Pavel Horák

LINEÁRNÍ ALGEBRA A GEOMETRIE I.

UČEBNÍ TEXT

2 0 0 7

Ú V O D

Tento učební text je určen pro předmět M 1115 Lineární algebra a geometrie I., který je povinným předmětem v bakalářském studijním programu Matematika, studijních oborech Matematika se zaměřením na vzdělávání a Matematika pro víceoborové studium na přírodovědecké fakultě Masarykovy Univerzity v Brně. Jedná se o jednosemestrální kurz, který je doporučeno absolvovat ve 2. semestru studia a který navazuje na předmět M 1125 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 $\blacksquare$, 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 $1, 2, 3, \dots$

$\mathbb{Z}$ … množina všech celých čísel

$\mathbb{Q}$ … množina všech racionálních čísel

$\mathbb{R}$ … množina všech reálných čísel

$\mathbb{C}$ … množina všech komplexních čísel.

Kapitola 1

Vektorové prostory

§1. Vektorový prostor, podprostory

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 situace poněkud komplikuje v tom, že pracujeme současně se dvěma algebraickými strukturami, a to s jistou komutativní grupou $(V, +)$, jejíž prvky budeme označovat tučnými písmeny, a dále s jistým číselným tělesem $(T, +, \cdot)$. Mezi těmito dvěma strukturami pak budou platit určité vazby.

Pro zjednodušení vyjadřování si zaveďme následující úmluvu : při zapisování algebraických struktur už nebudeme vždy důsledně vypisovat symboly operací, 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 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 pro libovolné $t, s \in T$ a $\boldsymbol{u}, \boldsymbol{v} \in V$ 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. $1 \cdot \boldsymbol{u} = \boldsymbol{u}$

Potom V se nazývá *vektorový prostor nad tělesem* T.

Označení.
Nulový prvek grupy V se nazývá *nulový vektor* a označuje se symbolem $\boldsymbol{o}$. Opačný prvek k vektoru $\boldsymbol{u}$ 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 vlastnosti 1. až 4. z definice vektorového prostoru.

Příklad 1.1.

1. Vektorový prostor T^n.

Nechť T je libovolné číselné těleso a nechť množinou vektorů je

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

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

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

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 a lehce se ověří, že platí vlastnosti 1. až 4. z definice vektorového prostoru.

Tedy T^n je vektorovým prostorem nad tělesem T.

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

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

2. Vektorový prostor $\mathbb{R}[x]$.

Číselným tělesem nechť je těleso $\mathbb{R}$ reálných čísel. Množinou vektorů bude množina všech polynomů o neurčité x s reálnými koeficienty, kterou označíme symbolem $\mathbb{R}[x]$. Sčítání vektorů definujeme jako obvyklé sčítání polynomů a součin čísla s vektorem definujeme jako obvyklé násobení reálného čísla s polynomem. Lehce se ověří, že $(\mathbb{R}[x], +)$ je komutativní grupa a že platí vlastnosti 1. až 4. z definice vektorového prostoru.

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. Vektorový prostor $\mathbb{R}_n[x]$.

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:

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

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 vlastnosti 1. až 4. z definice vektorového prostoru.

Tedy $\mathbb{R}_n[x]$ je vektorovým prostorem nad tělesem $\mathbb{R}$.

4. Nulový vektorový prostor.
Nechť T je libovolné číselné těleso a $V = \{\boldsymbol{o}\}$ je libovolná jednoprvková množina. Sčítání vektorů a součin čísla s vektorem definujeme (jediným možným způsobem) takto:

$$\boldsymbol{o} + \boldsymbol{o} = \boldsymbol{o} \qquad \text{a} \qquad t \cdot \boldsymbol{o} = \boldsymbol{o}, \text{ pro každé } t \in T.$$

Pak zřejmě $(V, +)$ je komutativní grupa a platí vlastnosti 1. až 4. z definice vektorového prostoru.

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.

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 obvyklé úmluvy budeme místo $\boldsymbol{u} + (-\boldsymbol{v})$ psát stručně $\boldsymbol{u} - \boldsymbol{v}$. V následující větě nyní uvedeme další základní pravidla pro počítání s vektory.

Věta 1.1.
Nechť V je vektorový prostor nad tělesem T, nechť $t, s, \in T$, $\boldsymbol{u}, \boldsymbol{v} \in V$. 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. $t \cdot (-\boldsymbol{u}) \;=\; (-t) \cdot \boldsymbol{u} \;=\; -(t \cdot \boldsymbol{u})\,;$ *speciálně pak* $(-1) \cdot \boldsymbol{u} \;=\; -\boldsymbol{u}\,.$

Důkaz.
Důkaz provedeme užitím předchozí úmluvy a užitím axiomů 1. až 4. z definice vektorového prostoru, případně užitím již dokázaných početních pravidel. Rozmyslete si vždy sami, která z uvedených vlastností se právě používá.

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: dokážeme postupně obě implikace.

„$\Rightarrow$“: Nechť $t \cdot \boldsymbol{u} = \boldsymbol{o}$ a nechť $t \neq 0$. Potom je:

$$\boldsymbol{u} \;=\; 1 \cdot \boldsymbol{u} \;=\; \Big(\frac{1}{t} \cdot t\Big) \cdot \boldsymbol{u} \;=\; \frac{1}{t} \cdot (t \cdot \boldsymbol{u}) \;=\; \frac{1}{t} \cdot \boldsymbol{o} \;=\; \frac{1}{t} \cdot (\boldsymbol{o} - \boldsymbol{o}) \;=\; \frac{1}{t} \cdot \boldsymbol{o} - \frac{1}{t} \cdot \boldsymbol{o} \;=\; \boldsymbol{o}\,.$$

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

Je-li $\boldsymbol{u} = \boldsymbol{o}$, pak $t \cdot \boldsymbol{u} \;=\; t \cdot \boldsymbol{o} \;=\; t \cdot (\boldsymbol{o} - \boldsymbol{o}) \;=\; t \cdot \boldsymbol{o} - t \cdot \boldsymbol{o} \;=\; \boldsymbol{o}\,.$

4: $\;t \cdot (-\boldsymbol{u}) \;=\; t \cdot (\boldsymbol{o} - \boldsymbol{u}) \;=\; t \cdot \boldsymbol{o} - t \cdot \boldsymbol{u} \;=\; \boldsymbol{o} - t \cdot \boldsymbol{u} \;=\; -(t \cdot \boldsymbol{u})\,,$

$(-t) \cdot \boldsymbol{u} \;=\; (0 - t) \cdot \boldsymbol{u} \;=\; 0 \cdot \boldsymbol{u} - t \cdot \boldsymbol{u} \;=\; \boldsymbol{o} - t \cdot \boldsymbol{u} \;=\; -(t \cdot \boldsymbol{u})\,.$ ∎

Poznámka.
V předchozí větě je důležitá zejména její třetí část, která uvádí nutnou a dostatečnou podmínku pro to, aby součin čísla s vektorem byl roven nulovému vektoru. Pomocí ní můžeme mimo jiné upřesnit naši představu o počtu vektorů ve vektorovém prostoru.

Je-li V libovolný vektorový prostor nad T různý od nulového prostoru (jinými slovy řečeno – prostor V obsahuje alespoň jeden nenulový vektor), pak musí tento vektorový prostor obsahovat nekonečně mnoho vektorů.

Vezmeme-li totiž libovolný nenulový vektor $\boldsymbol{u} \in V$ a tvoříme součiny všech prvků z číselného tělesa T (kterých je nekonečně mnoho, protože, jak víme, každé číselné těleso T obsahuje množinu racionálních čísel $\mathbb{Q}$) s tímto vektorem $\boldsymbol{u}$, dostáváme nekonečně mnoho navzájem různých vektorů, protože platí:

$$\boldsymbol{u} \neq \boldsymbol{o} \quad \wedge \quad t_1 \neq t_2 \qquad \Longrightarrow \qquad t_1 \cdot \boldsymbol{u} \;\neq\; t_2 \cdot \boldsymbol{u}\,.$$

Dokažme toto tvrzení (nepřímo).

Je-li $t_1 \cdot \boldsymbol{u} = t_2 \cdot \boldsymbol{u}$ a $\boldsymbol{u} \neq \boldsymbol{o}$, pak $(t_1 - t_2) \cdot \boldsymbol{u} = \boldsymbol{o}$, odkud podle věty 1.1. 3. plyne, že je $(t_1 - t_2) = 0$, neboli $t_1 = t_2$.

Vidíme tedy, že vektorový prostor nad číselným tělesem musí sestávat buď z jednoho vektoru (nulového) nebo z nekonečně mnoha vektorů.

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

1. $\boldsymbol{u}, \boldsymbol{v} \in U$ libovolné $\Longrightarrow$ $\boldsymbol{u} + \boldsymbol{v} \in U$
2. $t \in T$, $\boldsymbol{u} \in U$ libovolné $\Longrightarrow$ $t \cdot \boldsymbol{u} \in U$.

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

3. $\boldsymbol{u}, \boldsymbol{v} \in U$, $t, s \in T$ libovolné $\Longrightarrow$ $t \cdot \boldsymbol{u} + s \cdot \boldsymbol{v} \in U$.

2. Každý podprostor U vektorového prostoru V musí vždycky obsahovat nulový vektor (je-li $\boldsymbol{u} \in U$ libovolný, pak podle 2. a podle věty 1.1. 3. je $0 \cdot \boldsymbol{u} = \boldsymbol{o} \in U$).
Vidíme tedy, že dva podprostory vektorového prostoru V nemohou být nikdy disjunktní !!

Věta 1.2.
Nechť U je podprostor vektorového prostoru V nad tělesem T. Pak U je sám vektorovým prostorem nad tělesem T.

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

Nyní dokážeme, že $(U, +)$ je komutativní grupa, a to tak, že dokážeme, že $(U, +)$ je podgrupou grupy $(V, +)$. K tomu stačí (jak víme) například dokázat, že pro dva vektory $\boldsymbol{u}, \boldsymbol{v} \in U$ platí: $\boldsymbol{u} - \boldsymbol{v} \in U$.

Nechť $\boldsymbol{u}, \boldsymbol{v} \in U$ libovolné. Pak $(-1) \cdot \boldsymbol{v} = -\boldsymbol{v} \in U$, a tedy $\boldsymbol{u} - \boldsymbol{v} = \boldsymbol{u} + (-\boldsymbol{v}) \in U$ (podle věty 1.1. 4. a definice podprostoru). Tedy $(U, +)$ je komutativní grupou.

Podmínky 1. až 4. z definice vektorového prostoru jsou v U zřejmě splněny (poněvadž jsou splněny v celém V).

Tedy U je vektorový prostor nad tělesem T. ■

Příklad 1.2.
1. Nechť V je libovolný vektorový prostor nad tělesem T. Pak zřejmě

$$U = \{\boldsymbol{o}\} \qquad \text{a} \qquad U = V$$

jsou vždy podprostory ve V. Tyto dva podprostory se nazývají *triviální podprostory.* Všechny ostatní podprostory ve V (pokud existují) se nazývají *netriviální podprostory.*

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

$U_1 = \{(x, y, 0) \mid x, y \in \mathbb{R} \text{ lib.}\}$ je podprostor vektorového prostoru $\mathbb{R}^3$,

$U_2 = \{(x, y, z) \mid x, y, z \in \mathbb{R} \wedge x - 2y + 3z = 0\}$ je podprostor v $\mathbb{R}^3$,

Nechť (a, b, c) je pevný vektor prostoru $\mathbb{R}^3$. Potom

$$U_3 = \{k \cdot (a, b, c) \mid k \in \mathbb{R}\} \text{ je podprostor v } \mathbb{R}^3.$$

Z posledního příkladu je vidět, že vektorový prostor $\mathbb{R}^3$ obsahuje nekonečně mnoho podprostorů. Na druhé straně je jasné, že každá podmnožina v $\mathbb{R}^3$ nemusí být podprostorem $\mathbb{R}^3$. Například $U_4 = \{(x, y, 1) \mid x, y \in \mathbb{R}\}$ není podprostorem v $\mathbb{R}^3$ (zdůvodněte proč!).

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

$U_1 = \{f(x) \in \mathbb{R}[x] \mid f(x) = f(-x)\}$ je podprostor v $\mathbb{R}[x]$

$U_2 = \{f(x) \in \mathbb{R}[x] \mid 2 \cdot f(0) + 3 \cdot f(1) = 0\}$ je podprostor v $\mathbb{R}[x]$.

Na druhé straně například množina $U_3 = \{x^2 + ax + b \mid a, b \in \mathbb{R} \text{ lib.}\}$ není podprostorem v $\mathbb{R}[x]$ (proč ?).

Definice.
Nechť V je vektorový prostor nad T, nechť $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ je konečná posloupnost vektorů z V a $t_1, \ldots, t_k \in T$. Pak vektor:

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

se nazývá *lineární kombinace vektorů* $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$.
Množinu všech lineárních kombinací vektorů $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ budeme nazývat *lineární obal vektorů* $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ a budeme ji označovat symbolem $L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k)$. Je tedy

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

Poznámka.
1. V předchozí definici hovoříme o „konečné posloupnosti vektorů $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$“. Znamená to, 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 posledním paragrafu této kapitoly). Z důvodů stručnosti budeme však v dalším místo „konečná posloupnost vektorů $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$“ říkat obvykle pouze „vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$“.
2. Symbol $L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k)$ označuje množinu všech (možných) lineárních kombinací vektorů $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$, kterých je zřejmě obecně nekonečně mnoho. Uvědomme si dále, že množina $L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k)$ obsahuje vždy mimo jiné:

– každý z vektorů $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ (neboť $\boldsymbol{u}_i = 0 \cdot \boldsymbol{u}_1 + \cdots + 0 \cdot \boldsymbol{u}_{i-1} + 1 \cdot \boldsymbol{u}_i + 0 \cdot \boldsymbol{u}_{i+1} + \cdots + 0 \cdot \boldsymbol{u}_k$)

– nulový vektor (neboť $\boldsymbol{o} = 0 \cdot \boldsymbol{u}_1 + \cdots + 0 \cdot \boldsymbol{u}_k$).

Věta 1.3.
Nechť V je vektorový prostor nad T a nechť $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ je konečná posloupnost vektorů z V. Pak lineární obal $L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k)$ je podprostorem ve V.

Důkaz.
Tvrzení dostaneme bezprostředním ověřením definice podprostoru. ■

V tomto textu budeme často dokazovat, že lineární obaly dvou konečných posloupností vektorů jsou v inkluzi nebo že se rovnají. Následující věta nám umožní zjednodušit technické výpočty při těchto důkazech.

Věta 1.4.
Nechť V je vektorový prostor nad T a nechť $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ a $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s$ jsou konečné posloupnosti vektorů z V. Pak platí:

$$\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k \in L(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s) \implies L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k) \subseteq L(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s)\,.$$

Důkaz.
Tvrzení se dokáže bezprostředním technickým rozepsáním. ■

Jak již bylo řečeno, předchozí větu lze s výhodou použít při práci s lineárními obaly vektorů. Například k tomu, abychom dokázali, že platí množinová rovnost

$$L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k) \;=\; L(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s)$$

tedy na základě předchozí věty stačí dokázat, že platí

$$\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k \in L(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s)$$

a dále, že platí

$$\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s \in L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k).$$

§2. Generování podprostorů

Na úvod tohoto paragrafu si nejprve všimneme chování podprostorů vektorového prostoru vzhledem k množinovému průniku. Ukážeme, že průnik libovolného systému podprostorů vektorového prostoru V je opět podprostorem ve V. Všimněte si přitom způsobu, jak jsou uvažované podprostory označovány. Vzhledem k tomu, že nevíme "kolik" jich je, musíme k jejich označování použít indexovou množinu.

Věta 2.1.
Nechť V je vektorový prostor nad tělesem T, nechť I je neprázdná indexová množina a nechť pro každé $\alpha \in I$ je U_α podprostor ve V. Potom $\bigcap\limits_{\alpha\in I} U_\alpha$ je podprostor ve V.

Důkaz.
Množina $\bigcap\limits_{\alpha\in I} U_\alpha$ je zřejmě neprázdná (neboť obsahuje jistě nulový vektor $\boldsymbol{o}$). Zbývá tedy ověřit platnost podmínek 1. a 2. z definice podprostoru.
Nechť $\boldsymbol{u}, \boldsymbol{v} \in \bigcap\limits_{\alpha\in I} U_\alpha$, $t \in T$ libovolné. Potom $\boldsymbol{u}, \boldsymbol{v} \in U_\alpha$ pro každé $\alpha \in I$, a tedy (poněvadž U_α je podprostor) je také $\boldsymbol{u} + \boldsymbol{v} \in U_\alpha$ a $t \cdot \boldsymbol{u} \in U_\alpha$ pro každé $\alpha \in I$. To však znamená, že $\boldsymbol{u} + \boldsymbol{v} \in \bigcap\limits_{\alpha\in I} U_\alpha$ a $t \cdot \boldsymbol{u} \in \bigcap\limits_{\alpha\in I} U_\alpha$. Podmínky 1. a 2. jsou tedy splněny. ■

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 $[M]$ (čti "M v hranaté závorce"). Tedy:

$$[M] = \bigcap U_\alpha \; (\, U_\alpha \text{ je podprostor ve } V \text{ takový, že } M \subseteq U_\alpha \,) \tag{1}$$

a platí následující tvrzení.

Věta 2.2.
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 2.1.
2: Plyne z 1 a ze základních vlastností množinového průniku. ■

Může se stát, že množina M je prázdná. Potom je $[\,\emptyset\,] = \{\boldsymbol{o}\}$, tj. podprostor generovaný prázdnou množinou je roven nulovému podprostoru (rozmyslete si proč).

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 $[\boldsymbol{u}_1, \dots, \boldsymbol{u}_k]$ (čti "$\boldsymbol{u}_1$ až $\boldsymbol{u}_k$ v hranaté závorce"). Je tedy:

$$[\boldsymbol{u}_1, \dots, \boldsymbol{u}_k] = \bigcap U_\alpha \,(\, U_\alpha \text{ je podprostor ve } V \text{ takový, že } \boldsymbol{u}_1, \dots, \boldsymbol{u}_k \in U_\alpha \,) \qquad (2)$$

Definice.
Nechť M je podmnožina ve vektorovém prostoru V. Pak podprostor $[M]$ se nazývá *podprostor generovaný množinou M.*
Dále, podprostor $[\boldsymbol{u}_1, \dots, \boldsymbol{u}_k]$ se nazývá *podprostor generovaný vektory* $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ a vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ se nazývají *generátory* tohoto podprostoru.

Poznámka.
V předchozí úvaze a definici 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 ani jejich pořadí zde nehrají žádnou roli) a použít stejnou symboliku. Následující věta nám ukáže, že podprostor generovaný vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ a lineární obal vektorů $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ jsou vlastně jedno a totéž.

Věta 2.3.
Nechť V je vektorový prostor a nechť $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ je konečná posloupnost vektorů z V. Pak platí:

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

Důkaz.
Vzhledem k (2) budeme dokazovat množinovou rovnost :

$$\bigcap U_\alpha \,(\, U_\alpha \text{ je podprostor ve } V \;\wedge\; \boldsymbol{u}_1, \dots, \boldsymbol{u}_k \in U_\alpha \,) \;=\; L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k)\,. \qquad (3)$$

„$\subseteq$“: Plyne z vlastností množinového průniku, uvědomíme-li si, že $L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k)$ je podprostor ve V (podle věty 1.3.) a že je $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k \in L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k)$.
„$\supseteq$“: Množina na levé straně (3) je podprostorem ve V obsahujícím vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$, tzn. musí pak obsahovat také jejich libovolnou lineární kombinaci. ∎

Příklad 2.1.
1. Rozepsáním se lehce ověří, že například

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

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:

$$\boldsymbol{e}_1 = (1,0,0,\dots,0,0)\,, \quad \boldsymbol{e}_2 = (0,1,0,\dots,0,0)\,, \quad \dots \quad , \quad \boldsymbol{e}_n = (0,0,0,\dots,0,1)\,.$$

Potom zřejmě platí, že $T^n = L(\boldsymbol{e}_1, \dots, \boldsymbol{e}_k) = [\boldsymbol{e}_1, \dots, \boldsymbol{e}_n]$ (dokažte si podrobně sami) , tzn. vektory $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ jsou generátory vektorového prostoru T^n .

