvercová matice, v níž všude mimo hlavní diagonálu stojí samé nuly. Přitom v hlavní diagonále nuly být mohou, ale nemusí.)

Skutečně, je-li $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ báze prostoru V sestávající z vlastních vektorů lineární transformace φ příslušných vlastním hodnotám $\lambda_1, \dots, \lambda_n$, pak je $\varphi(\boldsymbol{u}_1) = \lambda_1 \cdot \boldsymbol{u}_1, \dots, \varphi(\boldsymbol{u}_n) = \lambda_n \cdot \boldsymbol{u}_n$, a tedy matice lineární transformace φ v bázi $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ má tvar:

$$\begin{pmatrix} \lambda_1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & \lambda_2 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \lambda_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_{n-1} & 0 \\ 0 & 0 & 0 & \cdots & 0 & \lambda_n \end{pmatrix}. \tag{4}$$

Naopak, má-li lineární transformace φ v nějaké bázi $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ diagonální matici tvaru (4), pak $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ jsou zřejmě vlastními vektory lineární transformace φ příslušnými vlastním hodnotám $\lambda_1, \ldots, \lambda_n$ (jak plyne ihned z definice matice lineární transformace).

Následující úvahy nás přivedou k jedné dostatečné podmínce pro existenci výše popsané báze, tj. báze sestávající z vlastních vektorů dané lineární transformace.

Věta 3.4. *Nechť φ je lineární transformace prostoru V. Pak vlastní vektory lineární transformace φ příslušné navzájem různým vlastním hodnotám jsou lineárně nezávislé.*

Důkaz. Nechť $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ jsou vlastní vektory lineární transformace φ příslušné navzájem různým vlastním hodnotám $\lambda_1, \ldots, \lambda_k$. Z posloupnosti vektorů $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ vybereme libovolnou maximální lineárně nezávislou posloupnost. Bez újmy na obecnosti lze předpokládat, že ji tvoří například prvních r vektorů, tj. $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r$. Zřejmě je $1 \leq r \leq k$. Dále pokračujme sporem. Předpokládejme, že $r < k$. Pak lze ale psát:

$$\boldsymbol{u}_{r+1} = \sum_{i=1}^{r} t_i \cdot \boldsymbol{u}_i, \quad t_i \in T, \tag{5}$$

odkud po vynásobení číslem λ_{r+1} dostáváme:

$$\lambda_{r+1} \cdot \boldsymbol{u}_{r+1} = \sum_{i=1}^{r} \lambda_{r+1} \cdot t_i \cdot \boldsymbol{u}_i.$$

Současně však je:

$$\lambda_{r+1} \cdot \boldsymbol{u}_{r+1} = \varphi(\boldsymbol{u}_{r+1}) = \varphi\left(\sum_{i=1}^{r} t_i \cdot \boldsymbol{u}_i\right) = \sum_{i=1}^{r} t_i \cdot \lambda_i \cdot \boldsymbol{u}_i.$$

Porovnáním pravých stran pak dostáváme:

$$\sum_{i=1}^{r} \lambda_{r+1} \cdot t_i \cdot \boldsymbol{u}_i = \sum_{i=1}^{r} t_i \cdot \lambda_i \cdot \boldsymbol{u}_i,$$

odkud:

$$\sum_{i=1}^{r} t_i \cdot (\lambda_{r+1} - \lambda_i) \cdot \boldsymbol{u}_i = \boldsymbol{o}.$$

Z předpokládané lineární nezávislosti vektorů $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r$ však plyne, že $t_i \cdot (\lambda_{r+1} - \lambda_i) = 0$ pro $i = 1, \ldots, r$. Podle předpokladu věty je však $\lambda_{r+1} - \lambda_i \neq 0$, a tedy musí být $t_i = 0$ pro $i = 1, \ldots, r$. Po dosazení do (5) pak dostáváme, že $\boldsymbol{u}_{r+1} = \boldsymbol{o}$, což je ale spor s definicí vlastního vektoru. Je tedy $r = k$, tzn. vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ jsou lineárně nezávislé. $\square$