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

$$\boldsymbol{f}_1 = 1\,, \quad \boldsymbol{f}_2 = x\,, \quad \boldsymbol{f}_3 = x^2\,, \quad \ldots \quad \boldsymbol{f}_{n+1} = x^n\,.$$

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

Uvědomme si, že na rozdíl od průniku podprostorů není množinové sjednocení podprostorů (dokonce ani dvou) obecně podprostorem daného vektorového prostoru. Například pro podprostory U_1 a U_2 vektorového prostoru $\mathbb{R}^3$ z příkladu 1.2. 2. jejich sjednocení $U_1 \cup U_2$ není podprostorem v $\mathbb{R}^3$ (neboť např. $(1,1,0), (1,2,1) \in U_1 \cup U_2$, ale $(1,1,0) + (1,2,1) = (2,3,1) \notin U_1 \cup U_2$).

V dalším si nyní zavedeme pojem tzv. součtu podprostorů, dokážeme, že je podprostorem a ukážeme, jaký má vztah k množinovému sjednocení těchto podprostorů.

Definice.
Nechť $U_1, U_2, \ldots, U_k$ $(k \geq 2)$ jsou podprostory vektorového prostoru V. Pak množina $U_1 + U_2 + \cdots + U_k$ definovaná:

$$U_1 + U_2 + \cdots + U_k \;=\; \{\boldsymbol{u}_1 + \boldsymbol{u}_2 + \cdots + \boldsymbol{u}_k \mid \boldsymbol{u}_1 \in U_1,\; \boldsymbol{u}_2 \in U_2,\; \ldots,\; \boldsymbol{u}_k \in U_k\}$$

se nazývá *součet podprostorů* $U_1, U_2, \ldots, U_k$.

Věta 2.4.
Nechť $U_1, U_2, \ldots, U_k$ $(k \geq 2)$ jsou podprostory ve V. Pak platí:

1. *součet podprostorů $U_1 + U_2 + \cdots + U_k$ je podprostorem ve V*
2. *$U_1 + U_2 + \cdots + U_k = [\,U_1 \cup U_2 \cup \cdots \cup U_k\,]$, tj. součet podprostorů $U_1, U_2, \ldots, U_k$ je roven podprostoru generovanému jejich množinovým sjednocením.*

Důkaz.
1: Zřejmě je $U_1 + \cdots + U_k \neq \emptyset$ (neboť $U_i \neq \emptyset$). Dále nechť $\boldsymbol{u}, \boldsymbol{v} \in U_1 + \cdots + U_k$, $t \in T$ libovolné. Potom $\boldsymbol{u} = \boldsymbol{u}_1 + \cdots + \boldsymbol{u}_k$, $\boldsymbol{v} = \boldsymbol{v}_1 + \cdots + \boldsymbol{v}_k$, kde $\boldsymbol{u}_i, \boldsymbol{v}_i \in U_i$, $i = 1, \ldots, k$. Potom ale:

$$\boldsymbol{u} + \boldsymbol{v} = (\boldsymbol{u}_1 + \cdots + \boldsymbol{u}_k) + (\boldsymbol{v}_1 + \cdots + \boldsymbol{v}_k) = (\boldsymbol{u}_1 + \boldsymbol{v}_1) + \cdots + (\boldsymbol{u}_k + \boldsymbol{v}_k) \in U_1 + \cdots + U_k,$$

$$t \cdot \boldsymbol{u} = t \cdot (\boldsymbol{u}_1 + \cdots + \boldsymbol{u}_k) = t \cdot \boldsymbol{u}_1 + \cdots + t \cdot \boldsymbol{u}_k \in U_1 + \cdots + U_k,$$

a tedy $U_1 + \cdots + U_k$ je podprostor ve V.

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

$$U_1 + \cdots + U_k \;=\; \bigcap W_\alpha \;(\,W_\alpha \text{ je podprostor ve } V \text{ takový, že } U_1 \cup \cdots \cup U_k \subseteq W_\alpha\,)\,.$$

„$\subseteq$“: Nechť $\boldsymbol{u} \in U_1 + \cdots + U_k$. Potom $\boldsymbol{u} = \boldsymbol{u}_1 + \cdots + \boldsymbol{u}_k$, kde $\boldsymbol{u}_i \in U_i$. Je tedy také $\boldsymbol{u}_i \in W_\alpha$, kde W_α je libovolný podprostor ve V takový, že $U_1 \cup \cdots \cup U_k \subseteq W_\alpha$. Potom však $\boldsymbol{u}_1 + \cdots + \boldsymbol{u}_k = \boldsymbol{u} \in W_\alpha$, a tedy $\boldsymbol{u} \in \bigcap W_\alpha$ (W_α je podprostor ve $V \wedge U_1 \cup \cdots \cup U_k \subseteq W_\alpha$).

„$\supseteq$“: Zřejmě je $U_i \subseteq U_1 + \cdots + U_k$ (neboť pro $\boldsymbol{u}_i \in U_i$ libovolný je $\boldsymbol{u}_i = \boldsymbol{o} + \cdots + \boldsymbol{u}_i + \cdots + \boldsymbol{o} \in U_1 + \cdots + U_k$), a tedy $U_1 \cup \cdots \cup U_k \subseteq U_1 + \cdots + U_k$. Podle 1. části věty je však $U_1 + \cdots + U_k$ podprostorem ve V, tzn. z vlastností množinového průniku pak již plyne žádaná množinová inkluze. ■

Vidíme tedy, že součet podprostorů $U_1 + \cdots + U_k$ je nejmenším podprostorem ve V obsahujícím množinové sjednocení $U_1 \cup \cdots \cup U_k$ těchto podprostorů. Dá se očekávat, že součet podprostorů obecně nebude roven jejich množinovému sjednocení.

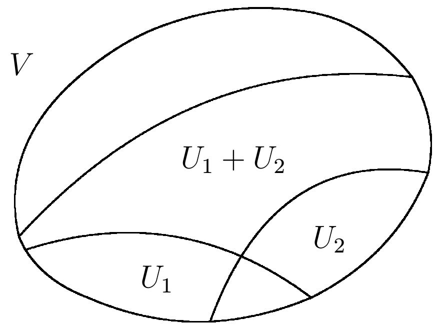
Dále si uvědomme, že vyjádření vektoru $\boldsymbol{u} \in U_1 + \cdots + U_k$ ve tvaru:

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

kde $\boldsymbol{u}_1 \in U_1, \ldots, \boldsymbol{u}_k \in U_k$, nemusí být jednoznačné. Obojí si ukážeme na jednoduchém příkladu, a to pro $k = 2$, což je situace, s níž se budeme v praxi nejčastěji setkávat. V tomto případě je tedy:

$$U_1 + U_2 = \{\boldsymbol{u}_1 + \boldsymbol{u}_2 \mid \boldsymbol{u}_1 \in U_1,\ \boldsymbol{u}_2 \in U_2\} = [U_1 \cup U_2].$$

Schematicky je tato situace znázorněna na obr. 1.



Obr. 1.

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

$$U_1 = \{(x, y, 0) \mid x, y \in \mathbb{R}\} \qquad \text{a} \qquad U_2 = \{(u, 0, v) \mid u, v \in \mathbb{R}\}.$$

Zřejmě platí, že:

$$U_1 \cup U_2 = \{(a, b, c) \mid a, b, c \in \mathbb{R},\ b = 0 \text{ nebo } c = 0\}, \qquad \text{resp.} \qquad U_1 + U_2 = \mathbb{R}^3.$$

Vidíme tedy, že $U_1 \cup U_2 \subsetneqq U_1 + U_2$, tzn. součet obou podprostorů není roven jejich množinovému sjednocení. Dále, vyjádření vektoru $\boldsymbol{u} \in U_1 + U_2$ ve tvaru:

$$\boldsymbol{u} = \boldsymbol{u}_1 + \boldsymbol{u}_2, \quad \text{kde } \boldsymbol{u}_1 \in U_1,\ \boldsymbol{u}_2 \in U_2,$$

zde není jednoznačné, neboť například vektor $(0, 0, 0) \in U_1 + U_2$, a přitom

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

jsou dvě různá vyjádření vektoru $(0, 0, 0)$ v uvedeném tvaru. Poznamenejme, že v takovém případě má každý vektor z $U_1 + U_2$ dokonce nekonečně mnoho různých vyjádření uvedeného tvaru.

Definice.
Nechť $U_1, U_2, \ldots, U_k$ $(k \geq 2)$ jsou podprostory vektorového prostoru V. Součet podprostorů $U_1, U_2, \ldots, U_k$ se nazývá *přímý součet* a označuje $U_1 \dot{+} U_2 \dot{+} \cdots \dot{+} U_k$, jestliže každý vektor $\boldsymbol{u} \in U_1 + \cdots + U_k$ lze vyjádřit jediným způsobem ve tvaru:

$$\boldsymbol{u} = \boldsymbol{u}_1 + \cdots + \boldsymbol{u}_k, \qquad \text{kde } \boldsymbol{u}_1 \in U_1, \ldots, \boldsymbol{u}_k \in U_k. \tag{4}$$

Věta 2.5.
Nechť $U_1, U_2, \ldots, U_k$ *(*$k \geq 2$*) jsou podprostory vektorového prostoru* V*. Pak součet podprostorů* $U_1, U_2, \ldots, U_k$ *je přímým součtem právě když platí*

$$U_i \cap (U_1 + \cdots + U_{i-1} + U_{i+1} + \cdots + U_k) = \{\boldsymbol{o}\} \qquad \textit{pro každé } i = 1, 2, \ldots, k\,. \tag{5}$$

tj. průnik každého z podprostorů se součtem zbývajících podprostorů je roven nulovému prostoru.

Důkaz.
„$\Rightarrow$“: Nechť součet podprostorů $U_1, \ldots, U_k$ je přímý a nechť pro $1 \leq i \leq k$ je

$$\boldsymbol{x} \in U_i \cap (U_1 + \cdots + U_{i-1} + U_{i+1} + \cdots + U_k)\,.$$

Potom je možno psát: $\boldsymbol{x} = \boldsymbol{u}_1 + \cdots + \boldsymbol{u}_{i-1} + \boldsymbol{u}_{i+1} + \cdots + \boldsymbol{u}_k$, kde $\boldsymbol{u}_j \in U_j$. Kromě toho je $\boldsymbol{x} \in U_i$, tzn. také $-\boldsymbol{x} \in U_i$. Pak ale:

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

a

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

jsou dvě vyjádření nulového vektoru ve tvaru (4), tzn. podle předpokladu musí být $-\boldsymbol{x} = \boldsymbol{o}$ a tedy $\boldsymbol{x} = \boldsymbol{o}$. Dokázali jsme tak, že $U_i \cap (U_1 + \cdots + U_{i-1} + U_{i+1} + \cdots + U_k) \subseteq \{\boldsymbol{o}\}$. Opačná inkluze je však zřejmá (proč?), tzn. dohromady platí rovnost. Poněvadž i bylo libovolné (s vlastností $1 \leq i \leq k$), platí všechny podmínky (5).

„$\Leftarrow$“: Nechť platí podmínky (5), nechť $\boldsymbol{x} \in U_1 + \cdots + U_k$ libovolný a nechť:

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

kde $\boldsymbol{u}_i, \boldsymbol{u}'_i \in U_i$, $i = 1, 2, \ldots, k$ jsou dvě vyjádření vektoru $\boldsymbol{x}$ ve tvaru (4). Potom pro libovolné $i = 1, 2, \ldots, k$ po úpravě dostáváme:

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

odkud okamžitě plyne, že:

$$(\boldsymbol{u}_i - \boldsymbol{u}'_i) \in U_i \cap (U_1 + \cdots + U_{i-1} + U_{i+1} + \cdots + U_k)\,.$$

Podle předpokladu, z podmínek (5) plyne, že $(\boldsymbol{u}_i - \boldsymbol{u}'_i) = \boldsymbol{o}$, neboli $\boldsymbol{u}_i = \boldsymbol{u}'_i$. Tedy vyjádření vektoru $\boldsymbol{x}$ ve tvaru (4) je jednoznačné a součet podprostorů $U_1, \ldots, U_k$ je přímý. ■

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

pro $k = 2$: *součet podprostorů* U_1, U_2 *je přímým součtem* $\iff$ $U_1 \cap U_2 = \{\boldsymbol{o}\}$,

pro $k = 3$: *součet podprostorů* U_1, U_2, U_3 *je přímým součtem* $\iff$

$$U_1 \cap (U_2 + U_3) = \{\boldsymbol{o}\} \quad \wedge \quad U_2 \cap (U_1 + U_3) = \{\boldsymbol{o}\} \quad \wedge \quad U_3 \cap (U_1 + U_2) = \{\boldsymbol{o}\}.$$

§3. Lineární závislost a nezávislost vektorů

Definice.
Nechť V je vektorový prostor nad T a nechť $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ 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:

$$t_1 \cdot \boldsymbol{u}_1 + \cdots + t_k \cdot \boldsymbol{u}_k \;=\; \boldsymbol{o}\,, \tag{1}$$

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

jestliže pro všechna $t_1, \ldots, t_k \in T$, z nichž alespoň jedno je různé od nuly, platí:

$$t_1 \cdot \boldsymbol{u}_1 + \cdots + t_k \cdot \boldsymbol{u}_k \neq \boldsymbol{o}\,,$$

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

2. Z definice lineární nezávislosti bezprostředně plyne, že:

vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ jsou lineárně nezávislé právě když platí implikace:

$$t_1 \cdot \boldsymbol{u}_1 + \cdots + t_k \cdot \boldsymbol{u}_k = \boldsymbol{o} \quad \Longrightarrow \quad t_1 = t_2 = \cdots = t_k = 0\,.$$

3. Praktické zjišťování lineární závislosti či nezávislosti daných vektorů $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ provádíme obvykle tak, že napíšeme rovnost

$$t_1 \cdot \boldsymbol{u}_1 + \cdots + t_k \cdot \boldsymbol{u}_k \;=\; \boldsymbol{o}$$

a hledáme všechna čísla $t_1, \ldots, t_k \in T$, která tuto rovnost splňují. Přitom mohou nastat dvě možnosti:

– zjistíme, že rovnost je splněna pouze pro $t_1 = \cdots = t_k = 0$. Pak jsou vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ lineárně nezávislé.
– zjistíme, že rovnost je splněna i pro nějaké $t_i \neq 0$. Pak jsou vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ lineárně závislé.

Příklad 3.1.
1. Ve vektorovém prostoru $\mathbb{R}^2$ jsou například vektory $(1, 0)$, $(0, 1)$ lineárně nezávislé. Podobně vektory $(1, 1)$, $(1, 2)$ jsou též lineárně nezávislé. Obojí dostaneme rozepsáním podle návodu uvedeného v předchozí poznámce.

Na druhé straně například vektory $(1, 3)$, $(2, 1)$, $(1, -1)$, $(-2, 3)$ jsou lineárně závislé, což opět zjistíme výpočtem podle výše uvedeného návodu.

Poznamenejme, že všechny výše zmiňované výpočty vedou v tomto případě na řešení soustav lineárních rovnic se dvěma neznámými.

2. Ve vektorovém prostoru T^n jsou vektory

$$\boldsymbol{e}_1 = (1, 0, 0, \ldots, 0, 0)\,, \quad \boldsymbol{e}_2 = (0, 1, 0, \ldots, 0, 0)\,, \quad \ldots \quad , \quad \boldsymbol{e}_n = (0, 0, 0, \ldots, 0, 1)$$

lineárně nezávislé.

Je-li totiž $t_1 \cdot \boldsymbol{e}_1 + \cdots + t_n \cdot \boldsymbol{e}_n = (0, \ldots, 0)$, pak po dosazení a úpravě dostáváme, že $(t_1, \ldots, t_n) = (0, \ldots, 0)$, a tedy $t_1 = t_2 = \cdots = t_n = 0$.

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

$$\boldsymbol{f}_1 = 1\,,\ \ \boldsymbol{f}_2 = x\,,\ \ \ldots\ \ ,\ \ \boldsymbol{f}_{n+1} = x^n$$

lineárně nezávislé. Je-li totiž

$$t_1 \cdot 1 \,+\, t_2 \cdot x \,+\, \cdots \,+\, t_{n+1} \cdot x^n \;=\; \boldsymbol{o}\,,$$

kde $\boldsymbol{o}$ značí nulový polynom, tj. polynom, jehož všechny koeficienty jsou rovny nule, potom je $t_1 = t_2 = \cdots = t_n = 0$ (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:

$$\textit{vektor } \boldsymbol{u} \textit{ je lineárně závislý} \iff \boldsymbol{u} = \boldsymbol{o}. \tag{2}$$

Pokud uvažovaná posloupnost vektorů obsahuje alespoň dva vektory, pak ekvivalentní podmínku pro jejich lineární závislost nám udává následující věta.

Věta 3.1.
Nechť V je vektorový prostor nad T, nechť $k \geq 2$ a nechť $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \in V$. Pak následující výroky jsou ekvivalentní:

1. *vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ jsou lineárně závislé*
2. *$\exists i$ $(1 \leq i \leq k)$ tak, že vektor $\boldsymbol{u}_i$ je lineární kombinací zbývajících vektorů (tj. vektorů $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{i-1}, \boldsymbol{u}_{i+1}, \ldots, \boldsymbol{u}_k$),*

Důkaz.
„1 ⇒ 2“: Nechť vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ jsou lineárně závislé. Pak existují čísla $t_1, \ldots, t_k \in T$, z nichž alespoň jedno je nenulové, tak, že $t_1 \cdot \boldsymbol{u}_1 + \cdots + t_k \cdot \boldsymbol{u}_k = \boldsymbol{o}$. 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 ⇒ 1“: Nechť platí 2, tzn. existuje index i tak, že

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

Pak (po úpravě, s využitím toho, že $-\boldsymbol{u}_i = (-1)\cdot\boldsymbol{u}_i$) dostáváme

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

tzn. (podle definice lineární závislosti) vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ jsou lineárně závislé. ■

Poznámka.
Je třeba si uvědomit, že druhá část předchozí věty nám pouze zajišťuje existenci vektoru, který lze vyjádřit jako lineární kombinaci zbývajících vektorů. Nelze tedy obecně tvrdit, že každý z lineárně závislých vektorů $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ 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 např. $2\cdot\boldsymbol{u}_1 + 0\cdot\boldsymbol{u}_2 + 1\cdot\boldsymbol{u}_3 = \boldsymbol{o}$), ale přitom je zřejmé, že vektor $\boldsymbol{u}_2$ nelze vyjádřit jako lineární kombinaci vektorů $\boldsymbol{u}_1, \boldsymbol{u}_3$.

Věta 3.2.
Nechť V je vektorový prostor nad T a nechť $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ je konečná posloupnost vektorů z V. Pak platí:

1. *obsahuje-li posloupnost $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ nulový vektor, pak je lineárně závislá*
2. *obsahuje-li posloupnost $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ dva stejné vektory, pak je lineárně závislá*
3. *je-li nějaká posloupnost vybraná z posloupnosti $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ lineárně závislá, pak je i celá posloupnost $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ lineárně závislá*
4. *je-li posloupnost $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ lineárně nezávislá, pak je každá posloupnost z ní vybraná také lineárně nezávislá.*

Důkaz.
První tři tvrzení plynou bezprostředně z definice lineární závislosti vektorů (proveďte příslušné důkazy podrobně sami!). Čtvrté tvrzení je zřejmě ekvivalentní s třetím tvrzením (jedná se o obměnu implikace), tzn. není třeba je dokazovat. ■

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

1. $r \leq s$,
2. *po 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 jistě platí, že $r \leq s$. Nyní dokážeme pro $r = 1$ ještě druhou část tvrzení věty. Podle předpokladů věty je vektor $\boldsymbol{u}_1$ lineárně nezávislý a platí:

$$\boldsymbol{u}_1 = t_1 \cdot \boldsymbol{v}_1 + \cdots + t_s \cdot \boldsymbol{v}_s\,. \tag{3}$$

Protože je $\boldsymbol{u}_1$ lineárně nezávislý, pak podle (2) je $\boldsymbol{u}_1 \neq \boldsymbol{o}$ a tedy alespoň jedno z čísel $t_1, \ldots, t_s$ musí být nenulové. Přečíslujme vektory $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s$ tak, aby $t_1 \neq 0$. Potom po úpravě z rovnice (3) dostáváme:

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

což znamená, že $\boldsymbol{v}_1 \in L(\boldsymbol{u}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_s)$. Triviálně je však $\boldsymbol{v}_2, \ldots, \boldsymbol{v}_s \in L(\boldsymbol{u}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_s)$, a tedy podle věty 1.4. dostáváme, že $L(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s) \subseteq L(\boldsymbol{u}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_s)$.

Opačná inkluze plyne ze (3) a ze zřejmého faktu, že $\boldsymbol{v}_2, \ldots, \boldsymbol{v}_s \in L(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s)$, opět užitím věty 1.4.. Platí tedy rovnost: $L(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s) = L(\boldsymbol{u}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_s)$.

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

Uvažujme vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{r-1}$. Podle předpokladů věty a podle věty 3.2. (část 4.) jsou vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{r-1}$ lineárně nezávislé a platí $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{r-1} \in L(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s)$. Vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{r-1}$ tedy splňují předpoklady věty a můžeme na ně použít indukční předpoklad. Jeho užitím dostáváme, že platí:

$$r-1 \leq s \tag{4}$$

a po vhodném přečíslování vektorů $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s$ platí:

$$L(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s) = L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{r-1}, \boldsymbol{v}_r, \ldots, \boldsymbol{v}_s). \tag{5}$$

Nyní uvažme vektor $\boldsymbol{u}_r$. Podle předpokladu věty je $\boldsymbol{u}_r \in L(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s)$, odkud podle vztahu (5) dostáváme, že $\boldsymbol{u}_r \in L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{r-1}, \boldsymbol{v}_r, \ldots, \boldsymbol{v}_s)$, tzn.

$$\boldsymbol{u}_r = t_1 \cdot \boldsymbol{u}_1 + \cdots + t_{r-1} \cdot \boldsymbol{u}_{r-1} + t_r \cdot \boldsymbol{v}_r + \cdots + t_s \cdot \boldsymbol{v}_s. \tag{6}$$

Z (6) a z předpokladu, že $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r$ jsou lineárně nezávislé pak plyne, že v (4) nemůže nastat rovnost (při $r-1 = s$ by totiž platilo, že $\boldsymbol{u}_r = t_1 \cdot \boldsymbol{u}_1 + \cdots + t_{r-1} \cdot \boldsymbol{u}_{r-1}$, a vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r$ by byly lineárně závislé). Je tedy $r-1 < s$, odkud ihned plyne, že

1. platí $r \leq s$, což je první část tvrzení věty.

2. alespoň jedno z čísel $t_r, \ldots, t_s$ musí být nenulové. Přečíslujme vektory $\boldsymbol{v}_r, \ldots, \boldsymbol{v}_s$ tak, aby bylo $t_r \neq 0$. Potom z (6) úpravou dostáváme:

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

Podle věty 1.4., užitím (7) a (6), pak dostáváme (rozmyslete si podrobně sami, že skutečně platí obě množinové inkluze), že

$$L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{r-1}, \boldsymbol{v}_r, \ldots, \boldsymbol{v}_s) = L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r, \boldsymbol{v}_{r+1}, \ldots, \boldsymbol{v}_s). \tag{8}$$

Ze vztahů (5) a (8) pak ihned 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 druhá část tvrzení věty. ∎

§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.

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".

Připomeňme, že podmínka „vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ generují vektorový prostor V" znamená, že lineárním obalem vektorů $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ je celý prostor V, což jinak řečeno znamená, že platí rovnost:

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

Uvědomme si, že předchozí definice nezaručuje existenci báze ani nic neříká o tom, kolik bází se ve vektorovém prostoru V dá sestrojit. Z následujících dvou příkladů bude vidět, že vektorový prostor buď bázi nemá nebo má nekonečně mnoho bází (rozmyslete si vždy proč).

Příklad 4.1.
Z příkladů 2.1. a 3.1. bezprostředně plyne, že:

1. Bází vektorového prostoru $\mathbb{R}^2$ jsou např. vektory $(1,0), (0,1)$ nebo vektory $(1,1), (1,2)$.
Vektorový prostor $\mathbb{R}^2$ má zřejmě nekonečně mnoho různých bází.

2. Bází vektorového prostoru T^n jsou například vektory

$$\boldsymbol{e}_1 = (1,0,\dots,0)\,, \quad \boldsymbol{e}_2 = (0,1,0,\dots,0)\,, \ \dots \ , \quad \boldsymbol{e}_n = (0,\dots,0,1)\,.$$

Vektorový prostor T^n má zřejmě nekonečně mnoho různých bází.

3. Bází vektorového prostoru $\mathbb{R}_n[x]$ jsou například vektory (tj. polynomy)

$$\boldsymbol{f}_1 = 1\,, \quad \boldsymbol{f}_2 = x\,, \ \dots \ , \quad \boldsymbol{f}_{n+1} = x^n\,.$$

Vektorový prostor $\mathbb{R}_n[x]$ má zřejmě nekonečně mnoho různých bází.

Příklad 4.2.
1. Nulový vektorový prostor $V = \{\boldsymbol{o}\}$ nemá bázi,

neboť libovolná konečná posloupnost vektorů z V může v tomto případě sestávat pouze z nulových vektorů a je tedy lineárně závislá.

2. Vektorový prostor $\mathbb{R}[x]$ nemá bázi,

neboť konečná posloupnost vektorů (polynomů) z $\mathbb{R}[x]$ nikdy 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 $\boldsymbol{f} = x^t$ se evidentně nedá napsat jako lineární kombinace polynomů $\boldsymbol{g}_1, \dots, \boldsymbol{g}_n$ a je tedy $[\boldsymbol{g}_1, \dots, \boldsymbol{g}_n] \subsetneqq \mathbb{R}[x]$.

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

– báze $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ vektorového prostoru V je z hlediska lineární nezávislosti „nejpočetnější“ posloupností vektorů z V. Přesněji řečeno, pokud k bázi přidáme další vektor, pak získané vektory sice nadále budou generátory prostoru V, ale nebudou již lineárně nezávislé (plyne z věty 3.1. – rozmyslete si podrobně jak).

– báze $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ vektorového prostoru V je z hlediska generátorů „nejméně početná“ posloupnost vektorů. Přesněji řečeno, pokud bychom některý z vektorů báze $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ vypustili, pak zbývající vektory sice budou lineárně nezávislé, ale nebudou již generovat vektorový prostor V (plyne z věty 3.2.4. a věty 3.1. – rozmyslete si proč).

Následují dvě věty, z nichž první uvádí ekvivalentní podmínku pro to, aby vektory tvořily bázi vektorového prostoru a druhá popisuje další důležité vlastnosti bází.

Věta 4.1.
Vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ jsou bází vektorového prostoru V právě když každý vektor $\boldsymbol{x} \in V$ je možno jediným způsobem vyjádřit ve tvaru:

$$\boldsymbol{x} = t_1 \cdot \boldsymbol{u}_1 + \cdots + t_n \cdot \boldsymbol{u}_n \,, \qquad \textit{kde} \quad t_1, \ldots, t_n \in T \,. \tag{1}$$

Důkaz.
„$\Rightarrow$“: Nechť $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ je báze ve V. Pak:

– existence vyjádření (1) plyne ihned z definice báze (proč?)

– dokážeme jednoznačnost vyjádření (1). Nechť tedy:

$$\boldsymbol{x} \;=\; t_1 \cdot \boldsymbol{u}_1 + \cdots + t_n \cdot \boldsymbol{u}_n \;=\; r_1 \cdot \boldsymbol{u}_1 + \cdots + r_n \cdot \boldsymbol{u}_n \,, \quad \text{kde } t_i, r_i \in T.$$

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 $i = 1, \ldots, n$. Vyjádření (1) je tedy jednoznačné.

„$\Leftarrow$“: Nechť každý vektor $\boldsymbol{x} \in V$ se dá jednoznačně vyjádřit ve tvaru (1). Potom:

– vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ generují vektorový prostor V, protože z existence vyjádření (1) plyne, že $V \subseteq L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n)$ a opačná inkluze, tj. $L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n) \subseteq V$ je triviální. Dostáváme tak, že $V = L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n)$.

– zbývá ukázat, že vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ jsou lineárně nezávislé. Nechť tedy:

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

Nulový vektor se však zřejmě dá také napsat ve tvaru

$$0 \cdot \boldsymbol{u}_1 + \cdots + 0 \cdot \boldsymbol{u}_n \;=\; \boldsymbol{o}.$$

Vidíme, že jsme nulový vektor vyjádřili dvěma způsoby ve tvaru (1). Z předpokladu jednoznačnosti vyjádření (1) pak plyne, že $t_1 = \cdots = t_n = 0$, což znamená, že vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ jsou lineárně nezávislé.

Dohromady pak dostáváme, že vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ jsou bází prostoru V. ■

Věta 4.2.
Nechť $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ je báze vektorového prostoru V. Pak platí:

1. *jestliže $\boldsymbol{v}_1, \dots, \boldsymbol{v}_k$ je báze prostoru V, pak je $k = n$*
2. *jestliže vektory $\boldsymbol{v}_1, \dots, \boldsymbol{v}_s$ generují prostor V, pak z nich lze vybrat bázi V*
3. *jestliže vektory $\boldsymbol{v}_1, \dots, \boldsymbol{v}_r$ jsou lineárně nezávislé, pak je lze doplnit na bázi V.*

Důkaz.
1: Aplikujeme-li dvakrát Steinitzovu větu (proveďte si podrobně sami!), dostáváme jednak $n \le k$ a jednak $k \le n$, odkud již plyne, že $k = n$.

2: Nechť vektory $\boldsymbol{v}_1, \dots, \boldsymbol{v}_s$ generují prostor V. Podle předpokladu má prostor V bázi, tzn. musí být $V \neq \{\boldsymbol{o}\}$. Pak lze vektory $\boldsymbol{v}_1, \dots, \boldsymbol{v}_s$ přečíslovat tak, že $\boldsymbol{v}_1, \dots, \boldsymbol{v}_i$ jsou lineárně nezávislé a $\boldsymbol{v}_1, \dots, \boldsymbol{v}_i, \boldsymbol{v}_j$ jsou lineárně závislé pro každé j s vlastností $i < j \le s$. Odtud plyne (proč?), že $\boldsymbol{v}_j \in L(\boldsymbol{v}_1, \dots, \boldsymbol{v}_i)$, a tedy $V = L(\boldsymbol{v}_1, \dots, \boldsymbol{v}_s) \subseteq L(\boldsymbol{v}_1, \dots, \boldsymbol{v}_i)$. Inkluze $L(\boldsymbol{v}_1, \dots, \boldsymbol{v}_i) \subseteq L(\boldsymbol{v}_1, \dots, \boldsymbol{v}_s)$ je však triviální a tedy je $V = L(\boldsymbol{v}_1, \dots, \boldsymbol{v}_i)$. Protože vektory $\boldsymbol{v}_1, \dots, \boldsymbol{v}_i$ jsou lineárně nezávislé, tvoří bázi prostoru V.

3: Nechť $\boldsymbol{v}_1, \dots, \boldsymbol{v}_r$ jsou lineárně nezávislé vektory z V. Podle Steinitzovy věty (rozmyslete si jak) je po vhodném přečíslování $V = L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n) = L(\boldsymbol{v}_1, \dots, \boldsymbol{v}_r, \boldsymbol{u}_{r+1}, \dots, \boldsymbol{u}_n)$. Vektory $\boldsymbol{v}_1, \dots, \boldsymbol{v}_r, \boldsymbol{u}_{r+1}, \dots, \boldsymbol{u}_n$ tedy generují prostor V a podle právě dokázané části 2 z nich lze vybrat bázi V. Podle části 1 však tato báze musí sestávat z n vektorů, což znamená, že vektory $\boldsymbol{v}_1, \dots, \boldsymbol{v}_r, \boldsymbol{u}_{r+1}, \dots, \boldsymbol{u}_n$ jsou bází 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, pak 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 nenulový prostor, který nemá bázi, říkáme, že *dimenze V je nekonečno.*

Píšeme potom: $\dim V = 0$, 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. speciálně 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. speciálně např. $\dim \mathbb{R}_5[x] = 6$, atd.),

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

Úmluva.
Všude v dalším v tomto textu 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 musí být zřejmě sám také konečnědimenzionálním vektorovým prostorem.

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 (tzn. vektorů je tolik, kolik je dimenze prostoru) je bází. V takovém případě stačí ověřovat pouze jednu z podmínek 1 a 2 z definice báze, jak ukazuje následující věta.

Věta 4.3.
Nechť V je vektorový prostor nad T, $\dim V = n$ $(n \geq 1)$ a nechť $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ je konečná posloupnost n vektorů z V. Pak následující výroky jsou ekvivalentní:

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

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

„$2 \Rightarrow 3$“: Nechť $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ jsou lineárně nezávislé vektory. Podle věty 4.2. 3. je lze doplnit na bázi, která však musí obsahovat n vektorů (vzhledem k předpokladu, že $\dim V = n$). Tedy vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ jsou bází prostoru V, což znamená, že také generují prostor V.

„$3 \Rightarrow 1$“: Nechť $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ generují prostor V. Podle věty 4.2. 2. z nich lze vybrat bázi, která však musí obsahovat n vektorů (vzhledem k předpokladu že $\dim V = n$). Tedy vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ jsou bází prostoru V. ■

Věta 4.4.
Nechť U_1, U_2 jsou podprostory vektorového prostoru V takové, že $U_1 \subseteq U_2$. Potom platí:

1. $\dim U_1 \leq \dim U_2$
2. $\dim U_1 = \dim U_2 \iff U_1 = U_2$.

Důkaz.
Pokud $U_1 = \{\boldsymbol{o}\}$ nebo $U_2 = \{\boldsymbol{o}\}$, pak obě tvrzení zřejmě platí (rozmyslete si podrobně proč).

Nechť tedy $U_1, U_2 \neq \{\boldsymbol{o}\}$ a nechť $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r$ je báze U_1, resp. $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s$ je báze U_2. Podle předpokladu věty je $U_1 \subseteq U_2$, tzn. musí být $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r \in U_2 = L(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s)$, přičemž vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r$ jsou lineárně nezávislé. Jsou tedy splněny předpoklady Steinitzovy věty. Potom:

1: podle Steinitzovy věty je $r \leq s$, neboli $\dim U_1 \leq \dim U_2$.

2: implikace „$\Leftarrow$“ zřejmě platí.

Dokazujme implikaci opačnou. Je-li tedy $\dim U_1 = \dim U_2$, tzn. $r = s$, pak opět podle Steinitzovy věty dostáváme, že $L(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s) = L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r)$, neboli $U_1 = U_2$. ■

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 U_1 vlastní podmnožinou podprostoru U_2 (tzn. $U_1 \subsetneqq U_2$), potom je $\dim U_1 < \dim U_2$. Jinými slovy řečeno, nemůže se stát, aby dva podprostory stejné dimenze byly ostře v inkluzi.

Věta 4.5. (Věta o dimenzi součtu a průniku podprostorů)
Nechť U_1, U_2 jsou podprostory vektorového prostoru V. Pak platí:

$$\dim(U_1 + U_2) \ + \ \dim(U_1 \cap U_2) \ = \ \dim U_1 \ + \ \dim U_2 \, .$$

Důkaz.
Je-li $U_1 = \{\boldsymbol{o}\}$ nebo $U_2 = \{\boldsymbol{o}\}$, pak tvrzení zřejmě platí (rozmyslete si podrobně proč!). Nechť tedy $\dim U_1 = r \neq 0$ a $\dim U_2 = s \neq 0$.

Průnik $U_1 \cap U_2$ je podprostorem ve V, a tedy je buď $U_1 \cap U_2 = \{\boldsymbol{o}\}$, nebo existuje báze $U_1 \cap U_2$, tj. lineárně nezávislé vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ s vlastností $U_1 \cap U_2 = L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k)$.

Podle věty 4.2.3. lze lineárně nezávislé vektory doplnit na bázi. Existují tedy vektory $\boldsymbol{a}_{k+1}, \dots, \boldsymbol{a}_r \in U_1$ tak, že $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k, \boldsymbol{a}_{k+1}, \dots, \boldsymbol{a}_r$ je báze U_1, a podobně existují vektory $\boldsymbol{b}_{k+1}, \dots, \boldsymbol{b}_s \in U_2$ tak, že $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k, \boldsymbol{b}_{k+1}, \dots, \boldsymbol{b}_s$ je báze U_2 (v případě $U_1 \cap U_2 = \{\boldsymbol{o}\}$ je zřejmě $k = 0$).

Nyní dokážeme, že vektory:

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

jsou bází podprostoru $U_1 + U_2$.

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

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

Označme:

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

Ze (3) při tomto označení dostáváme, že $\boldsymbol{x} = -t'_{k+1} \cdot \boldsymbol{b}_{k+1} - \dots - t'_s \cdot \boldsymbol{b}_s$. To však znamená, že $\boldsymbol{x} \in U_1 \cap U_2$ a lze pak psát:

$$\boldsymbol{x} \ = \ p_1 \cdot \boldsymbol{u}_1 + \dots + p_k \cdot \boldsymbol{u}_k \ = \ p_1 \cdot \boldsymbol{u}_1 + \dots + p_k \cdot \boldsymbol{u}_k + 0 \cdot \boldsymbol{a}_{k+1} + \dots + 0 \cdot \boldsymbol{a}_r. \tag{5}$$

Ale $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k, \boldsymbol{a}_{k+1}, \dots, \boldsymbol{a}_r$ je báze U_1, a tedy ze (4), (5) a z jednoznačnosti vyjádření vektoru pomocí báze plyne (mimo jiné), že $t_{k+1} = \dots = t_r = 0$. Dosadíme-li tyto hodnoty do (3), dostáváme:

$$t_1 \cdot \boldsymbol{u}_1 + \dots + t_k \cdot \boldsymbol{u}_k + t'_{k+1} \cdot \boldsymbol{b}_{k+1} + \dots + t'_s \cdot \boldsymbol{b}_s \ = \ \boldsymbol{o} \, .$$

Vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k, \boldsymbol{b}_{k+1}, \dots, \boldsymbol{b}_s$ jsou však bází U_2, tzn. jsou lineárně nezávislé a dostáváme tedy, že také $t_1 = \dots = t_k = t'_{k+1} = \dots = t'_s = 0$.

Ukázali jsme, že všechny koeficienty v rovnici (3) jsou rovny nule, a tedy vektory (2) jsou lineárně nezávislé.

β) Dokážeme, že vektory (2) generují podprostor $U_1 + U_2$, tzn. že platí rovnost:

$$L(\boldsymbol{w}_1, \dots, \boldsymbol{w}_k, \boldsymbol{u}_{k+1}, \dots, \boldsymbol{u}_r, \boldsymbol{v}_{k+1}, \dots, \boldsymbol{v}_s) \ = \ U_1 + U_2 \, . \tag{6}$$

„$\subseteq$“ : tato inkluze zřejmě platí (dokažte si sami technickým rozepsáním).

„$\supseteq$“ : nechť $\boldsymbol{x} \in U_1 + U_2$, tzn. lze psát $\boldsymbol{x} = \boldsymbol{x}_1 + \boldsymbol{x}_2$, kde $\boldsymbol{x}_1 \in U_1$, $\boldsymbol{x}_2 \in U_2$. Potom však

$$\boldsymbol{x}_1 \in U_1 = L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k, \boldsymbol{a}_{k+1}, \dots, \boldsymbol{a}_r) \subseteq L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k, \boldsymbol{a}_{k+1}, \dots, \boldsymbol{a}_r, \boldsymbol{b}_{k+1}, \dots, \boldsymbol{b}_s)$$
$$\boldsymbol{x}_2 \in U_2 = L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k, \boldsymbol{b}_{k+1}, \dots, \boldsymbol{b}_s) \subseteq L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k, \boldsymbol{a}_{k+1}, \dots, \boldsymbol{a}_r, \boldsymbol{b}_{k+1}, \dots, \boldsymbol{b}_s) \, ,$$

odkud již plyne, že
$$x = x_1 + x_2 \in L(w_1, \dots, w_k, u_{k+1}, \dots, u_r, v_{k+1}, \dots, v_s).$$
Dohromady tak dostáváme žádanou rovnost (6).

Dokázali jsme, že vektory (2) jsou bází $U_1 + U_2$, tzn. $\dim(U_1 + U_2) = r + s - k$. Potom však:
$$\dim(U_1 + U_2) + \dim(U_1 \cap U_2) = r + s - k + k = r + s = \dim U_1 + \dim U_2 ,$$
což je požadované tvrzení věty. ■

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:
$$U_1 = \{(a, b, 0) \mid a, b \in \mathbb{R}\}, \quad U_2 = \{(r, 0, s) \mid r, s \in \mathbb{R}\}, \quad U_3 = \{(0, u, v) \mid u, v \in \mathbb{R}\}.$$
Zřejmě je $\dim U_1 = \dim U_2 = \dim U_3 = 2$ a dále je (rozmyslete si proč)
$$U_1 + U_2 + U_3 = \mathbb{R}^3 \qquad \text{a} \qquad U_1 \cap U_2 \cap U_3 = \{\boldsymbol{o}\}.$$
Je tedy
$$\dim(U_1 + U_2 + U_3) + \dim(U_1 \cap U_2 \cap U_3) = 3 , \text{ ale } \dim U_1 + \dim U_2 + \dim U_3 = 6.$$

Poznámka.
V našich úvahách o konečných posloupnostech vektorů v předchozím textu (tj. v úvahách o lineární závislosti či nezávislosti vektorů a úvahách o generování) nehrálo pořadí vektorů žádnou podstatnou roli. Se zavedením pojmu báze se však otázka pořadí vektorů okamžitě vynoří a bude podstatné, v jakém pořadí vektory báze uvažujeme.