Důsledek. *Nechť φ je lineární transformace n-dimenzionálního vektorového prostoru V, která má n navzájem různých vlastních hodnot. Pak matice lineární transformace φ v bázi sestávající z vlastních vektorů příslušných těmto vlastním hodnotám je diagonální.*

Důkaz. Nechť $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ jsou vlastní vektory příslušné navzájem různým vlastním hodnotám $\lambda_1, \dots, \lambda_n$ lineární transformace φ. Pak podle předchozí věty vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ tvoří bázi prostoru V a tvrzení důsledku ihned plyne z 2. části poslední poznámky. $\square$

§4. Ortogonální zobrazení, ortogonální matice

V tomto paragrafu se vrátíme k euklidovským vektorovým prostorům (tj. k vektorovým prostorům nad $\mathbb{R}$, v nichž je definován skalární součin) a budeme studovat vzájemné vztahy mezi nimi. Použijeme k tomu lineárních zobrazení (podobně jako u vektorových prostorů v §1 a §2), která však navíc budou „zachovávat skalární součin“.

Definice. Nechť V, V' jsou euklidovské vektorové prostory. Nechť $\varphi : V \to V'$ je lineární zobrazení, pro něž platí:

$$\boldsymbol{u} \cdot \boldsymbol{v} = \varphi(\boldsymbol{u}) \cdot \varphi(\boldsymbol{v})$$

pro každé $\boldsymbol{u}, \boldsymbol{v} \in V$. Pak φ se nazývá *ortogonální zobrazení* euklidovského prostoru V do V'.

Je-li navíc zobrazení φ bijektivní, pak se nazývá *izomorfismus euklidovského prostoru* V na V' a euklidovské prostory V, V' se nazývají izomorfní.

Je-li specielně $V' = V$, pak se ortogonální zobrazení φ nazývá *ortogonální transformace* euklidovského prostoru V.

Podmínku „zachování skalárního součinu“ z předchozí definice je možné vyjádřit několika ekvivalentními způsoby, jak ukazuje následující věta.

Věta 4.1. *Nechť V, V' jsou euklidovské prostory a $\varphi : V \to V'$ je lineární zobrazení. Pak následující výroky jsou ekvivalentní:*

(1) $\boldsymbol{u} \cdot \boldsymbol{v} = \varphi(\boldsymbol{u}) \cdot \varphi(\boldsymbol{v})$ *pro každé* $\boldsymbol{u}, \boldsymbol{v} \in V$,

(2) $\| \boldsymbol{u} \| = \| \varphi(\boldsymbol{u}) \|$ *pro každé* $\boldsymbol{u} \in V$,

(3) *jsou-li* $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ *ortonormální vektory ve* V, *pak* $\varphi(\boldsymbol{u}_1), \ldots, \varphi(\boldsymbol{u}_k)$ *jsou ortonormální vektory ve* V'.

Důkaz. „(1) $\Rightarrow$ (2)“: Nechť platí (1) a nechť $\boldsymbol{u} \in V$. Pak (užitím (1)) dostáváme:

$$\| \boldsymbol{u} \|^2 = \boldsymbol{u} \cdot \boldsymbol{u} = \varphi(\boldsymbol{u}) \cdot \varphi(\boldsymbol{u}) = \| \varphi(\boldsymbol{u}) \|^2,$$

odkud pak $\| \boldsymbol{u} \| = \| \varphi(\boldsymbol{u}) \|$.

„(2) $\Rightarrow$ (3)“: Nechť platí (2) a nechť $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ jsou ortonormální vektory ve V. Nechť $i, j = 1, \ldots, k$. Pak (užitím (2)):

– pro $i = j$ platí:

$$\varphi(\boldsymbol{u}_i) \cdot \varphi(\boldsymbol{u}_i) = \| \varphi(\boldsymbol{u}_i) \|^2 = \| \boldsymbol{u}_i \|^2 = 1,$$