Přesněji řečeno, danou bází $u_1, \dots, u_n$ vektorového prostoru V chápeme jako uspořádanou n-tici vektorů z V, a tedy například 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
$$u_1, \dots, u_n$$
je báze vektorového prostoru V a nechť vektor $u \in V$ je vyjádřen ve tvaru:
$$u = t_1 \cdot u_1 + \dots + t_n \cdot u_n .$$
Pak číslo t_i nazýváme *i-tou souřadnicí vektoru u v bázi $u_1, \dots, u_n$* a uspořádanou n-tici čísel $(t_1, \dots, t_n)$ nazýváme *souřadnicemi vektoru u v bázi $u_1, \dots, u_n$*.

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 4.1. zajišťuje korektnost předchozí definice v tom smyslu, že každý vektor $u \in V$ má v dané bázi $u_1, \dots, u_n$ souřadnice a navíc jsou tyto souřadnice určeny jednoznačně.

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 $\boldsymbol{u} = (1, -2, 3)$. Potom:

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

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

3. vektor $\boldsymbol{u}$ 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 souřadnic vektoru v bázi (proveďte si podrobně sami).

Věta 4.6.
Nechť $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ je báze vektorového prostoru V. Nechť $t \in T$ a nechť vektor $\boldsymbol{x} \in V$, resp. $\boldsymbol{y} \in V$ má v bázi $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ souřadnice $(x_1, \dots, x_n)$, resp. $(y_1, \dots, y_n)$. Potom:

1. *vektor $\boldsymbol{x} + \boldsymbol{y}$ má v bázi $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ souřadnice $(x_1 + y_1, \dots, x_n + y_n)$*
2. *vektor $t \cdot \boldsymbol{x}$ má v bázi $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ souřadnice $(t \cdot x_1, \dots, t \cdot x_n)$.*

Důkaz.
Podle předpokladu je

$$\boldsymbol{x} = x_1 \cdot \boldsymbol{u}_1 + \dots + x_n \cdot \boldsymbol{u}_n \,, \qquad \text{resp.} \qquad \boldsymbol{y} = y_1 \cdot \boldsymbol{u}_1 + \dots + y_n \cdot \boldsymbol{u}_n \,,$$

tzn. potom (po úpravě) dostáváme, že

$$\boldsymbol{x} + \boldsymbol{y} = (x_1 + y_1) \cdot \boldsymbol{u}_1 + \dots + (x_n + y_n) \cdot \boldsymbol{u}_n$$

$$t \cdot \boldsymbol{x} = (t \cdot x_1) \cdot \boldsymbol{u}_1 + \dots + (t \cdot x_n) \cdot \boldsymbol{u}_n$$

odkud již ihned 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 tentokrát nebude studium obecných vlastností permutací libovolných množin, nýbrž permutace nám budou pouze pomocným nástrojem ke studiu dalších 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. $M = \{1, 2, \ldots, n\}$.

í části

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

Nechť $R = (r_1, \ldots, r_n)$ 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 $R = (r_1, \ldots, r_n)$, $S = (s_1, \ldots, s_n)$ 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.
Nejprve 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 vzhledem k n.

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

β) Předpokládejme, že obě tvrzení platí pro $1, \ldots, n-1$, a budeme je dokazovat pro n. Nechť $(r_1, \ldots, r_n)$ 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. ■

Věta 1.2.
Provedení jedné transpozice změní paritu daného pořadí.

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

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

β) Nechť $R = (r_1, \ldots, r_i, \ldots, r_j, \ldots, r_n)$ je dané pořadí. Provedením transpozice prvků r_i a r_j dostaneme pořadí $R' = (r_1, \ldots, r_j, \ldots, r_i, \ldots, r_n)$. 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. ■

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

Důkaz.
Tvrzení věty plyne ihned v vět 1.1. a 1.2. ■

Definice.
Nechť $M = \{1, 2, \ldots, n\}$ 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 předpisem: $P(i_t) = j_t$, pro $t = 1, \ldots, n$, budeme zapisovat ve tvaru dvouřádkové tabulky:

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

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:

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

Příklad 1.2.
Pro $n = 5$ jsou:

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

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 číslu $n!$.

Důkaz.
Zapíšeme-li každou permutaci v základním tvaru (1), pak různých permutací bude přesně tolik, kolik bude různých pořadí v dolním řádku. Těch je však $n!$, podle věty 1.1.1. ■

Definice.
Permutace P se nazývá *sudá permutace*, resp. *lichá permutace*, jestliže součet 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 $\frac{n!}{2}$ permutací sudých a $\frac{n!}{2}$ permutací lichých.

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. ■

§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 v ní hovořit o rovnosti dvou matic). Zcela přesně by bylo možné 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 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.

Výraz

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

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. $n = 1, 2, 3$.

$$n = 1: \quad \begin{vmatrix} a_{11} \end{vmatrix} = a_{11} \qquad\qquad n = 2: \quad \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11} \cdot a_{22} - a_{12} \cdot a_{21}$$

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

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 zjednoduší.

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 $(j_1, j_2, \dots, j_n)$ 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:

$$a_{k1} = b_{k1} + c_{k1}\,, \quad a_{k2} = b_{k2} + c_{k2}\,, \quad \dots \quad a_{kn} = b_{kn} + c_{kn}$$

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

$$\det A \;=\; \det B \,+\, \det C\,.$$

Schématicky zapsáno tedy 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:

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

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:

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

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

■

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 násobkem jiného řádku. 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*

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.. ■

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 tedy platí 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 vytvořená ze zvolených řádků a sloupců, tj. matice

$$M = \begin{pmatrix} a_{i_1 j_1} & a_{i_1 j_2} & \cdots & a_{i_1 j_k} \\ a_{i_2 j_1} & a_{i_2 j_2} & \cdots & a_{i_2 j_k} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i_k j_1} & a_{i_k j_2} & \cdots & a_{i_k j_k} \end{pmatrix}$$

se nazývá *submatice* matice A určená řádky $i_1, \ldots, i_k$ a sloupci $j_i \ldots, j_k$. 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:

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

Doplňkovou submaticí je pak:

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

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 čísla 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:

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

kde $I(t_1, \ldots, t_k)$ značí počet inverzí v permutaci $\begin{pmatrix} 1 & \cdots & k \\ t_1 & \cdots & t_k \end{pmatrix}$, resp. $I(t_{k+1}, \ldots, t_n)$ značí počet inverzí v permutaci $\begin{pmatrix} k+1 & \cdots & n \\ t_{k+1} & \cdots & t_n \end{pmatrix}$. Označíme-li $I(t_1, \ldots, t_n)$ počet inverzí v permutaci $\begin{pmatrix} 1 & \cdots & n \\ t_1 & \cdots & t_n \end{pmatrix}$, pak platí (rozmyslete si proč!): $I(t_1, \ldots, t_k) + I(t_{k+1}, \ldots, t_n) = I(t_1, \ldots, t_n)$. Potom však vynásobením obou členů z (3) dostáváme: $(-1)^{I(t_1,\ldots,t_n)} \cdot b_{1t_1} \cdot \cdots \cdot b_{nt_n}$, 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 je čtvercová matice řádu n a nechť je pevně zvoleno k řádků matice A, kde $0 < k < n$.
Pak determinant matice A je roven součtu všech $\binom{n}{k}$ součinů minorů řádu k, vybraných ze zvolených k řádků, s jejich algebraickými doplňky.

Důkaz.
Ze zvolených k řádků lze zřejmě vybrat submatici řádu k právě $\binom{n}{k}$ různými způsoby. Podle věty 2.6. součin členu příslušného minoru s členem jeho algebraického doplňku je členem determinantu matice A. Přitom je zřejmé, že dostáváme navzájem různé členy determinantu matice A.

K důkazu našeho tvrzení tedy stačí spočítat, zda uvedeným způsobem dostaneme všechny členy determinantu matice 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:

$$k! \cdot (n-k)! \cdot \tbinom{n}{k} = k! \cdot (n-k)! \cdot \tfrac{n!}{k! \cdot (n-k)!} = n!$$

členů determinantu matice 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 matice určitého řádu převádíme na výpočet jistého počtu determinantů matic menšího řádu.

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. Pak platí

1. *nechť i je pevně zvolený řádkový index. Potom*

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

2. *nechť j je pevně zvolený sloupcový index. Potom*

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

Důkaz.
První část důsledku je doslovným přepisem Laplaceovy věty, a sice pro $k = 1$. Druhá část důsledku je Laplaceova věta přeformulovaná pro sloupce (ve smyslu předchozí poznámky), a to opět pro $k = 1$. ■

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

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

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 stále 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:

$$c_{ij} = a_{ij} + b_{ij} \qquad \text{pro } i = 1, \ldots, m\,,\ \ j = 1, \ldots, n$$

   se nazývá *součet matic* A, B

2. matice $t \cdot A = (d_{ij}) \in \mathrm{Mat}_{mn}(T)$ definovaná:

$$d_{ij} = t \cdot a_{ij} \qquad \text{pro } i = 1, \ldots, m\,,\ \ j = 1, \ldots, n$$

   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.

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

Důkaz.
Z předchozí definice a ze známých vlastností obyčejného sčítání čísel ihned plyne, že $(\mathrm{Mat}_{mn}(T), +)$ je pologrupa, která je komutativní.

Lehce se ověří, že nulová matice 0_{mn} je nulou této pologrupy. Dále, pro libovolnou matici $A = (a_{ij}) \in \mathrm{Mat}_{mn}(T)$ je zřejmě 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, že pro pro libovolné $t, s \in T$ a $A, B \in \mathrm{Mat}_{mn}(T)$ platí:

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. $1 \cdot A = A$.

Tedy z definice vektorového prostoru plyne, že $\mathrm{Mat}_{mn}(T)$ je vektorový prostor nad T. Roli vektorů zde tedy hrají 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 $r = 1, \ldots, m$, $s = 1, \ldots, n$ 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:

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

Dostáváme tak celkem $m \cdot n$ matic:

$$U_{11}\,,\ \ldots\,,\ U_{1n}\,,\ U_{21}\,,\ \ldots\,,\ U_{2n}\,,\ \ldots\,,\ U_{m1}\,,\ \ldots\,,\ U_{mn}\,,$$

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

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

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

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:

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

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 typu m/p a platí:

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

tzn. dokázali jsme 1.

2: Dokáže se analogickým způsobem jako 1. ■

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

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

(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 je pro $n \geq 2$ nekomutativní 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 je matice typu m/n a B 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.
Nechť $A = (a_{ij})$ je typu m/n, resp. $B = (b_{ij})$ je typu n/p. Pak matice $(A \cdot B)' = (c_{ij})$ je typu p/m, přičemž její prvek c_{ij} je prvkem, který v matici $A \cdot B$ stojí v j-tém řádku a i-tém sloupci, tzn. $c_{ij} = \sum\limits_{k=1}^{n} a_{jk} \cdot b_{ki}$.

Analogicky, matice $B' \cdot A' = (d_{ij})$ je typu p/m, kde $d_{ij} = \sum\limits_{k=1}^{n} b_{ki} \cdot a_{jk} = \sum\limits_{k=1}^{n} a_{jk} \cdot b_{ki}$.

Dostáváme tak, že $c_{ij} = d_{ij}$, tzn. platí dokazovaná rovnost. ∎

Věta 3.7. (Cauchyova věta)
Nechť A, B jsou čtvercové matice řádu n. Pak platí:

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

Důkaz.
Nechť $A = (a_{ij})$, $B = (b_{ij})$. 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:

$$|H| \;=\; |A| \cdot |B|\,. \tag{1}$$

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 řádků matice K pak dostáváme:

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

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 ihned tvrzení věty. ■

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

Důsledek.
Nechť A, B jsou čtvercové matice stejného řádu n. Pak platí:

$$\textit{matice } A \cdot B \textit{ je regulární} \iff \textit{obě matice } A \textit{ i } B \textit{ jsou regulární.}$$

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

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

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

se nazývá *inverzní matice k matici* A a označuje se symbolem A^{-1}.

Poznámka.
Předchozí definice zřejmě nezaručuje, že k dané čtvercové matici A musí existovat matice inverzní. Nicméně, z faktu, že $(\mathrm{Mat}_{nn}(T), \cdot)$ je pologrupa s jedničkou E_n (což bezprostředně vyplývá z věty 3.5.) a z faktu, že pojem inverzní matice k matici A je totožný s pojmem inverzního prvku k danému prvku v této pologrupě, plyne , že k matici A existuje nejvýše jedna inverzní matice a používání označení A^{-1} je tedy korektní.

Následující věta uvede nutnou a dostatečnou podmínku existence inverzní matice k matici A. Její důsledek pak uvede vzorec pro výpočet této inverzní matice A^{-1}. K tomu však bude potřeba nejprve zavést následující pojem.

Definice.
Nechť $A = (a_{ij})$ je čtvercová matice řádu n. Pak matice

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

se nazývá *adjungovaná matice* k matici A.

Poznámka.
Vidíme, že v adjungované matici A^* se na i, j-tém místě nachází číslo A_{ji} (pozor na pořadí indexů!), tzn. algebraický doplněk prvku stojícího na j, i-tém místě v původní matici A. Ilustrujme si tento pojem na jednoduchém příkladu (příslušné výpočty si sami ověřte).

$$\text{Nechť} \quad A = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 3 & 2 \\ 1 & 0 & 2 \end{pmatrix}. \quad \text{Potom} \quad A^* = \begin{pmatrix} A_{11} & A_{21} & A_{31} \\ A_{12} & A_{22} & A_{32} \\ A_{13} & A_{23} & A_{33} \end{pmatrix} = \begin{pmatrix} 6 & -4 & 1 \\ 2 & 1 & -2 \\ -3 & 2 & 3 \end{pmatrix}.$$

Věta 3.8.
Nechť A je čtvercová matice řádu n. Pak platí:

$$\text{k matici } A \text{ existuje matice inverzní} \iff A \text{ je regulární matice.}$$

Důkaz.
Nechť $A = (a_{ij})$ je čtvercová matice řádu n. Dokážeme postupně obě implikace.

„$\Rightarrow$“: Nechť k matici A existuje inverzní matice A^{-1}. Pak platí $E_n = A \cdot A^{-1}$, odkud přechodem k determinantům a použitím Cauchyovy věty dostáváme:

$$1 = |E_n| = |A \cdot A^{-1}| = |A| \cdot |A^{-1}|.$$

Musí tedy být $|A| \neq 0$, což znamená, že A je regulární matice.

„$\Leftarrow$“: Nechť A je regulární matice, tzn. $|A| \neq 0$. Nyní vezmeme matici $X = \frac{1}{|A|} \cdot A^*$ a dokážeme, že X je inverzní maticí k matici A.
Označme $A \cdot X = (c_{ij})$. Potom po rozepsání dostáváme:

$$\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ \vdots & \vdots & & \vdots \\ c_{i1} & c_{i2} & \cdots & c_{in} \\ \vdots & \vdots & & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{pmatrix} = \frac{1}{|A|} \cdot \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} A_{11} & \cdots & A_{j1} & \cdots & A_{n1} \\ A_{12} & \cdots & A_{j2} & \cdots & A_{n2} \\ \vdots & & \vdots & & \vdots \\ \vdots & & \vdots & & \vdots \\ A_{1n} & \cdots & A_{jn} & \cdots & A_{nn} \end{pmatrix}$$

odkud

$$c_{ij} = \frac{1}{|A|} \cdot (a_{i1} \cdot A_{j1} + a_{i2} \cdot A_{j2} + \cdots + a_{in} \cdot A_{jn}).$$

Potom

– pro $i = j$ dostáváme (užitím důsledku Laplaceovy věty)

$$c_{ii} = \frac{1}{|A|} \cdot (a_{i1} \cdot A_{i1} + a_{i2} \cdot A_{i2} + \cdots + a_{in} \cdot A_{in}) = \frac{1}{|A|} \cdot |A| = 1.$$

– pro $i \neq j$ dostáváme (opět užitím důsledku Laplaceovy věty)

$$c_{ii} = \frac{1}{|A|} \cdot (a_{i1} \cdot A_{j1} + a_{i2} \cdot A_{j2} + \cdots + a_{in} \cdot A_{jn}) = \frac{1}{|A|} \cdot 0 = 0.$$

uvědomme si, že výraz v závorce je roven nule, protože podle důsledku Laplaceovy věty se jedná o determinant matice, v níž i-tý a j-tý řádek jsou stejné (oba dva zmiňované řádky sestávají z prvků $a_{i1}, a_{i2}, \cdots a_{in}$).

Dostáváme tedy, že $A \cdot X = E_n$. Analogickým způsobem se dokáže, že také $X \cdot A = E_n$, což znamená, že matice X je hledaná inverzní maticíe k matici A. ■

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

Důkaz.
Tvrzení plyne ihned z 2. části důkazu předchozí věty. ■

Poznámka.
Pokud ověřujeme, zda matice X je inverzní maticí k matici A, pak stačí ověřovat pouze jednu z obou podmínek uvedených v definici inverzní matice k matici A, tj. jednu z rovností

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

protože druhá rovnost je v tomto případě již vynucena. Je−li například $A \cdot X = E_n$, pak je matice A regulární a existuje matice A^{-1}. Po vynásobení výchozího vztahu zleva maticí A^{-1} a zprava maticí A dostáváme

$$A^{-1} \cdot (A \cdot X) \cdot A = A^{-1} \cdot E_n \cdot A \,,$$

odkud po úpravě vychází $X \cdot A = E_n$.

Některé jednoduché základní vlastnosti inverzních matic k regulárním maticím 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. $|A^{-1}| = \dfrac{1}{|A|}$
4. $(A')^{-1} = (A^{-1})'$.

Důkaz.
1. a 2. plynou z věty 3.8., z faktu, že $(\mathrm{Mat}_{nn}(T), \cdot)$ je pologrupa s jedničkou a ze známých vlastností pologrup.

3: Zřejmě $A \cdot A^{-1} = E_n$, odkud podle Cauchyovy věty je

$$|A| \cdot |A^{-1}| = |E_n| = 1 \,, \text{ tzn. } |A^{-1}| = \tfrac{1}{|A|} \,.$$

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.
Množina všech regulárních matic řádu n (nad T) s operací násobení matic je grupa, která je pro $n \geq 2$ nekomutativní.

Důkaz.
Označme množinu všech regulárních matic řádu n nad T symbolem $(\mathrm{Reg}_{nn}(T), \cdot)$.

Podle důsledku Cauchyovy věty je $(\mathrm{Reg}_{nn}(T), \cdot)$ grupoidem, podle věty 3.3. je pologrupou a zřejmě $E_n \in \mathrm{Reg}_{nn}(T)$ je zde jedničkou. Podle věty 3.8. ke každému prvku (tj. matici) z $\mathrm{Reg}_{nn}(T)$ existuje prvek (matice) inverzní, a tedy $(\mathrm{Reg}_{nn}(T), \cdot)$ je grupou.

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

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

Potom zřejmě A, B jsou regulární, tj. $A, B \in \mathrm{Reg}_{nn}(T)$ a platí $A \cdot B \neq B \cdot A$ (ověřte si sami výpočtem – počítejte přitom prvek v prvním řádku a $(n-1)$ - ním sloupci obou součinů matic). Tedy uvažovaná grupa není komutativní. ■

Poznamenejme, že výše uvedená multiplikativní grupa regulárních matic řádu n $(n \geq 2)$ je dalším poměrně jednoduchým příkladem nekomutativní grupy.

§4. Hodnost matice

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

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \qquad \text{kde } a_{ij} \in T\,.$$

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 U 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 zřejmé, že T^n a T^m jsou obecně dva různé vektorové prostory a totéž platí i o podprostorech U a H. Přesto však ukážeme, že dimenze obou těchto podprostorů musí být stejné, tzn. $\dim U = \dim H$.

Definice.
Nechť A je matice typu m/n nad T. Pak dimenze podprostoru vektorového prostoru T^n, který je generován 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 vektorového prostoru a z definice báze vektorového prostoru. ■

Poznámka.
Z předchozího je zřejmé, že hodnost matice A je rovna nule, právě když A je nulovou maticí. Je-li 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, tzn. podle věty 3.1. kapitoly I. a 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 $h(A) = k$. ∎

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 $h(A) = h(A')$. ∎

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. ∎

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 a uvedeme charakterizaci regulární matice pomocí její hodnosti, resp. pomocí lineární nezávislosti jejích řádků nebo sloupců.

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 ⇒ 2“: Nechť A je regulární, tzn. $|A| \neq 0$. Pak z věty 4.2. plyne, že $h(A) = n$.
„2 ⇒ 3“: Plyne z věty 4.1.
„3 ⇒ 4“: Plyne z vět 4.1. a 4.3.
„4 ⇒ 1“: Plyne z vět 4.3. a 4.2. ■

Předchozí věta nám samozřejmě zároveň podává i odpovídající 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.

Nyní se vrátíme ještě k obdélníkovým maticím a ukážeme si, co je možno říci o hodnosti součinu dvou matic.

Věta 4.5.
Nechť A je matice typu m/n. Pak platí:
1. *je-li B matice typu n/p, pak:*
$$h(A \cdot B) \leq h(A) \qquad a \qquad h(A \cdot B) \leq h(B),$$
2. *je-li R regulární matice řádu n, resp. S je regulární matice řádu m, pak:*
$$h(A \cdot R) = h(A) \qquad a \qquad h(S \cdot A) = h(A).$$

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 (vpravo) přidáno jistých p sloupců. Z definice součinu matic ale plyne, že:

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

pro pevné j a pro každé $i = 1, \ldots, m$. Jinak zapsáno to znamená, že pro každé $j = 1, \ldots, p$ platí:

$$\begin{pmatrix} c_{1j} \\ \vdots \\ c_{mj} \end{pmatrix} = b_{1j} \cdot \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix} + b_{2j} \cdot \begin{pmatrix} a_{12} \\ \vdots \\ a_{m2} \end{pmatrix} + \cdots + b_{nj} \cdot \begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix}.$$

Vidíme tedy, že každý přidaný sloupec je vždy lineární kombinací prvních n sloupců, odkud vyplývá, že $h(D) = h(A)$.

Matici D však můžeme také chápat jakožto matici $A \cdot B$, k níž jsme (zleva) přidali jistých n sloupců. Přidáním sloupců k nějaké matici se však hodnost buď nezmění nebo zvětší. Poto tedy platí $h(A \cdot B) \leq h(D)$.

Dohromady tak dostáváme, že $h(A \cdot B) \leq h(A)$.

Analogickým způsobem (tj. přidáním všech řádků matice $A \cdot B$ k řádkům matice B) se dokáže, že $h(A \cdot B) \leq h(B)$ (rozmyslete si podrobně sami!).

2: Podle právě dokázané části 1 je $h(A \cdot R) \leq h(A)$. Dokážeme, že platí také opačná nerovnost. Podle předpokladu je matice R regulární, tzn. existuje k ní inverzní matice R^{-1} a lze psát:

$$A = (A \cdot R) \cdot R^{-1}.$$

Nyní však opět podle již dokázané části 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 (proveďte si podrobně sami). ■

Na závěr tohoto paragrafu si odvodíme jednu jednoduchou praktickou metodu výpočtu hodnosti matice. K tomu však bude potřeba nejprve zavést následující pojem.

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 U. Důležité je (jak ukáže následující věta), že provedení libovolné elementární řádkové úpravy neovlivní tento podprostor U.

Věta 4.6.
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 $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m$. Podle věty 2.3. 2., kap. I., je podprostor generovaný řádky matice A roven množině všech lineárních kombinací těchto řádků, tzn.:

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

Podprostor $L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m)$ se nezmění, jestliže:

α) zaměníme libovolně pořadí řádků matice A, což je zřejmé.

β) vynásobíme i-tý řádek matice A nenulovým číslem $t \in T$.

Zřejmě je $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_i, \ldots, \boldsymbol{u}_m \in L(\boldsymbol{u}_1, \ldots, t \cdot \boldsymbol{u}_i, \ldots, \boldsymbol{u}_m)$ (rozmyslete si, jak se přitom využije fakt, že $t \neq 0$), a tedy podle věty 1.4., kap. I. je

$$L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_i, \ldots, \boldsymbol{u}_m) \subseteq L(\boldsymbol{u}_1, \ldots, t \cdot \boldsymbol{u}_i, \ldots, \boldsymbol{u}_m).$$

Podobně je $\boldsymbol{u}_1, \ldots, t \cdot \boldsymbol{u}_i, \ldots, \boldsymbol{u}_m \in L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_i, \ldots, \boldsymbol{u}_m)$, a tedy opět podle věty 1.4., kap. I. je

$$L(\boldsymbol{u}_1, \ldots, t \cdot \boldsymbol{u}_i, \ldots, \boldsymbol{u}_m) \subseteq L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_i, \ldots, \boldsymbol{u}_m).$$

Dohromady pak dostáváme požadovanou rovnost:

$$L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_i, \ldots, \boldsymbol{u}_m) = L(\boldsymbol{u}_1, \ldots, t \cdot \boldsymbol{u}_i, \ldots, \boldsymbol{u}_m).$$

γ) přičteme k i-tému řádku matice A t-násobek j-tého řádku ($i \neq j$).

Platí, že $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_i, \ldots, \boldsymbol{u}_m \in L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_i + t \cdot \boldsymbol{u}_j, \ldots, \boldsymbol{u}_m)$ (rozmyslete si podrobně proč tomu tak je a zejména si uvědomte, jakým způsobem se vektor $\boldsymbol{u}_i$ napíše jako lineární kombinace vektorů $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_i + t \cdot \boldsymbol{u}_j, \ldots, \boldsymbol{u}_m$). Potom podle věty 1.4., kapitoly I. dostáváme, že $L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_i, \ldots, \boldsymbol{u}_m) \subseteq L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_i + t \cdot \boldsymbol{u}_j, \ldots, \boldsymbol{u}_m)$.

Podobně je $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_i + t \cdot \boldsymbol{u}_j, \ldots, \boldsymbol{u}_m \in L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_i, \ldots, \boldsymbol{u}_m)$, a tedy podle věty 1.4., kapitoly I. dostáváme, že $L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_i + t \cdot \boldsymbol{u}_j, \ldots, \boldsymbol{u}_m) \subseteq L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_i, \ldots, \boldsymbol{u}_m)$.

Dohromady potom platí rovnost: $L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_i, \ldots, \boldsymbol{u}_m) = L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_i + t \cdot \boldsymbol{u}_j, \ldots, \boldsymbol{u}_m)$.

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

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

Důkaz.
Tvrzení plyne bezprostředně z definice hodnosti matice a z předchozí věty. ∎

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“. Speciálně, 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:

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

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 4.7.
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!). ■

Věta 4.8.
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 $h(A) = k$. ■

Pomocí posledních dvou vět a důsledku věty 4.6. 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 4.7., který byl konstruktivní), v němž pak jen spočítáme počet nenulových řádků. Celý postup si ukážeme na následujícím příkladu.

Příklad 4.1.
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 $\rightarrow$. Z úsporných důvodů provádíme obvykle vždy několik elementárních řádkových úprav typu 3 najednou. Tedy:

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

$$\rightarrow \begin{pmatrix} 1 & 2 & 0 & 0 & -1 & -2 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & -4 & -9 \\ 0 & 0 & 0 & 0 & 4 & 9 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 2 & 0 & 0 & -1 & -2 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & -4 & -9 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

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

§5. Další vlastnosti a užití matic

V tomto paragrafu si nejprve ukážeme možnosti užití výpočtu hodnosti matice při řešení úloh o vektorových prostorech T^n a následně odvodíme další metodu výpočtu inverzní matice k dané matici. Na závěr se budeme zabývat užitím maticového aparátu při studiu vztahů mezi dvěma bázemi téhož vektorového prostoru.

Metodu výpočtu hodnosti matice pomocí elementárních řádkových úprav 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 U, 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 U (jak plyne z vět 4.6. a 4.8.). Podobným způsobem lze postupovat například při zjišťování dimenze a báze součtu dvou podprostorů v T^n, jak ukazuje následující příklad.

Příklad 5.1.
Ve vektorovém prostoru $\mathbb{R}^5$ jsou dány podprostory $U_1 = [\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3]$ a $U_2 = [\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3]$, kde

$$\boldsymbol{a}_1 = (1, -1, 2, 4, 0),\ \boldsymbol{a}_2 = (0, 0, 1, 3, 2),\ \boldsymbol{a}_3 = (1, -1, 1, 1, -2)\,,$$

resp.

$$\boldsymbol{b}_1 = (0, 1, 0, 2, -2),\ \boldsymbol{b}_2 = (-1, 2, 1, 3, -2),\ \boldsymbol{b}_3 = (-1, 0, 1, -1, 2)\,.$$

Určete dimenzi a bázi podprostoru $U_1 + U_2$.

Řešení: Vektory $\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3, \boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3$ generují podprostor $U_1 + U_2$, tzn.

$$U_1 + U_2 = [\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3, \boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3]$$

(rozepište si podrobně sami, že tomu tak skutečně je!). Stačí tedy napsat uvedených šest vektorů do řádků matice a tuto matici převést elementárními řádkovými úpravami na schodovitý tvar.

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

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

Tedy $\dim(W_1 + W_2) = 4$, přičemž bázi $W_1 + W_2$ tvoří například nenulové řádky poslední matice, tj. vektory

$$\boldsymbol{u}_1 = (1, -1, 2, 4, 0),\ \boldsymbol{u}_2 = (0, 1, 0, 2, -2),\ \boldsymbol{u}_3 = (0, 0, 1, 3, 2),\ \boldsymbol{u}_4 = (0, 0, 0, 4, 6)\,.$$

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:

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

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 5.1.
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 jedné 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 4.7. a 4.8.) 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 bezprostředně vyplývá 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 současně 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:

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

což znamená, že $(R_s \cdot \cdots \cdot R_2 \cdot R_1) = A^{-1}$. Současně však tytéž úpravy aplikujeme na jednotkovou matici E_n a dostaneme:

$$(R_s \cdot \cdots \cdot R_2 \cdot R_1) \cdot E_n = (R_s \cdot \cdots \cdot R_2 \cdot R_1) = A^{-1}.$$

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 přitom oddělovat šipkou.

Příklad 5.2.
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:

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

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

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. Nyní budeme vyšetřovat vzájemný vztah mezi dvěma bázemi daného vektorového prostoru, resp. vztah mezi souřadnicemi téhož vektoru v různých bázích daného prostoru.

Definice.
Nechť V je vektorový prostor nad T a nechť $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ a $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ jsou dvě báze prostoru V. Nechť dále je:

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

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 přechodu od báze* $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ *k bázi* $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$.

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 žádným způsobem zaměňovat.

2. Matice přechodu od jedné báze k druhé bázi vektorového prostoru V musí být vždy regulární, což plyne z rovnic (1) a z lineární nezávislosti vektorů druhé báze (proveďte si sami podrobné rozepsání).

Příklad 5.3.

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

$$\boldsymbol{u}_1 = (1,1,1), \quad \boldsymbol{u}_2 = (1,1,0), \quad \boldsymbol{u}_3 = (1,0,0),$$
$$\boldsymbol{v}_1 = (2,3,2), \quad \boldsymbol{v}_2 = (3,1,2), \quad \boldsymbol{v}_3 = (4,3,3).$$

Technickým rozepsáním se ověří, že platí:

$$\begin{aligned} \boldsymbol{v}_1 &= 2 \cdot \boldsymbol{u}_1 + \boldsymbol{u}_2 - \boldsymbol{u}_3 \\ \boldsymbol{v}_2 &= 2 \cdot \boldsymbol{u}_1 - \boldsymbol{u}_2 + 2 \cdot \boldsymbol{u}_3 \\ \boldsymbol{v}_3 &= 3 \cdot \boldsymbol{u}_1 + \boldsymbol{u}_3 \end{aligned} \qquad \text{resp.} \qquad \begin{aligned} \boldsymbol{u}_1 &= \boldsymbol{v}_1 + \boldsymbol{v}_2 - \boldsymbol{v}_3 \\ \boldsymbol{u}_2 &= -4 \cdot \boldsymbol{v}_1 - 5 \cdot \boldsymbol{v}_2 + 6 \cdot \boldsymbol{v}_3 \\ \boldsymbol{u}_3 &= -3 \cdot \boldsymbol{v}_1 - 3 \cdot \boldsymbol{v}_2 + 4 \cdot \boldsymbol{v}_3 \end{aligned}$$

odkud již plyne, že matice A přechodu od báze $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ k bázi $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$, resp. matice B přechodu od báze $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ k bázi $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ mají tvar:

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

Vidíme tedy, že především je $A \neq B$, ale na druhé straně se výpočtem lehce zjistí, že $A \cdot B = E_3$, což znamená, že $B = A^{-1}$. Tedy, zaměněním pořadí bází $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ a $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ jsme v tomto případě dostali matici přechodu, která je k původní matici přechodu inverzní. Následující věta ukáže, že tomu tak musí být vždycky.

Věta 5.2.

Nechť $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ a $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ jsou dvě báze vektorového prostoru V. Nechť matice A je maticí přechodu od báze $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ k bázi $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$.

Potom maticí přechodu od báze $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ k bázi $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ je matice A^{-1}.

Důkaz.

Nechť $A = (a_{ij})$. Pak podle definice matice přechodu od báze $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ k bázi $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ je:

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

Nechť dále $B = (b_{ij})$ je matice přechodu od báze $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ k bázi $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$. Pak je:

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

Po dosazení dostáváme:

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

pro každé $j = 1, \ldots, n$.

Podle věty 4.1., kap. I., se každý vektor z V dá napsat pouze jediným způsobem jako lineární kombinace vektorů dané báze. Zřejmě však lze také psát :

$$\boldsymbol{v}_j \;=\; 0 \cdot \boldsymbol{v}_1 + \cdots + 0 \cdot \boldsymbol{v}_{j-1} + 1 \cdot \boldsymbol{v}_j + 0 \cdot \boldsymbol{v}_{j+1} + \cdots + 0 \cdot \boldsymbol{v}_n, \qquad \text{pro každé } j = 1, \ldots, n.$$

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 dvou bází prostoru V je jednoznačně určena matice přechodu od první báze ke druhé bázi, tj. jistá regulární matice A.

Podobně však, máme-li dánu bázi $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ a nějakou regulární matici A, pak je těmito dvěma údaji (pomocí vztahů (1)) jednoznačně určena báze $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ taková, že matice A je maticí přechodu od báze $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ k bázi $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$.

Stejně tak, zadáním báze $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ a regulární matice A je jednoznačně určena báze $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ taková, že A je maticí přechodu od báze $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ k bázi $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$. Bázi $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ můžeme v tomto případě zkonstruovat např. užitím věty 5.2. (tzn. ze vztahů (1), pomocí báze $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ a 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

$$\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n \qquad \text{a} \qquad \boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$$

jsou dvě báze vektorového prostoru V a nechť $A = (a_{ij})$ je matice přechodu od báze $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ k bázi $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$. Dále nechť $\boldsymbol{w} \in V$ je vektor, přičemž $\boldsymbol{w}$ má v bázi $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$, resp. v bázi $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$, souřadnice:

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

To ale znamená, že platí:

$$\boldsymbol{w} = x_1 \cdot \boldsymbol{u}_1 + \cdots + x_n \cdot \boldsymbol{u}_n \tag{2}$$

$$\boldsymbol{w} = y_1 \cdot \boldsymbol{v}_1 + \cdots + y_n \cdot \boldsymbol{v}_n \tag{3}$$

Dosadíme-li do (3) vztahy (1), dostáváme:

$$\boldsymbol{w} = \sum_{j=1}^{n} y_j \cdot \boldsymbol{v}_j = \sum_{j=1}^{n} y_j \cdot \sum_{k=1}^{n} a_{kj} \cdot \boldsymbol{u}_k = \sum_{k=1}^{n} \left(\sum_{j=1}^{n} a_{kj} \cdot y_j \right) \cdot \boldsymbol{u}_k. \tag{4}$$

Nyní však porovnáním pravých stran (2) a (4) 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 způsobem jsme tedy dostali souřadnice vektoru $\boldsymbol{w}$ v bázi $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ vyjádřené pomocí souřadnic téhož vektoru v bázi $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$.

Kdybychom chtěli naopak vyjádřit souřadnice vektoru $\boldsymbol{w}$ v bázi $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ pomocí jeho souřadnic v bázi $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$, 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 T).

Řešení soustavy (1) je každá uspořádaná n-tice $(t_1, \dots, t_n)$ prvků z T taková, že po dosazení t_i za x_i $(i = 1, \dots, n)$ 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:

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

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:

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

pak můžeme zřejmě soustavu (1) zapsat stručněji 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 její řešení (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 této soustavy:*

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 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 uspořádaná n–tice $(t_1, \ldots, t_n)$ řešením soustavy (1), pak zřejmě je $(t_1, \ldots, t_n)$ také řešením soustavy (2).

Naopak, nechť $(t_1, \dots, t_n)$ 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 $(t_1, \dots, t_n)$ 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 $p_2, \dots, p_k \in T$. 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 $(t_1, \dots, t_n)$ je řešením (3), právě když $(t_1, \dots, t_n)$ 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 rovnic 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 4.7., 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 budeme též nazývat *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 této matice, tj. ve třetí rovnici poslední soustavy, jsou všechny koeficienty u neznámých nulové a absolutní člen je od nuly různý.

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

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

Řešení:

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

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

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

Dostáváme soustavu rovnic, 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.

Výsledek můžeme podle potřeby též zapsat v množinovém tvaru, tzn. můžeme říci, že daná soustava lineárních rovnic má množinu řešení

$$\{(2t - s, t, 2, s) \mid t, s \in \mathbb{R} \text{ libovolná } \}\,.$$

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. Například v soustavě dvou lineárních 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 (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 musí být 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. ■

Frobeniova věta je jednoduchým 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 speciální 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 platí:

$$x_j = \frac{|A_j|}{|A|} \qquad \textit{pro } j = 1, 2, \ldots, n\,,$$

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:

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

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 provedeného 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. Dosazením do (3) dostáváme:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_j \\ \vdots \\ x_n \end{pmatrix} = \frac{1}{|A|} \cdot \begin{pmatrix} A_{11} & A_{21} & \cdots & A_{n1} \\ \vdots & \vdots & \vdots & \vdots \\ A_{1j} & A_{2j} & \cdots & A_{nj} \\ \vdots & \vdots & \vdots & \vdots \\ A_{1n} & A_{2n} & \cdots & A_{nn} \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_j \\ \vdots \\ b_n \end{pmatrix}$$

Vyjádříme-li z této maticové rovnice neznámou x_j, pak rozepsáním a užitím důsledku Laplaceovy věty dostáváme:

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

Tedy skutečně je: $x_j = \dfrac{|A_j|}{|A|}$ pro každé $j = 1, \dots, n$. ■

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 bez újmy na obecnosti 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 lineárních rovnic:

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= b_1 \\ &\vdots \\ a_{r1}x_1 + \cdots + a_{rn}x_n &= b_r \end{aligned} \tag{4}$$

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 nyní použít Cramerovo pravidlo, čímž dostaneme jediné řešení $(c_1, \dots, c_r)$ soustavy (5).
Potom však je uspořádaná n-tice $(c_1, \dots, c_r, c_{r+1}, \dots, c_n)$ zřejmě řešením soustavy (4), a tedy i řešením soustavy (1).

Naopak musíme ukázat, že každé řešení soustavy (1) lze obdržet popsaným způsobem. Nechť tedy $(c_1, \dots, c_n)$ je libovolné řešení soustavy (1). Pak $(c_1, \dots, c_n)$ je řešením soustavy (4). Dosadíme-li c_j za x_j pro $j = r+1, \dots, n$, pak $(c_1, \dots, c_r)$ je řešením soustavy (5), a musí tedy být rovno tomu jedinému řešení, které dostaneme použitím Cramerova pravidla. Tedy řešení $(c_1, \dots, c_n)$ jsme dostali postupem uvedeným ve větě. ■

Důsledek.
Nechť je dána soustava lineárních rovnic (1)*. Potom:*

1. *soustava* (1) *má jediné řešení právě když* $h(A) = h(\overline{A}) = n$,
2. *soustava* (1) *má nekonečně mnoho řešení právě když* $h(A) = h(\overline{A}) < n$.

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.