– pro $i \neq j$ platí:

$$2 \cdot \varphi(\boldsymbol{u}_i) \cdot \varphi(\boldsymbol{u}_j) = \varphi(\boldsymbol{u}_i + \boldsymbol{u}_j) \cdot \varphi(\boldsymbol{u}_i + \boldsymbol{u}_j) - \varphi(\boldsymbol{u}_i) \cdot \varphi(\boldsymbol{u}_i) - \varphi(\boldsymbol{u}_j) \cdot \varphi(\boldsymbol{u}_j) = \| \varphi(\boldsymbol{u}_i + \boldsymbol{u}_j) \|^2 - \| \varphi(\boldsymbol{u}_i) \|^2 - \| \varphi(\boldsymbol{u}_j) \|^2 = \| \boldsymbol{u}_i + \boldsymbol{u}_j \|^2 - \| \boldsymbol{u}_i \|^2 - \| \boldsymbol{u}_j \|^2 = 2 \cdot \boldsymbol{u}_i \cdot \boldsymbol{u}_j = 0,$$

odkud tedy $\varphi(\boldsymbol{u}_i) \cdot \varphi(\boldsymbol{u}_j) = 0$.

Dohromady dostáváme, že vektory $\varphi(\boldsymbol{u}_1), \ldots, \varphi(\boldsymbol{u}_k)$ jsou ortonormální.

„(3) $\Rightarrow$ (1)“: Nechť platí (3) a $\boldsymbol{u}, \boldsymbol{v} \in V$. Je-li $\boldsymbol{u} = \boldsymbol{o}$, pak zřejmě platí (1). Nechť tedy $\boldsymbol{u} \neq \boldsymbol{o}$. Mohou nastat dva případy:

α) Vektory $\boldsymbol{u}, \boldsymbol{v}$ jsou lineárně nezávislé.
Pak podle poznámky za větou 2.3., kap. IV., existují ortonormální vektory $\boldsymbol{e}_1, \boldsymbol{e}_2$ tak, že $\boldsymbol{u} = u_1 \cdot \boldsymbol{e}_1 + u_2 \cdot \boldsymbol{e}_2$, $\boldsymbol{v} = v_1 \cdot \boldsymbol{e}_1 + v_2 \cdot \boldsymbol{e}_2$. Podle (3) však $\varphi(\boldsymbol{e}_1), \varphi(\boldsymbol{e}_2)$ jsou ortonormální vektory a platí:

$$\varphi(\boldsymbol{u}) \cdot \varphi(\boldsymbol{v}) = \varphi(u_1 \cdot \boldsymbol{e}_1 + u_2 \cdot \boldsymbol{e}_2) \cdot \varphi(v_1 \cdot \boldsymbol{e}_1 + v_2 \cdot \boldsymbol{e}_2) = u_1 v_1 + u_2 v_2 = \boldsymbol{u} \cdot \boldsymbol{v}.$$

β) Vektory $\boldsymbol{u}, \boldsymbol{v}$ jsou lineárně závislé.
Pak opět podle poznámky za větou 2.3., kap. IV., existuje normovaný vektor $\boldsymbol{e}$ tak, že $\boldsymbol{u} = t \cdot \boldsymbol{e}$, $\boldsymbol{v} = s \cdot \boldsymbol{e}$. Podle (3) je vektor $\varphi(\boldsymbol{e})$ normovaný a platí:

$$\varphi(\boldsymbol{u}) \cdot \varphi(\boldsymbol{v}) = \varphi(t \cdot \boldsymbol{e}) \cdot \varphi(s \cdot \boldsymbol{e}) = t \cdot s = (t \cdot \boldsymbol{e}) \cdot (s \cdot \boldsymbol{e}) = \boldsymbol{u} \cdot \boldsymbol{v}.$$

Dohromady tak dostáváme, že platí (1). $\square$

Věta 4.2. (Věta o izomorfismu euklidovských prostorů) *Dva euklidovské prostory jsou izomorfní, právě když mají stejnou dimenzi.*

Důkaz. Nechť V, V' jsou euklidovské prostory. Potom:

„$\Rightarrow$“: Nechť V, V' jsou izomorfní (ve smyslu izomorfismu euklidovských prostorů). Pak jsou V, V' izomorfní jako vektorové prostory a podle věty o izomorfismu vektorových prostorů je $\dim V = \dim V'$.