§3. Homogenní soustavy lineárních rovnic

Definice.
Soustava lineárních rovnic

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= 0 \\ &\vdots \\ a_{k1}x_1 + a_{k2}x_2 + \cdots + a_{kn}x_n &= 0 \end{aligned} \tag{1}$$

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. Uspořádaná n-tice $(0, 0, \ldots, 0)$ je zřejmě vždy 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 je dána homogenní soustava (1) *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 $h(\overline{A}) = h(A)$. ∎

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 U 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 U všech řešení homogenní soustavy (1) *je podprostorem ve vektorovém prostoru T^n a platí:* $\dim U = n - h(A)$.

Důkaz.
I. Dokážeme, že U je podprostor v T^n.
Zřejmě je $(0, 0, \ldots, 0) \in U$, tzn. $U \neq \emptyset$. Dále, nechť $(c_1, \ldots, c_n), (d_1, \ldots, d_n) \in U$, $t, s \in T$ libovolné, tzn. je: $\sum\limits_{j=1}^{n} a_{ij}c_j = 0$, $\sum\limits_{j=1}^{n} a_{ij}d_j = 0$ pro každé $i = 1, \ldots, k$. Potom je:

$$\sum_{j=1}^{n} a_{ij}(t \cdot c_j + s \cdot d_j) \;=\; t \cdot \sum_{j=1}^{n} a_{ij}c_j + s \cdot \sum_{j=1}^{n} a_{ij}d_j \;=\; t \cdot 0 + s \cdot 0 \;=\; 0$$

pro každé $i = 1, \dots, k$. To však znamená, že $t \cdot (c_1, \dots, c_n) + s \cdot (d_1, \dots, d_n) \in U$, a tedy U je podprostor v T^n.

II. Dokážeme, že $\dim U = n - h(A)$.
Označme $h(A) = r$. Zřejmě musí být $0 \leq r \leq n$. Je-li $r = 0$, pak $U = T^n$, resp. je-li $r = n$, pak $U = \{(0, 0, \dots, 0)\}$, a v obou případech platí, že $\dim U = n - r = n - h(A)$.

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 U rovno množině všech řešení soustavy:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1r}x_r + a_{1,r+1}x_{r+1} + \cdots + a_{1n}x_n &= 0 \\ &\vdots \\ a_{r1}x_1 + a_{r2}x_2 + \cdots + a_{rr}x_r + a_{r,r+1}x_{r+1} + \cdots + a_{rn}x_n &= 0 \end{aligned} \tag{2}$$

v níž volnými neznámými jsou neznámé $x_{r+1}, \dots, x_n$.

Označme $\boldsymbol{u}_1, \dots, \boldsymbol{u}_{n-r}$ následující řešení soustavy (2), a tedy i soustavy (1):

$$\begin{aligned} \boldsymbol{u}_1 &= (c_{11}, \quad \dots, c_{1r}, \quad 1, 0, 0, \dots, 0, 0) \\ \boldsymbol{u}_2 &= (c_{21}, \quad \dots, c_{2r}, \quad 0, 1, 0, \dots, 0, 0) \\ &\vdots \\ \boldsymbol{u}_{n-r} &= (c_{n-r,1}, \dots, c_{n-r,r}, 0, 0, 0, \dots, 0, 1). \end{aligned}$$

Tedy $\boldsymbol{u}_1, \dots, \boldsymbol{u}_{n-r} \in U$ a ukážeme, že tyto vektory tvoří bázi podprostoru U.

α) Vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_{n-r}$ jsou zřejmě lineárně nezávislé (rozmyslete si podrobně proč).

β) Dokážeme, že vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_{n-r}$ generují U, tzn., že $L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_{n-r}) = U$.

Inkluze „$\subseteq$“ je zřejmá a stačí tedy dokázat inkluzi opačnou. Nechť $\boldsymbol{v} = (v_1, \dots, v_n) \in U$, tzn. $\boldsymbol{v}$ je řešením soustavy (1). Uvažme vektor

$$\boldsymbol{y} = v_{r+1} \cdot \boldsymbol{u}_1 + \cdots + v_n \cdot \boldsymbol{u}_{n-r}.$$

Zřejmě je $\boldsymbol{y} \in U$ a platí $\boldsymbol{y} = (y_1, \dots, y_r, v_{r+1}, \dots, v_n)$, kde $y_1, \dots, y_r$ jsou nějaká čísla z T. Vidíme, že vektory $\boldsymbol{v}$ a $\boldsymbol{y}$ mají posledních $(n - r)$ složek shodných a oba jsou z U, tzn. oba jsou řešeními (2). Pak ovšem podle obecného Cramerova pravidla musí být

$$y_1 = v_1, \ \dots, \ y_r = v_r,$$

odkud plyne, že $\boldsymbol{v} = \boldsymbol{y}$. Vektor $\boldsymbol{v}$ je tedy lineární kombinací vektorů $\boldsymbol{u}_1, \dots, \boldsymbol{u}_{n-r}$, což jsme měli dokázat.

Dohromady dostáváme, že $\dim U = n - r = n - h(A)$. ■

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 U je nejvýhodnější postupovat tak, že si nejprve obecně vyjádříme řešení dané homogenní soustavy, potom $(n - h(A))$ volných neznámých zvolíme $(n - h(A))$ lineárně nezávislými způsoby a spočítáme vektory báze U. Je zřejmé, že bází U 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 U homogenní soustavy (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, například x_2 a x_4, přičemž pak je $x_3 = -x_4$, $x_1 = -x_2 + 2x_4$. Řešení soustavy jsou tedy tvaru

$$(-t + 2s, t, -s, s) \qquad \text{pro libovolná } t, s \in \mathbb{R}\,.$$

1. volíme-li například $t = 1,\ s = 0$, resp. $t = 0,\ s = 1$, dostáváme bázi podprostoru řešení U tvaru

$$(-1, 1, 0, 0)\,,\ (2, 0, -1, 1)\,.$$

2. podobně, volíme-li například $t = 1,\ s = 1$, resp. $t = -1,\ s = \sqrt{2}$ (uvědomme si, že se jedná o dvě lineárně nezávislé volby!), dostáváme bázi podprostoru řešení U 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 U je libovolný podprostor vektorového prostoru T^n. Pak existuje homogenní soustava lineárních rovnic (o n neznámých, nad T), jejíž množina řešení je rovna U.

Důkaz.
Je-li $U = \{(0, \dots, 0)\}$, resp. $U = T^n$, pak věta zřejmě platí (hledanou soustavou je pak např. soustava s maticí soustavy E_n, resp. 0_{nn}).

Nechť tedy $\{(0, \dots, 0)\} \subsetneqq U \subsetneqq T^n$ a nechť vektory:

$$\boldsymbol{u}_1 = (u_{11}, u_{12}, \dots, u_{1n})\,,\ \dots\,,\ \boldsymbol{u}_k = (u_{k1}, u_{k2}, \dots, u_{kn})$$

jsou bází podprostoru U. Utvořme nejprve homogenní soustavu lineárních rovnic

$$\begin{aligned} u_{11}x_1 + u_{12}x_2 + \cdots + u_{1n}x_n &= 0 \\ &\vdots \\ u_{k1}x_1 + u_{k2}x_2 + \cdots + u_{kn}x_n &= 0\,. \end{aligned} \tag{3}$$

Hodnost matice soustavy (3) je rovna k, neboť její řádky jsou lineárně nezávislé. Označme písmenem W podprostor řešení soustavy (3). Podle věty 3.2. je $\dim W = n - k\,(> 0)$. Nechť:

$$\boldsymbol{w}_1 = (w_{11}, w_{12}, \dots, w_{1n})\,,\ \dots\,,\ \boldsymbol{w}_{n-k} = (w_{n-k,1}\,,\ w_{n-k,2}\,,\ \dots\,,\ w_{n-k,n})$$

je pevná báze podprostoru W. Utvořme další homogenní soustavu lineárních rovnic

$$\begin{aligned} w_{11}x_1 + \quad w_{12}x_2 + \cdots + \quad w_{1n}x_n &= 0 \\ &\vdots \\ w_{n-k,1}x_1 + w_{n-k,2}x_2 + \cdots + w_{n-k,n}x_n &= 0\,. \end{aligned} \tag{4}$$

o níž dokážeme, že je hledanou soustavou, tzn. označíme-li podprostor řešení soustavy (4) jako H, musíme dokázat, že $U = H$.

α) Nejprve dokážeme množinovou inkluzi $U \subseteq H$.
Platí, že vektor $\boldsymbol{u}_1$ je řešením soustavy (4), protože po jeho dosazení do (4), úpravě a využití toho, že vektory $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{n-k}$ splňují první rovnici ze (3) dostáváme:

$$\begin{aligned} w_{11}u_{11} + \cdots + \quad w_{1n}u_{1n} &= \quad u_{11}w_{11} + \cdots + \quad u_{1n}w_{1n} = 0 \\ &\vdots \qquad\qquad\qquad\qquad \vdots \\ w_{n-k,1}u_{11} + \cdots + w_{n-k,n}u_{1n} &= u_{11}w_{n-k,1} + \cdots + u_{1n}w_{n-k,n} = 0\,. \end{aligned}$$

Tedy $\boldsymbol{u}_1 \in H$. Analogickým způsobem se dokáže, že také $\boldsymbol{u}_2, \ldots, \boldsymbol{u}_k \in H$. To však znamená, že $L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k) \subseteq H$, neboli $U \subseteq H$.

β) Dále, hodnost matice soustavy (4) je zřejmě $n-k$, tzn. podle věty 3.2. je pak

$$\dim H = n - (n-k) = k = \dim U\,.$$

Dokázali jsme tedy, že

$$U \subseteq H \quad \wedge \quad \dim U = \dim H,$$

odkud již podle věty 4.4. 2., kap. I., dostáváme, že $U = H$. ■

Poznámka.
Je třeba si uvědomit, že homogenní soustava, jejíž existenci předchozí věta zaručuje, není zřejmě určena jednoznačně. Dále připomeňme, že obratů uvedených v důkazu předchozí věty se používá při řešení konkrétních příkladů, a je proto nutné algoritmus popsaný v důkazu věty znát.

Příklad 3.2.
Nalezněte soustavu homogenních lineárních rovnic (nad $\mathbb{R}$), jejíž množina řešení je rovna podprostoru U vektorového prostoru $\mathbb{R}^4$, kde U je generován vektory:

$$\boldsymbol{u}_1 = (1,2,1,1), \quad \boldsymbol{u}_2 = (0,1,-1,1), \quad \boldsymbol{u}_3 = (1,3,0,2)\,.$$

Řešení: Nejprve si napíšeme soustavu (3) (přitom není nutné z generátorů podprostoru U předem vybírat bázi U, neboť eventuelní nadbytečné rovnice v (3) během výpočtu stejně vypadnou), pak najdeme bázi jejího podprostoru řešení W a nakonec pak složky vektorů báze W budou vystupovat jako koeficienty v hledané soustavě (4).
Nejprve tedy řešíme soustavu lineárních rovnic:

$$\begin{aligned} x_1 + 2x_2 + x_3 + \ x_4 &= 0 \\ x_2 - x_3 + \ x_4 &= 0 \\ x_1 + 3x_2 \qquad + 2x_4 &= 0 \end{aligned} \quad \Rightarrow \quad \left(\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 0 \\ 0 & 1 & -1 & 1 & 0 \\ 1 & 3 & 0 & 2 & 0 \end{array}\right) \to \cdots \to \left(\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 0 \\ 0 & 1 & -1 & 1 & 0 \end{array}\right),$$

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:

$$\begin{aligned} -3x_1 + x_2 + x_3 &= 0 \\ x_1 - x_2 + x_4 &= 0 \end{aligned}$$

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 $\boldsymbol{u} = (u_1, \ldots, u_n)$ je řešení soustavy (5) a nechť $\boldsymbol{v}' = (v'_1, \ldots, v'_n)$ je řešení k ní zhomogenizované soustavy (6), tzn. platí:

$$\sum_{j=1}^{n} a_{ij}u_j = b_i \qquad \text{a} \qquad \sum_{j=1}^{n} a_{ij}v'_j = 0 \qquad \text{pro } i = 1, \ldots, k.$$

Pak $\boldsymbol{u} + \boldsymbol{v}' = (u_1 + v'_1, \ldots, u_n + v'_n)$ a platí:

$$\sum_{j=1}^{n} a_{ij}(u_j + v'_j) = \sum_{j=1}^{n} a_{ij}u_j + \sum_{j=1}^{n} a_{ij}v'_j = b_i + 0 = b_i \qquad \text{pro } i = 1, \ldots, k,$$

a tedy $\boldsymbol{u} + \boldsymbol{v}'$ je řešením soustavy (5).
2: Nechť $\boldsymbol{u} = (u_1, \ldots, u_n)$, resp. $\boldsymbol{v} = (v_1, \ldots, v_n)$ jsou dvě řešení soustavy (5), tzn. platí:

$$\sum_{j=1}^{n} a_{ij}u_j = b_i \qquad \text{a} \qquad \sum_{j=1}^{n} a_{ij}v_j = b_i \qquad \text{pro } i = 1, \ldots, k.$$

Pak $\boldsymbol{u} - \boldsymbol{v} = (u_1 - v_1, \ldots, u_n - v_n)$ a platí:

$$\sum_{j=1}^{n} a_{ij}(u_j - v_j) \;=\; \sum_{j=1}^{n} a_{ij}u_j \;-\; \sum_{j=1}^{n} a_{ij}v_j \;=\; b_i \;-\; b_i \;=\; 0 \qquad \text{pro } i = 1, \ldots, k,$$

a tedy $\boldsymbol{u} - \boldsymbol{v}$ je řešením zhomogenizované soustavy (6). ■

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.. ■

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, generování, 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 reálných čísel $\mathbb{R}$.

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 každé $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in V$, $r \in \mathbb{R}$ 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 speciálně V euklidovským prostorem, tzn. je to reálný vektorový prostor 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 $\boldsymbol{u} \cdot \boldsymbol{v} = u_1 v_1 + u_2 v_2$,
jsou zřejmě splněny axiomy skalárního součinu a $\mathbb{R}^2$ s tímto skalárním součinem je euklidovským prostorem.

2. Položíme-li $\boldsymbol{u} \cdot \boldsymbol{v} = 4u_1 v_1 + 2u_1 v_2 + 2u_2 v_1 + 3u_2 v_2$,
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, tj. polynomy. Položíme-li

$$\boldsymbol{f} \cdot \boldsymbol{g} \;=\; \int_0^1 f(x) \cdot g(x)\; dx\,,$$

pak rozepsáním (s využitím 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 $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ je pevná báze prostoru V. Pak libovolné vektory $\boldsymbol{u}, \boldsymbol{v} \in V$ lze (jednoznačně) vyjádřit ve tvaru:

$$\boldsymbol{u} \;=\; x_1 \cdot \boldsymbol{e}_1 + \cdots + x_n \cdot \boldsymbol{e}_n \quad \text{resp.} \quad \boldsymbol{v} = y_1 \cdot \boldsymbol{e}_1 + \cdots + y_n \cdot \boldsymbol{e}_n\,.$$

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 technickým rozepsáním se lehce ověří, že jsou splněny axiomy 1. – 4. z definice 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 a nechť $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}, \boldsymbol{u}_i, \boldsymbol{v}_j \in V$, $r, p_i, r_j \in \mathbb{R}$. 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. $\boldsymbol{o} \cdot \boldsymbol{u} \;=\; \boldsymbol{u} \cdot \boldsymbol{o} \;=\; 0$
5. $\boldsymbol{u} \cdot \boldsymbol{u} \;=\; 0 \iff \boldsymbol{u} \;=\; \boldsymbol{o}\,.$

Důkaz.
1 a 2: bezprostředně vyplývá z definice skalárního součinu.
3: dokáže se matematickou indukcí.
4: $\boldsymbol{o} \cdot \boldsymbol{u} = (0 \cdot \boldsymbol{o}) \cdot \boldsymbol{u} = 0 \cdot (\boldsymbol{o} \cdot \boldsymbol{u}) = 0$. Zbytek tvrzení se dokáže analogicky.
5: „$\Rightarrow$“: plyne z axiomu 4 skalárního součinu
„$\Leftarrow$“: plyne z právě dokázané části 4. ∎

Definice.
Nechť V je euklidovský prostor, $\boldsymbol{u} \in V$. Pak nezáporné reálné číslo

$$\sqrt{\boldsymbol{u} \cdot \boldsymbol{u}}$$

se nazývá *velikost vektoru* $\boldsymbol{u}$ a označuje se symbolem $\|\boldsymbol{u}\|$.
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.

Nechť tedy $\boldsymbol{v} \neq \boldsymbol{o}$. 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 $r = \dfrac{\boldsymbol{u} \cdot \boldsymbol{v}}{\boldsymbol{v} \cdot \boldsymbol{v}}$ (což lze, neboť $\boldsymbol{v} \neq \boldsymbol{o}$, a tedy $\boldsymbol{v} \cdot \boldsymbol{v} > 0$), 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 úpravě a sečtení posledních dvou členů a následném vynásobení obou stran nerovnosti (kladným!) číslem $\boldsymbol{v} \cdot \boldsymbol{v}$ 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

$$\boldsymbol{v} = \boldsymbol{o} \qquad \vee \qquad \boldsymbol{u} - r \cdot \boldsymbol{v} = \boldsymbol{o}\,,$$

tzn. právě když vektory $\boldsymbol{u}, \boldsymbol{v}$ jsou lineárně závislé. ■

Poznámka.
Schwarzovu nerovnost (1) často zapisujeme v ekvivalentním tvaru:

$$(\boldsymbol{u} \cdot \boldsymbol{v})^2 \leq \|\boldsymbol{u}\|^2 \cdot \|\boldsymbol{v}\|^2.$$

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. $\|\boldsymbol{u}\| \geq 0$, *přičemž* $\|\boldsymbol{u}\| = 0$ *právě když* $\boldsymbol{u} = \boldsymbol{o}$
2. $\|r \cdot \boldsymbol{u}\| = |r| \cdot \|\boldsymbol{u}\|$
3. $\|\boldsymbol{u} + \boldsymbol{v}\| \leq \|\boldsymbol{u}\| + \|\boldsymbol{v}\|$
4. *je-li* $\boldsymbol{u} \neq \boldsymbol{o}$, *pak* $\dfrac{1}{\|\boldsymbol{u}\|} \cdot \boldsymbol{u}$ *je normovaný vektor.*

Důkaz.
1. a 4. jsou bezprostředními důsledky definice velikosti vektoru.

2: užitím definice velikosti vektoru, úpravou a odmocněním dostáváme:

$$\|r \cdot \boldsymbol{u}\| = \sqrt{(r \cdot \boldsymbol{u}) \cdot (r \cdot \boldsymbol{u})} = \sqrt{r^2 \cdot (\boldsymbol{u} \cdot \boldsymbol{u})} = |r| \cdot \|\boldsymbol{u}\|.$$

3: Z definice velikosti vektoru, rozepsáním a užitím Schwarzovy nerovnosti dostáváme:

$$\|\boldsymbol{u} + \boldsymbol{v}\|^2 = (\boldsymbol{u} + \boldsymbol{v}) \cdot (\boldsymbol{u} + \boldsymbol{v}) = (\boldsymbol{u} \cdot \boldsymbol{u}) + 2 \cdot (\boldsymbol{u} \cdot \boldsymbol{v}) + (\boldsymbol{v} \cdot \boldsymbol{v}) \leq$$

$$\leq (\boldsymbol{u} \cdot \boldsymbol{u}) + 2 \cdot \|\boldsymbol{u}\| \cdot \|\boldsymbol{v}\| + (\boldsymbol{v} \cdot \boldsymbol{v}) = \|\boldsymbol{u}\|^2 + 2 \cdot \|\boldsymbol{u}\| \cdot \|\boldsymbol{v}\| + \|\boldsymbol{v}\|^2 = \big(\|\boldsymbol{u}\| + \|\boldsymbol{v}\|\big)^2.$$

Protože však $\|\boldsymbol{u} + \boldsymbol{v}\|$ i $\big(\|\boldsymbol{u}\| + \|\boldsymbol{v}\|\big)$ jsou nezáporná čísla, dostáváme po odmocnění žádané tvrzení. ■

Poznámka.
1. Nerovnost uvedená ve 3. části věty se obvykle nazývá „trojúhelníková nerovnost“.

2. Použijeme-li obratu provedeného ve 4. části věty (tzn. nenulový vektor $\boldsymbol{u}$ vynásobíme převrácenou hodnotou jeho velikosti), 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:

$$\cos\varphi = \frac{\boldsymbol{u} \cdot \boldsymbol{v}}{\|\boldsymbol{u}\| \cdot \|\boldsymbol{v}\|} \qquad \wedge \qquad 0 \leq \varphi \leq \pi \tag{2}$$

se nazývá *odchylka vektorů* $\boldsymbol{u}, \boldsymbol{v}$.