„$\Leftarrow$“: Nechť $\dim V = \dim V' = n$. Je-li $n = 0$, pak zřejmě V a V' jsou izomorfní. Nechť tedy $n \geq 1$ a nechť dále:

$$\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n \text{ je ortonormální báze } V,$$

resp.

$$\boldsymbol{e}'_1, \ldots, \boldsymbol{e}'_n \text{ je ortonormální báze } V'.$$

Nechť $\boldsymbol{u} \in V$ je libovolný vektor, přičemž:

$$\boldsymbol{u} = \sum_{i=1}^{n} u_i \cdot \boldsymbol{e}_i.$$

Položme:

$$\varphi(\boldsymbol{u}) = \sum_{i=1}^{n} u_i \cdot \boldsymbol{e}'_i.$$

Pak φ je zřejmě zobrazení prostoru V do V', o němž se rozepsáním lehce ověří, že je bijektivní a že je lineárním zobrazením. Navíc je:

$$\|\varphi(\boldsymbol{u})\|^2 = \varphi(\boldsymbol{u}) \cdot \varphi(\boldsymbol{u}) = \left(\sum_{i=1}^{n} u_i \cdot \boldsymbol{e}'_i\right) \cdot \left(\sum_{j=1}^{n} u_j \cdot \boldsymbol{e}'_j\right) =$$
$$u_1 u_1 + \cdots + u_n u_n = \boldsymbol{u} \cdot \boldsymbol{u} = \|\boldsymbol{u}\|^2,$$

tzn. $\|\varphi(\boldsymbol{u})\| = \|\boldsymbol{u}\|$, a tedy φ je podle věty 4.1. ortogonální zobrazení. Dohromady pak φ je izomorfismem euklidovského prostoru V na V'. $\square$

Věta 4.3. *Nechť V, V' jsou euklidovské prostory, $\varphi : V \to V'$ je ortogonální zobrazení. Pak φ je injektivní zobrazení.*

Důkaz. Nechť $\boldsymbol{x} \in \operatorname{Ker} \varphi$, tzn. $\varphi(\boldsymbol{x}) = \boldsymbol{o}'$. Pak podle věty 4.1. je:

$$\|\boldsymbol{x}\| = \|\varphi(\boldsymbol{x})\| = \|\boldsymbol{o}'\| = 0,$$

a tedy (podle věty 1.4. (1), kap. IV.) je $\boldsymbol{x} = \boldsymbol{o}$. Dostáváme, že $\operatorname{Ker} \varphi = \{\boldsymbol{o}\}$, odkud podle věty 1.6. plyne, že φ je injektivní zobrazení. $\square$

Ve zbývající části tohoto paragrafu se budeme zabývat ortogonálními transformacemi daného euklidovského prostoru V. Je-li specielně $V = \{\boldsymbol{o}\}$ nulový euklidovský prostor, pak zřejmě jedinou možnou ortogonální transformací prostoru V je identické zobrazení. Tento triviální případ nebudeme v dalším uvažovat a budeme se zabývat pouze ortogonálními transformacemi nenulového euklidovského prostoru V. Některé základní vlastnosti ortogonální transformace nenulového euklidovského prostoru popisuje následující věta.

Věta 4.4. *Nechť $\varphi : V \to V$ je ortogonální transformace euklidovského prostoru V. Pak platí:*

(1) *φ je bijektivní zobrazení,*
(2) *inverzní zobrazení φ^{-1} je ortogonální transformací prostoru V,*
(3) *je-li λ vlastní hodnota ortogonální transformace φ, pak $\lambda = \pm 1$.*

Důkaz. (1): Plyne přímo z vět 4.3. a 2.1.

(2): Zřejmě $\varphi^{-1} : V \to V$ a podle důkazu věty 1.8. je φ^{-1} lineární zobrazení. Dále, nechť $\boldsymbol{u}, \boldsymbol{v} \in V$ libovolné. Označme $\varphi^{-1}(\boldsymbol{u}) = \boldsymbol{x}$, $\varphi^{-1}(\boldsymbol{v}) = \boldsymbol{y}$. Potom $\varphi(\boldsymbol{x}) = \boldsymbol{u}$, $\varphi(\boldsymbol{y}) = \boldsymbol{v}$ a platí:

$$\boldsymbol{u} \cdot \boldsymbol{v} = \varphi(\boldsymbol{x}) \cdot \varphi(\boldsymbol{y}) = \boldsymbol{x} \cdot \boldsymbol{y} = \varphi^{-1}(\boldsymbol{u}) \cdot \varphi^{-1}(\boldsymbol{v}),$$

tzn. dostáváme, že φ^{-1} je ortogonální transformace euklidovského prostoru V.