Poznámka.
Je potřeba si rozmyslet, že uvedená definice odchylky je korektní, tzn. že číslo φ splňující podmínky (2) existuje, a to jediné. Ale užitím pravidel pro počítání s absolutními hodnotami a užitím Schwarzovy nerovnosti dostáváme:

$$\left| \frac{\boldsymbol{u} \cdot \boldsymbol{v}}{\| \boldsymbol{u} \| \cdot \| \boldsymbol{v} \|} \right| = \frac{|\boldsymbol{u} \cdot \boldsymbol{v}|}{\| \boldsymbol{u} \| \cdot \| \boldsymbol{v} \|} \leq 1\,,$$

což znamená, že platí:

$$-1 \leq \frac{\boldsymbol{u} \cdot \boldsymbol{v}}{\| \boldsymbol{u} \| \cdot \| \boldsymbol{v} \|} \leq 1\,.$$

Vidíme tedy (na základě našich znalostí o goniometrických funkcích), že existuje právě jedno reálné číslo φ, splňující podmínky (2).

Zdůrazněme, že v definici odchylky dvou vektorů je podstatný předpoklad, že oba uvažované vektory jsou nenulové! Znamená to, že odchylka dvou vektorů není definována pro případ, kdy některý z těchto vektorů je nulovým vektorem.

§2. Ortogonálnost

Definice.
Nechť V je euklidovský prostor a nechť $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ je konečná posloupnost vektorů z V. Řekneme, že posloupnost vektorů $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ je ortogonální nebo stručně, že *vektory* $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ *jsou ortogonální*, jestliže

$$\text{pro každé } i \neq j \quad \text{je} \quad \boldsymbol{u}_i \cdot \boldsymbol{u}_j = 0\,.$$

Je-li každý z ortogonálních vektorů $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ navíc normovaný, pak říkáme, že *vektory* $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ *jsou ortonormální*.

Jsou-li ortogonální (resp. ortonormální) vektory navíc bází, prostoru V, nazývají se *ortogonální báze* (resp. *ortonormální báze*) prostoru V.

Poznámka.
Rozebereme si definici ortogonálních vektorů $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ pro nejjednodušší hodnoty k.

α) $k = 1$.
Posloupnost sestávající z jednoho vektoru je vždy ortogonální (bez ohledu na to, zda např. daný vektor je nulový či nikoliv). Tento fakt plyne ihned z předchozí definice (rozmyslete si podrobně proč)

β) $k = 2$.
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).

Jsou-li dva vektory $\boldsymbol{u}_1, \boldsymbol{u}_2$ nenulové, pak tyto vektory jsou ortogonální, právě když jejich odchylka je $\frac{\pi}{2}$ (plyne ihned z definice odchylky). Na druhé straně, dva vektory, z nichž alespoň jeden je nulový, jsou vždycky ortogonální, přičemž jejich odchylka samozřejmě není definována.

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 a 2: obě tvrzení ihned plynou 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 $i = 1, \dots, k$. Užitím věty 1.4.3. dostáváme

$$\boldsymbol{u} \cdot \left(\sum_{i=1}^{k} r_i \cdot \boldsymbol{w}_i\right) = \sum_{i=1}^{k} r_i \cdot (\boldsymbol{u} \cdot \boldsymbol{w}_i) = \sum_{i=1}^{k} r_i \cdot 0 = 0\,,$$

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 $\boldsymbol{u} \perp \boldsymbol{w}_i$, pro $i = 1, \dots, k$. ■

Následující důležité tvrzení ukazuje, jaká je vzájemná souvislost mezi ortogonálností vektorů a lineární nezávislostí vektorů.

Věta 2.2.
Nechť $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k \in V$ *jsou nenulové ortogonální vektory v euklidovském prostoru* V*. Potom vektory* $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k \in V$ *jsou lineárně nezávislé.*

Důkaz.
Předpokládáme, že $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k \in V$ jsou nenulové ortogonální vektory a budeme dokazovat, že jsou lineárně nezávislé. Nechť tedy:

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

Provedeme-li (pro libovolné $i = 1, \dots, k$) skalární součin vektoru $\boldsymbol{u}_i$ s oběma stranami této rovnosti, dostaneme:

$$(t_1 \cdot \boldsymbol{u}_1 + \cdots + t_k \cdot \boldsymbol{u}_k) \cdot \boldsymbol{u}_i \; = \; \boldsymbol{o} \cdot \boldsymbol{u}_i,$$

odkud po úpravě, s využitím ortogonálnosti zadaných vektorů dostáváme:

$$t_i \cdot (\boldsymbol{u}_i \cdot \boldsymbol{u}_i) \; = \; 0 \,.$$

Protože podle předpokladu je $\boldsymbol{u}_i \neq \boldsymbol{o}$, je potom $\boldsymbol{u}_i \cdot \boldsymbol{u}_i \neq 0$, a musí tedy být $t_i = 0$ (pro každé $i = 1, \dots, k$). To však znamená, že vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ jsou lineárně nezávislé. ■

Poznámka.
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.

Při úvahách o podprostorech euklidovských prostorů je výhodné pracovat s generátory nebo bázemi které sestávají z ortogonálních vektorů, protože skalární součiny ortogonálních vektorů jsou rovny nule a výpočty se technicky zjednoduší. Následující věta ukáže, jak se takové ortogonální vektory sestrojí. Důkaz věty je konstruktivní a jeho algoritmus se nazývá *Gram-Schmidtův ortogonalizační proces.*

Věta 2.3.
Nechť $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k \in V$ *jsou libovolné vektory z euklidovského prostoru* V*. 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* $L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k) = L(\boldsymbol{e}_1, \dots, \boldsymbol{e}_k)$*.*

Důkaz.
Důkaz provedeme matematickou indukcí vzhledem ke k.

α) nechť $k = 1$.
Položme $\boldsymbol{e}_1 = \boldsymbol{u}_1$. Pak vektor $\boldsymbol{e}_1$ je ortogonální (protože, jak víme, každá posloupnost sestávající z jednoho vektoru je vždy ortogonální) a zřejmě platí, že $L(\boldsymbol{u}_1) = L(\boldsymbol{e}_1)$.

β) Předpokládejme, že tvrzení věty platí pro $1, 2, \dots, k-1$ ($k \geq 2$). Dokážeme nyní tvrzení věty pro k.
Nechť tedy $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ jsou libovolné vektory z V. Vezměme z nich vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_{k-1}$. Podle indukčního předpokladu existují ortogonální vektory $\boldsymbol{e}_1, \dots, \boldsymbol{e}_{k-1}$ tak, že:

$$L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_{k-1}) = L(\boldsymbol{e}_1, \dots, \boldsymbol{e}_{k-1}). \tag{1}$$

Nyní zkonstruujeme vektor $\boldsymbol{e}_k$. Položíme:

$$\boldsymbol{e}_k = p_1 \cdot \boldsymbol{e}_1 + \cdots + p_{k-1} \cdot \boldsymbol{e}_{k-1} + \boldsymbol{u}_k, \tag{2}$$

kde $p_i \in \mathbb{R}$, a určíme koeficienty p_i tak, aby platilo

$$\boldsymbol{e}_k \cdot \boldsymbol{e}_1 = 0 \quad \wedge \quad \boldsymbol{e}_k \cdot \boldsymbol{e}_1 = 0 \quad \wedge \quad \ldots \quad \wedge \quad \boldsymbol{e}_k \cdot \boldsymbol{e}_{k-1} = 0\,.$$

To provedeme tak, že rovnici (2) postupně skalárně vynásobíme vektory $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_{k-1}$. Po provedení skalárního součinu vektoru $\boldsymbol{e}_i$ (pro $i = 1, 2, \ldots, k-1$) s oběma stranami rovnice (2) dostaneme:

$$\boldsymbol{e}_k \cdot \boldsymbol{e}_i \;=\; 0 \;=\; p_i \cdot (\boldsymbol{e}_i \cdot \boldsymbol{e}_i) + (\boldsymbol{u}_k \cdot \boldsymbol{e}_i)$$

(využili jsme přitom předpoklad, že vektory $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_{k-1}$ jsou ortogonální), odkud již lehce vypočítáme koeficienty p_i:

$$p_i = \begin{cases} -\dfrac{\boldsymbol{u}_k \cdot \boldsymbol{e}_i}{\boldsymbol{e}_i \cdot \boldsymbol{e}_i} & \text{je-li } \boldsymbol{e}_i \neq \boldsymbol{o} \\ \text{libovolné} & \text{je-li } \boldsymbol{e}_i = \boldsymbol{o} \end{cases}$$

Dosazením takto získaných hodnot $p_1, \ldots, p_{k-1}$ do rovnice (2) dostaneme vektor e_k. Vektory $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k$ jsou tedy nyní ortogonální.

Zbývá už jen dokázat množinovou rovnost $\quad L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k) = L(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k)\,.$

„$\subseteq$" : stačí dokázat, že $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k \in L(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k)$. Ale z (1) plyne:

$$\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{k-1} \in L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{k-1}) = L(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_{k-1}) \subseteq L(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k)$$

a ze (2) plyne:

$$\boldsymbol{u}_k = p_1 \cdot \boldsymbol{e}_1 + \cdots + p_{k-1} \cdot \boldsymbol{e}_{k-1} - \boldsymbol{e}_k \in L(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k).$$

„$\supseteq$" : stačí dokázat, že $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k \in L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k)$.
Ale z (1) plyne:

$$\boldsymbol{e}_1, \ldots, \boldsymbol{e}_{k-1} \in L(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_{k-1}) = L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{k-1}) \subseteq L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k).$$

Z (1) plyne, že každý z vektorů $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_{k-1}$ je lineární kombinací vektorů $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{k-1}$ a proto pak ze (2) plyne, že

$$\boldsymbol{e}_k \in L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k).$$

Platí tedy: $\quad L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k) = L(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k) \quad$ a celá věta je tak dokázána. ■

Poznámka.
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

$$\dim L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k) = r \ (\leq k), \ \text{ pak je samozřejmě také } \dim L(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k) = r\,,$$

což znamená (vzhledem k tomu, že vektory $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k$ jsou ortogonální), že právě $(k - r)$ z vektorů $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k$ musí být nulových. Zbývajících r vektorů je pak nenulových a tvoří ortogonální bázi podprostoru $L(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k)$.

Specielně, jsou-li výchozí 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 U 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 $U = L(\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3)$. Potom: $\boldsymbol{e}_1 = \boldsymbol{u}_1 = (0, 1, 2, 1)$.

Položíme $\boldsymbol{e}_2 = p \cdot \boldsymbol{e}_1 + \boldsymbol{u}_2$ a spočítáme koeficient p. Pak

$$\boldsymbol{e}_2 \cdot \boldsymbol{e}_1 \;=\; 0 \;=\; p \cdot \boldsymbol{e}_1 \cdot \boldsymbol{e}_1 + \boldsymbol{u}_2 \cdot \boldsymbol{e}_1 \;\Rightarrow\; p = -\tfrac{\boldsymbol{u}_2 \cdot \boldsymbol{e}_1}{\boldsymbol{e}_1 \cdot \boldsymbol{e}_1} = -\tfrac{2}{3}\,.$$

Tedy $\boldsymbol{e}_2 \;=\; -\frac{2}{3} \cdot \boldsymbol{e}_1 + \boldsymbol{u}_2 \;=\; (-1, \frac{1}{3}, -\frac{1}{3}, \frac{1}{3})\,.$

Položíme $\boldsymbol{e}_3 = p_1 \cdot \boldsymbol{e}_1 + p_2 \cdot \boldsymbol{e}_2 + \boldsymbol{u}_3$ a spočítáme koeficienty p_1 a p_2. Pak

$$\boldsymbol{e}_3 \cdot \boldsymbol{e}_1 \;=\; 0 \;=\; p_1 \cdot \boldsymbol{e}_1 \cdot \boldsymbol{e}_1 + p_2 \cdot \boldsymbol{e}_2 \cdot \boldsymbol{e}_1 + \boldsymbol{u}_3 \cdot \boldsymbol{e}_1 \;\Rightarrow\; p_1 = -\tfrac{\boldsymbol{u}_3 \cdot \boldsymbol{e}_1}{\boldsymbol{e}_1 \cdot \boldsymbol{e}_1} = -\tfrac{1}{3}\,.$$

$$\boldsymbol{e}_3 \cdot \boldsymbol{e}_2 \;=\; 0 \;=\; p_1 \cdot \boldsymbol{e}_1 \cdot \boldsymbol{e}_2 + p_2 \cdot \boldsymbol{e}_2 \cdot \boldsymbol{e}_2 + \boldsymbol{u}_3 \cdot \boldsymbol{e}_2 \;\Rightarrow\; p_2 = -\tfrac{\boldsymbol{u}_3 \cdot \boldsymbol{e}_2}{\boldsymbol{e}_2 \cdot \boldsymbol{e}_2} = 1\,.$$

Tedy $\boldsymbol{e}_3 = -\frac{1}{3} \cdot \boldsymbol{e}_1 + 1 \cdot \boldsymbol{e}_2 + \boldsymbol{u}_3 = (0, 0, 0, 0) = \boldsymbol{o}$.

Výsledek: ortogonální bázi podprostoru U tvoří například vektory $\boldsymbol{e}_1, \boldsymbol{e}_2$.

Definice.
Nechť A, B jsou libovolné podmnožiny euklidovského prostoru V. Je-li:

$$\boldsymbol{a} \cdot \boldsymbol{b} = 0 \qquad \text{pro každé } \boldsymbol{a} \in A\,,\ \boldsymbol{b} \in B\,,$$

pak říkáme, že A, B jsou *ortogonální množiny* a píšeme $A \perp B$ nebo též $B \perp A$.

Poznámka.
Řečeno jinými slovy, A, B jsou ortogonální množiny, právě když pro každé $\boldsymbol{a} \in A$, $\boldsymbol{b} \in B$ jsou vektory $\boldsymbol{a}, \boldsymbol{b}$ ortogonální.

Ve specielních případech dostáváme: prázdná množina a množina $\{\boldsymbol{o}\}$ jsou zřejmě ortogonální ke každé podmnožině ve V. Dále z definice bezprostředně plyne, že:

$$A \perp B \qquad \Longrightarrow \qquad A \cap B = \emptyset \;\vee\; A \cap B = \{\boldsymbol{o}\}\,.$$

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:

$$A \perp B \quad \Longleftrightarrow \quad [A] \perp [B]\,,$$

tzn. dvě množiny jsou ortogonální, právě když jsou ortogonální podprostory generované těmito množinami.

Důkaz.
„$\Leftarrow$“: Plyne z předchozí definice, uvědomíme-li si, že $A \subseteq [A]$ a $B \subseteq [B]$.

„$\Rightarrow$“: Předpokládejme, že $A \perp B$. Nechť dále $\boldsymbol{u} \in [A]$, $\boldsymbol{v} \in [B]$.
Podprostor $[A]$ je roven množině všech lineárních kombinací konečně mnoha vektorů z A. Tento fakt se dokáže analogickým způsobem, jako jsme dokazovali větu 2.3., kapitoly I. (proveďte si podrobně sami!). Podobně, podprostor $[B]$ je roven množině všech lineárních kombinací konečně mnoha vektorů z B. Je tedy:

$$\boldsymbol{u} = p_1 \cdot \boldsymbol{a}_1 + \cdots + p_k \cdot \boldsymbol{a}_k\,, \ \text{kde } \boldsymbol{a}_i \in A \quad \text{a} \quad \boldsymbol{v} = r_1 \cdot \boldsymbol{b}_1 + \cdots + r_m \cdot \boldsymbol{b}_m\,, \ \text{kde } \boldsymbol{b}_j \in B\,.$$

Potom však:

$$\boldsymbol{u} \cdot \boldsymbol{v} \;=\; \left(\sum_{i=1}^{k} p_i \cdot \boldsymbol{a}_i\right) \cdot \left(\sum_{j=1}^{m} r_j \cdot \boldsymbol{b}_j\right) \;=\; \sum_{i=1}^{k}\sum_{j=1}^{m} p_i r_j \cdot (\boldsymbol{a}_i \cdot \boldsymbol{b}_j) \;=\; 0,$$

protože $\boldsymbol{a}_i \cdot \boldsymbol{b}_j = 0$. Tedy platí $[A] \perp [B]$, což jsme měli dokázat. ■

Definice.
Nechť U je podprostor euklidovského prostoru V. Pak množina:

$$U^{\perp} = \{\boldsymbol{x} \in V \mid \boldsymbol{x} \cdot \boldsymbol{u} = 0 \text{ pro každé } \boldsymbol{u} \in U\}$$

se nazývá *ortogonální doplněk podprostoru* U (ve V).

Poznámka.
Zřejmě platí, že $U \perp U^{\perp}$, tzn. množiny U a $U^{\perp}$ jsou ortogonální. Ve speciálních případech přímo z definice ortogonálního doplňku dostáváme, že

$$V^{\perp} = \{\boldsymbol{o}\} \qquad \text{a} \qquad \{\boldsymbol{o}\}^{\perp} = V\,.$$

Základní vlastnosti ortogonálních doplňků podprostorů v euklidovském prostoru popisují následující dvě věty.

Věta 2.6.
Nechť U je podprostor euklidovského prostoru V. Pak platí:

1. $U^{\perp}$ *je podprostor ve* V
2. $V = U \dot{+} U^{\perp}$, *tzn. celý prostor V je přímým součtem podprostorů U a $U^{\perp}$.*

Důkaz.
1: Zřejmě $\boldsymbol{o} \in U^{\perp}$, a tedy $U^{\perp} \neq \emptyset$. Nechť $\boldsymbol{x}, \boldsymbol{y} \in U^{\perp}$, $r \in \mathbb{R}$. Dokážeme, že $\boldsymbol{x} + \boldsymbol{y} \in U^{\perp}$ a $r \cdot \boldsymbol{x} \in U^{\perp}$.
Nechť tedy $\boldsymbol{u}$ je libovolný vektor z podprostoru U. Pak:

$$(\boldsymbol{x} + \boldsymbol{y}) \cdot \boldsymbol{u} = (\boldsymbol{x} \cdot \boldsymbol{u}) + (\boldsymbol{y} \cdot \boldsymbol{u}) = 0 + 0 = 0 \qquad \text{a} \qquad (r \cdot \boldsymbol{x}) \cdot \boldsymbol{u} = r \cdot (\boldsymbol{x} \cdot \boldsymbol{u}) = r \cdot 0 = 0\,,$$

což znamená, že $\boldsymbol{x} + \boldsymbol{y} \in U^{\perp}$ a $r \cdot \boldsymbol{x} \in U^{\perp}$. Tedy $U^{\perp}$ je podprostor ve V.

2: Je-li $U = \{\boldsymbol{o}\}$, pak $U^{\perp} = V$ a tvrzení platí. Nechť tedy $U \neq \{\boldsymbol{o}\}$ a nechť $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k$ je ortonormální báze U (její existence je zaručena větou 2.4.).

a) Dokážeme, že $U + U^{\perp} = V$.

Inkluze „$\subseteq$“ je zřejmá. Budeme dokazovat inkluzi „$\supseteq$“. Nechť tedy $\boldsymbol{v} \in V$. Označme:

$$\boldsymbol{x} = (\boldsymbol{v} \cdot \boldsymbol{e}_1) \cdot \boldsymbol{e}_1 + \cdots + (\boldsymbol{v} \cdot \boldsymbol{e}_k) \cdot \boldsymbol{e}_k.$$

Pak zřejmě $\boldsymbol{x} \in U$. Dále vezměme vektor $(-\boldsymbol{x} + \boldsymbol{v})$ a pro libovolné $i = 1, \dots, k$ spočtěme skalární součin $(-\boldsymbol{x} + \boldsymbol{v}) \cdot \boldsymbol{e}_i$. Užitím předchozího vztahu dostaneme:

$$(-\boldsymbol{x} + \boldsymbol{v}) \cdot \boldsymbol{e}_i = -(\boldsymbol{x} \cdot \boldsymbol{e}_i) + (\boldsymbol{v} \cdot \boldsymbol{e}_i) = -(\boldsymbol{v} \cdot \boldsymbol{e}_i) + (\boldsymbol{v} \cdot \boldsymbol{e}_i) = 0\,.$$

Potom však je $(-\boldsymbol{x} + \boldsymbol{v}) \in U^\perp$ (proč?), odkud dostáváme, že $\boldsymbol{v} = \boldsymbol{x} + (-\boldsymbol{x} + \boldsymbol{v}) \in U + U^\perp$.

b) Dokážeme, že $U \cap U^\perp = \{\boldsymbol{o}\}$.