(3): Nechť λ je vlastní hodnota φ (tj. musí být $\lambda \in \mathbb{R}$) a nechť $\boldsymbol{u}$ je vlastní vektor φ příslušný vlastní hodnotě λ. Pak je $\varphi(\boldsymbol{u}) = \lambda \cdot \boldsymbol{u}$ a $\boldsymbol{u} \neq \boldsymbol{o}$, odkud:

$$\boldsymbol{u} \cdot \boldsymbol{u} = \varphi(\boldsymbol{u}) \cdot \varphi(\boldsymbol{u}) = (\lambda \cdot \boldsymbol{u}) \cdot (\lambda \cdot \boldsymbol{u}) = \lambda^2 \cdot (\boldsymbol{u} \cdot \boldsymbol{u}).$$

Ale $\boldsymbol{u} \cdot \boldsymbol{u} \neq 0$ (poněvadž $\boldsymbol{u} \neq \boldsymbol{o}$), a tedy musí být $\lambda^2 = 1$, neboli $\lambda = \pm 1$. $\square$

Každá ortogonální transformace (euklidovského) prostoru V je zřejmě lineární transformací tohoto (vektorového) prostoru V, a tedy můžeme sestrojit její matici v nějaké dané bázi prostoru V, specielně např. v dané ortonormální bázi prostoru V. Ukážeme, že v takovém případě bude pak mít tato matice jistý speciální tvar.

Definice. Nechť A je čtvercová matice nad $\mathbb{R}$ taková, že A je regulární a platí $A^{-1} = A'$ (tj. inverzní matice je rovna matici transponované). Pak matice A se nazývá *ortogonální matice.*

Věta 4.5. *Nechť A je čtvercová matice řádu n nad $\mathbb{R}$. Pak následující výroky jsou ekvivalentní:*
(1) *A je ortogonální matice,*
(2) $A \cdot A' = E_n$,
(3) $A' \cdot A = E_n$.

Důkaz. Věta plyne bezprostředně z definice ortogonální matice, definice inverzní matice a poznámky za větou 3.10., kap. II. □

Věta 4.6. *Nechť A, B jsou ortogonální matice řádu n. Pak platí:*
(1) *$A \cdot B$ je ortogonální matice,*
(2) *A^{-1} je ortogonální matice,*
(3) $|A| = \pm 1$.

Důkaz. (1): $(A \cdot B) \cdot (A \cdot B)' = A \cdot (B \cdot B') \cdot A' = A \cdot E_n \cdot A' = A \cdot A' = E_n$, a tedy podle věty 4.5. je $A \cdot B$ ortogonální maticí.

(2): Plyne z věty 4.5., uvážíme-li, že $(A')' = A$.

(3): Víme, že $|A| = |A'|$, tzn. pak z věty 4.5. a z Cauchyovy věty dostáváme:

$$1 = |E_n| = |A \cdot A'| = |A| \cdot |A'| = |A|^2,$$

odkud $|A| = \pm 1$. □

Důsledek. *Množina všech ortogonálních matic řádu n s operací násobení matic je grupou.*

Důkaz. Tvrzení plyne z předchozí věty, uvědomíme-li si, že násobení matic je asociativní a že jednotková matice E_n je ortogonální. □

Věta 4.7. *Nechť V je euklidovský prostor a $\varphi : V \to V$ je lineární transformace. Pak φ je ortogonální transformace $\iff$ matice transformace φ v ortonormální bázi prostoru V je ortogonální.*

Důkaz. Nechť:

$$\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n \tag{1}$$

je ortonormální báze prostoru V a nechť $A = (a_{ij})$ je matice lineární transformace φ v bázi (1). Dále:

„⇒“: Nechť φ je ortogonální transformace prostoru V. Pak podle věty 4.1. vektory $\varphi(\boldsymbol{e}_1), \ldots, \varphi(\boldsymbol{e}_n)$ tvoří ortonormální bázi prostoru V. Označme $A \cdot A' = B = (b_{ij})$. Potom:

$$b_{ij} = \sum_{k=1}^{n} a_{ik} \cdot a_{jk} = (a_{i1} \cdot \boldsymbol{e}_1 + \cdots + a_{in} \cdot \boldsymbol{e}_n) \cdot (a_{j1} \cdot \boldsymbol{e}_1 + \cdots + a_{jn} \cdot \boldsymbol{e}_n) = \varphi(\boldsymbol{e}_i) \cdot \varphi(\boldsymbol{e}_j),$$

odkud plyne, že $b_{ij} = 1$ pro $i = j$, resp. $b_{ij} = 0$ pro $i \neq j$. Tedy $A \cdot A' = E_n$ a podle věty 4.5. je matice A ortogonální.

„⇐“: Nechť matice A je ortogonální, tzn. platí (dle věty 4.5. (3)):

$$\sum_{k=1}^{n} a_{ki} \cdot a_{kj} = \begin{cases} 1 & \text{pro } i = j \\ 0 & \text{pro } i \neq j \end{cases} \tag{2}$$

Nechť dále $\boldsymbol{u} \in V$ libovolný, přičemž $\boldsymbol{u} = \sum_{i=1}^{n} u_i \cdot \boldsymbol{e}_i$. Potom:

$$\|\boldsymbol{u}\|^2 = \boldsymbol{u} \cdot \boldsymbol{u} = \sum_{i=1}^{n} u_i^2.$$

Dále:

$$\varphi(\boldsymbol{u}) = \sum_{i=1}^{n} u_i \cdot \varphi(\boldsymbol{e}_i) = \sum_{i=1}^{n} u_i \cdot \sum_{k=1}^{n} a_{ki} \cdot \boldsymbol{e}_k = \sum_{k=1}^{n} \left(\sum_{i=1}^{n} a_{ki} u_i \right) \cdot \boldsymbol{e}_k,$$

odkud rozepsáním a úpravou dostáváme:

$$\|\varphi(\boldsymbol{u})\|^2 = \varphi(\boldsymbol{u}) \cdot \varphi(\boldsymbol{u}) = \sum_{i=1}^{n} \sum_{j=1}^{n} \left(\sum_{k=1}^{n} a_{ki} a_{kj} \right) u_i u_j,$$

tzn. po dosazení (2) je pak:

$$\|\varphi(\boldsymbol{u})\|^2 = \sum_{i=1}^{n} u_i^2.$$

Dohromady tedy $\|\boldsymbol{u}\|^2 = \|\varphi(\boldsymbol{u})\|^2$, neboli $\|\boldsymbol{u}\| = \|\varphi(\boldsymbol{u})\|$, což znamená, že φ je ortogonální transformace. □

Na závěr ještě ukážeme, že maticemi přechodu od ortonormální báze k ortonormální bázi euklidovského prostoru jsou právě ortogonální matice.

Věta 4.8. *Nechť:*

$$\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n \tag{3}$$

$$\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \tag{4}$$

jsou báze euklidovského prostoru V a nechť báze (3) je ortonormální. Pak platí: matice přechodu od báze (3) k bázi (4) je ortogonální $\iff$ báze (4) je ortonormální.

Důkaz. Nechť $A = (a_{ij})$ je matice přechodu od báze (3) k bázi (4), tzn. platí:

$$\boldsymbol{v}_i = \sum_{k=1}^{n} a_{ki} \cdot \boldsymbol{u}_k$$

pro $i = 1, \ldots, n$. Potom však:

$$\boldsymbol{v}_i \cdot \boldsymbol{v}_j = \left(\sum_{k=1}^{n} a_{ki} \cdot \boldsymbol{u}_k \right) \cdot \left(\sum_{l=1}^{n} a_{lj} \cdot \boldsymbol{u}_l \right) = a_{1i}a_{1j} + \cdots + a_{ni}a_{nj},$$

odkud již (užitím věty 4.5.) bezprostředně plyne celé tvrzení věty. $\square$