Inkluze „$\supseteq$“ je zřejmá a budeme tedy dokazovat pouze inkluzi opačnou.

Nechť $\boldsymbol{v} \in U \cap U^\perp$. Pak je $\boldsymbol{v} \in U$ a $\boldsymbol{v} \in U^\perp$, a tedy $\boldsymbol{v} \cdot \boldsymbol{v} = 0$. To však znamená (podle věty 1.2. 5.), že je $\boldsymbol{v} = \boldsymbol{o}$.

Dohromady pak z a) a b) plyne, že $V = U \dotplus U^\perp$. ■

Věta 2.7.
Nechť U, S jsou podprostory euklidovského prostoru V. Pak platí:

1. $(U^\perp)^\perp = U$
2. $(U + S)^\perp = U^\perp \cap S^\perp$
3. $(U \cap S)^\perp = U^\perp + S^\perp$.

Důkaz.
1: Podle věty 2.6. je $U \dotplus U^\perp = V$ a také $U^\perp \dotplus (U^\perp)^\perp = V$, odkud plyne (užitím věty o dimenzi součtu a průniku podprostorů), že

$$\dim U = \dim V - \dim U^\perp \quad \text{a také} \quad \dim (U^\perp)^\perp = \dim V - \dim U^\perp\,.$$

Tedy dimenze podprostorů U a $(U^\perp)^\perp$ se rovnají a dále zřejmě platí, že $U \subseteq (U^\perp)^\perp$. Potom (podle věty 4.4. 2., kapitoly I.) je $U = (U^\perp)^\perp$.

2: Inkluze „$\subseteq$“ je zřejmá.

Dokážeme inkluzi „$\supseteq$“. Nechť $\boldsymbol{x} \in U^\perp \cap S^\perp$ a nechť $\boldsymbol{v} \in (U+S)$ je libovolný, tzn. $\boldsymbol{v} = \boldsymbol{u} + \boldsymbol{s}$, kde $\boldsymbol{u} \in U$, $\boldsymbol{s} \in S$. Potom:

$$\boldsymbol{x} \cdot \boldsymbol{v} = \boldsymbol{x} \cdot (\boldsymbol{u} + \boldsymbol{s}) = \boldsymbol{x} \cdot \boldsymbol{u} + \boldsymbol{x} \cdot \boldsymbol{s} = 0 + 0 = 0,$$

a tedy je $\boldsymbol{x} \in (U + S)^\perp$. Je tedy $U^\perp \cap S^\perp \subseteq (U + S)^\perp$ a dohromady platí žádaná rovnost.

3: Užitím 1 a 2 dostáváme:

$$(U \cap S) = (U^\perp)^\perp \cap (S^\perp)^\perp = (U^\perp + S^\perp)^\perp,$$

odkud plyne:

$$(U \cap S)^\perp = \left((U^\perp + S^\perp)^\perp\right)^\perp = U^\perp + S^\perp\,,$$

což je požadované tvrzení. ■

Definice.
Nechť U je podprostor ve V a nechť vektor $\boldsymbol{v} \in V$ je vyjádřen ve tvaru:

$$\boldsymbol{v} = \boldsymbol{x} + \boldsymbol{y} \qquad \text{kde } \boldsymbol{x} \in U, \quad \boldsymbol{y} \in U^\perp.$$

Pak vektor $\boldsymbol{x}$ se nazývá *ortogonální projekce vektoru $\boldsymbol{v}$ do podprostoru U* .

Poznámka.
Uvědomme si, že předchozí definice je korektní, protože podle 2. části předchozí věty se libovolný vektor $\boldsymbol{v} \in V$ dá napsat ve výše uvedeném tvaru, a to jediným způsobem. Tedy ortogonální projekce vektoru $\boldsymbol{v}$ do podprostoru U je vždy jednoznačně určena.

Věta 2.8.
Nechť U je podprostor euklidovského prostoru V. Nechť $\boldsymbol{x}$ je ortogonální projekce vektoru $\boldsymbol{v}$ do podprostoru U, nechť $\boldsymbol{x}'$ je ortogonální projekce vektoru $\boldsymbol{v}'$ do podprostoru U a nechť $r \in \mathbb{R}$ libovolné. Pak platí:

1. $(\boldsymbol{x} + \boldsymbol{x}')$ *je ortogonální projekce vektoru* $(\boldsymbol{v} + \boldsymbol{v}')$ *do* U
2. $r \cdot \boldsymbol{x}$ *je ortogonální projekce vektoru* $r \cdot \boldsymbol{v}$ *do* U.

Důkaz.
Obě tvrzení věty dostaneme bezprostředním technickým rozepsáním z definice ortogonální projekce (proveďte si podrobně sami). ■

Příklad 2.2.
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 projekci vektoru $\boldsymbol{v} = (4, -1, -3, 4)$ do podprostoru U generovaného vektory $\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3$. Přitom: $\boldsymbol{u}_1 = (1, 1, 1, 1)$, $\boldsymbol{u}_2 = (1, 0, 0, 3)$, $\boldsymbol{u}_3 = (1, 2, 2, -1)$.

Řešení: Je-li podprostor zadán pomocí generátorů, pak je dobré nejprve zkusit z generátorů vybrat bázi. Pokud zadané generátory bázi tvoří, pak je tento výpočet sice vlastně zbytečný, ale pokud generátory bázi netvoří, pak se celý další výpočet technicky velmi zjednoduší a zkrátí. Hledejme tedy bázi podprostoru U.

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 3 \\ 1 & 2 & 2 & -1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & -2 \\ 0 & -1 & -1 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & -2 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Vidíme, že $\dim U = 2$, tzn. bází podprostoru U jsou například vektory $\boldsymbol{u}_1, \boldsymbol{u}_2$.

Vektor $\boldsymbol{v}$ lze jednoznačně vyjádřit ve tvaru

$$\boldsymbol{v} = \boldsymbol{x} + \boldsymbol{y}, \qquad \text{kde } \boldsymbol{x} \in U, \ \boldsymbol{y} \in U^{\perp}.$$

Protože $\boldsymbol{x} \in U$, lze psát $\boldsymbol{x} = t_1 \cdot \boldsymbol{u}_1 + t_2 \cdot \boldsymbol{u}_2$, odkud po dosazení dostáváme:

$$\boldsymbol{v} \ = \ t_1 \cdot \boldsymbol{u}_1 \ + \ t_2 \cdot \boldsymbol{u}_2 \ + \ \boldsymbol{y}.$$

Poslední rovnici nyní skalárně vynásobíme nejprve vektorem $\boldsymbol{u}_1$ a potom vektorem $\boldsymbol{u}_2$ (využijeme přitom faktu, že $\boldsymbol{u}_1 \cdot \boldsymbol{y} = 0$ a $\boldsymbol{u}_2 \cdot \boldsymbol{y} = 0$). Dostáváme tak soustavu dvou lineárních rovnic o dvou neznámých t_1, t_2 tvaru:

$$\begin{array}{l} \boldsymbol{v}\cdot\boldsymbol{u}_1 \ = \ t_1 \cdot \boldsymbol{u}_1\cdot\boldsymbol{u}_1 \ + \ t_2 \cdot \boldsymbol{u}_2\cdot\boldsymbol{u}_1 \ + \ 0 \\ \boldsymbol{v}\cdot\boldsymbol{u}_2 \ = \ t_1 \cdot \boldsymbol{u}_1\cdot\boldsymbol{u}_2 \ + \ t_2 \cdot \boldsymbol{u}_2\cdot\boldsymbol{u}_2 \ + \ 0 \end{array} \qquad \Longrightarrow \qquad \begin{array}{rcr} 4\,t_1 + \ \ 4\,t_2 & = & 4 \\ 4\,t_1 + 10\,t_2 & = & 16 \end{array}$$

odkud po jednoduchém výpočtu vychází, že $t_1 = -1$, $t_2 = 2$. Tedy

$$\boldsymbol{x} \ = \ (-1) \cdot \boldsymbol{u}_1 \ + \ 2 \cdot \boldsymbol{u}_2 \ = \ (1, -1, -1, 5)$$

je hledaná ortogonální projekce vektoru $\boldsymbol{v}$ do podprostoru U.

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 nad číselným tělesem). 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 strukturu“ daných vektorových prostorů, 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 pro každé $\boldsymbol{u}, \boldsymbol{v} \in V$, $t \in T$ vztahy:

1. $\varphi(\boldsymbol{u} + \boldsymbol{v}) = \varphi(\boldsymbol{u}) + \varphi(\boldsymbol{v})$
2. $\varphi(t \cdot \boldsymbol{u}) = t \cdot \varphi(\boldsymbol{u})$

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. symbolem $\cdot$). Nebude moci dojít k nedorozumění, poněvadž ze souvislosti a z ostatní symboliky bude vždy zřejmé, co který symbol znamená. Pro ulehčení orientace budeme vektory z V' obvykle označovat čárkovaně, kdežto vektory z V nečárkovaně. Speciálně tedy symbol $\boldsymbol{o}'$ 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 pouze jedinou podmínku 3.

Matematickou indukcí lze zřejmě platnost podmínky 3 rozšířit na libovolný konečný počet sčítanců. Je-li tedy φ lineární zobrazení, pak pro $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k \in V$ a $t_1, \ldots t_k \in T$ 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:

$$\varphi(\boldsymbol{u}) = t \cdot \boldsymbol{u} \qquad \text{pro každé } \boldsymbol{u} \in V$$

je lineární zobrazení. Je-li $t \neq 0$, pak φ je dokonce izomorfismus (ověřte si rozepsáním!). Speciálně, pro $t = 1$ dostáváme identické zobrazení id_V, které je tedy izomorfismem vektorového prostoru V na V.
2. Zobrazení $\omega : V \to V'$ definované:

$$\omega(\boldsymbol{u}) = \boldsymbol{o}' \qquad \text{pro každé } \boldsymbol{u} \in V$$

je lineární zobrazení, které budeme nazývat *nulové lineární zobrazení.*

Příklad 1.2.
Zobrazení $\varphi : \mathbb{R}^3 \to \mathbb{R}^2$ definované:

$$\varphi\big((x_1, x_2, x_3)\big) = (2x_1 + x_3, x_1 - x_2 - x_3) \qquad \text{pro } \forall\ (x_1, x_2, x_3) \in \mathbb{R}^3$$

je lineární zobrazení, které není izomorfismem.
Dále, například zobrazení $\psi : \mathbb{R}^3 \to \mathbb{R}^2$ definované:

$$\psi\big((x_1, x_2, x_3)\big) = (2x_1 + 1, x_1 - x_2 - x_3) \qquad \text{pro } \forall\ (x_1, x_2, x_3) \in \mathbb{R}^3$$

není lineární zobrazení (ověřte si sami, že neplatí žádná z podmínek 1 , 2 z definice lineárního zobrazení).

Příklad 1.3.
Zobrazení $\delta : \mathbb{R}_n[x] \to \mathbb{R}_n[x]$ definované:

$$\delta\big(f(x)\big) = f'(x) \qquad \text{pro } \forall\ f(x) \in \mathbb{R}_n[x],$$

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). Zobrazení δ není bijektivní (proč?), a tedy není izomorfismem.

Následující tři věty uvedou další početní pravidla pro lineární zobrazení a ukáží, jak se lineární zobrazení chová vůči základním pojmům a vlastnostem vektorových prostorů (tzn. lineární závislosti vektorů, resp. podprostorům, jejich generování a dimenzi, resp. skládání lineárních zobrazení a izomorfizmu).

Věta 1.1.
Nechť $\varphi : V \to V'$ je lineární zobrazení. Pak platí:

1. $\varphi(\boldsymbol{o}) = \boldsymbol{o}'$, *tj. nulový vektor se vždy musí zobrazit na nulový vektor*
2. $\varphi(-\boldsymbol{u}) = -\varphi(\boldsymbol{u})$ *pro* $\forall \boldsymbol{u} \in V$
3. $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k \in V$ *jsou lineárně závislé vektory* $\implies$ $\varphi(\boldsymbol{u}_1), \ldots, \varphi(\boldsymbol{u}_k)$ *jsou lineárně závislé vektory (ve V').*

Důkaz.
1: zřejmě je $\boldsymbol{o} = 0 \cdot \boldsymbol{o}$, tzn. pak (užitím definice lineárního zobrazení a toho, že násobením nulou dostaneme vždy nulový vektor):

$$\varphi(\boldsymbol{o}) \;=\; \varphi(0 \cdot \boldsymbol{o}) \;=\; 0 \cdot \varphi(\boldsymbol{o}) \;=\; \boldsymbol{o}' .$$

2: užitím definice lineárního zobrazení a věty 1.1.4., kapitoly I dostáváme:

$$\varphi(-\boldsymbol{u}) \;=\; \varphi\big((-1) \cdot \boldsymbol{u}\big) \;=\; (-1) \cdot \varphi(\boldsymbol{u}) \;=\; -\varphi(\boldsymbol{u}) .$$

3: nechť $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ jsou lineárně závislé vektory. Potom existují čísla $t_1, \ldots, t_n \in T$, z nichž alespoň jedno je různé od nuly, tak, že platí:

$$t_1 \cdot \boldsymbol{u}_1 + \cdots + t_k \cdot \boldsymbol{u}_k \;=\; \boldsymbol{o} .$$

Pak $\varphi(t_1 \cdot \boldsymbol{u}_1 + \cdots + t_k \cdot \boldsymbol{u}_k) = \varphi(\boldsymbol{o})$, odkud užitím definice lineárního zobrazení a právě dokázané části 1. dostáváme:

$$t_1 \cdot \varphi(\boldsymbol{u}_1) + \cdots + t_k \cdot \varphi(\boldsymbol{u}_k) = \boldsymbol{o}' ,$$

což znamená (vzhledem k tomu, že alespoň jedno z čísel $t_1, \ldots, t_n \in T$ je různé od nuly), že vektory $\varphi(\boldsymbol{u}_1), \ldots, \varphi(\boldsymbol{u}_k)$ jsou lineárně závislé. ■

Všimněme si toho, že předchozí věta nic neříká o tom, jak se lineární zobrazení chová k lineárně nezávislým vektorům. Je to proto, že lineární zobrazení může lineárně nezávislé vektory někdy zobrazit na lineárně nezávislé vektory a jindy na lineárně závislé vektory (rozmyslete si sami příslušné příklady).

Další věta se zabývá otázkou, jak se lineární zobrazení chová vůči podprostorům. Připomeňme v této souvislosti dřívější úmluvu, že je-li $\varphi : V \to V'$ zobrazení a A je jakákoliv neprázdná podmnožina ve V, pak symbolem $\varphi(A)$ označujeme množinu obrazů všech prvků z A, tj.:

$$\varphi(A) = \{\boldsymbol{x}' \in V' \mid \exists\, \boldsymbol{u} \in A \text{ tak, že } \varphi(\boldsymbol{u}) = \boldsymbol{x}'\}.$$

Věta 1.2.
Nechť $\varphi : V \to V'$ je lineární zobrazení a nechť U je podprostor ve V. Pak:

1. *$\varphi(U)$ je podprostor ve V'*
2. *$\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ jsou generátory podprostoru U $\implies$ $\varphi(\boldsymbol{u}_1), \ldots, \varphi(\boldsymbol{u}_k)$ jsou generátory podprostoru $\varphi(U)$*
3. $\dim \varphi(U) \;\leq\; \dim U$.

Důkaz.
1: dokáže se přímým ověřením definice podprostoru (proveďte si sami).

2: nechť $\boldsymbol{x}' \in \varphi(U)$ je libovolný. Pak existuje $\boldsymbol{u} \in U$ tak, že $\boldsymbol{x}' = \varphi(\boldsymbol{u})$. Podle předpokladu je však $\boldsymbol{u} = t_1 \cdot \boldsymbol{u}_1 + \cdots + t_k \cdot \boldsymbol{u}_k$, a tedy

$$\boldsymbol{x}' \;=\; \varphi(\boldsymbol{u}) \;=\; \varphi(t_1 \cdot \boldsymbol{u}_1 + \cdots + t_k \cdot \boldsymbol{u}_k) \;=\; t_1 \cdot \varphi(\boldsymbol{u}_1) + \cdots + t_k \cdot \varphi(\boldsymbol{u}_k) ,$$

odkud plyne, že vektory $\varphi(\boldsymbol{u}_1), \ldots, \varphi(\boldsymbol{u}_k)$ jsou generátory podprostoru $\varphi(U)$.

3: je-li $U = \{\boldsymbol{o}\}$, pak $\varphi(U) = \{\boldsymbol{o}'\}$ a tvrzení zřejmě platí.
Nechť tedy $U \neq \{\boldsymbol{o}\}$ a nechť $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ je báze podprostoru U. Pak podle části 2 jsou vektory $\varphi(\boldsymbol{u}_1), \ldots, \varphi(\boldsymbol{u}_k)$ generátory podprostoru $\varphi(U)$, a tedy platí (proč?), že $\dim \varphi(U) \;\leq\; k \;=\; \dim U$. ■

Věta 1.3.

1. *složení dvou lineárních zobrazení je opět lineárním zobrazením*
2. *inverzní zobrazení k izomorfizmu je opět izomorfizmem.*

Důkaz.
1: Nechť $\varphi : V \to V'$, $\psi : V' \to V''$ jsou lineární zobrazení. Ověříme, že složené zobrazení $(\psi \circ \varphi)$ splňuje definici lineárního zobrazení. Nechť tedy $\boldsymbol{u}, \boldsymbol{v} \in V$, $t \in T$. Pak:

$$(\psi\circ\varphi)(\boldsymbol{u}+\boldsymbol{v})=\psi(\varphi(\boldsymbol{u}+\boldsymbol{v}))=\psi(\varphi(\boldsymbol{u})+\varphi(\boldsymbol{v}))=\psi(\varphi(\boldsymbol{u}))+\psi(\varphi(\boldsymbol{v}))=(\psi\circ\varphi)(\boldsymbol{u})+(\psi\circ\varphi)(\boldsymbol{v})$$

$$(\psi \circ \varphi)(t \cdot \boldsymbol{u}) = \psi\,(\varphi(t \cdot \boldsymbol{u})) = \psi\,(t \cdot \varphi(\boldsymbol{u})) = t \cdot (\psi(\varphi(\boldsymbol{u})) = t \cdot ((\psi \circ \varphi)(\boldsymbol{u})),$$

a tedy $(\psi \circ \varphi)$ je lineární zobrazení.

2: Nechť $\varphi : V \to V'$ je izomorfizmus. Vzhledem k tomu, že zobrazení φ je bijektivní, existuje k němu inverzní zobrazení $\varphi^{-1} : V' \to V$, které je (jak víme) také bijektivní. Zbývá tedy dokázat, že zobrazení φ^{-1} je lineárním zobrazením.

Nechť tedy $\boldsymbol{u}', \boldsymbol{v}' \in V'$, $t \in T$. Označme $\varphi^{-1}(\boldsymbol{u}') = \boldsymbol{u}$, $\varphi^{-1}(\boldsymbol{v}') = \boldsymbol{v}$. Potom z definice inverzního zobrazení φ^{-1} plyne, že $\varphi(\boldsymbol{u}) = \boldsymbol{u}'$, $\varphi(\boldsymbol{v}) = \boldsymbol{v}'$ a platí

$$\varphi(\boldsymbol{u} + \boldsymbol{v}) = \varphi(\boldsymbol{u}) + \varphi(\boldsymbol{v}) = \boldsymbol{u}' + \boldsymbol{v}' \quad \text{a tedy} \quad \varphi^{-1}(\boldsymbol{u}' + \boldsymbol{v}') = \boldsymbol{u} + \boldsymbol{v} = \varphi^{-1}(\boldsymbol{u}') + \varphi^{-1}(\boldsymbol{v}')$$

$$\varphi(t \cdot \boldsymbol{u}) = t \cdot \varphi(\boldsymbol{u}) = t \cdot \boldsymbol{u}' \quad \text{a tedy} \quad \varphi^{-1}(t \cdot \boldsymbol{u}') = t \cdot \boldsymbol{u} = t \cdot \varphi^{-1}(\boldsymbol{u}')\,.$$

Dokázali jsme tak, že φ^{-1} je izomorfizmus. ■

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 se ale takovýto výsledek dá celkem očekávat, pokud si uvědomíme, že každý vektor z V je jistou, jednoznačně určenou 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 $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ je báze prostoru V a nechť $\boldsymbol{v}'_1, \dots, \boldsymbol{v}'_n$ jsou libovolné vektory z V'.
Pak existuje jediné lineární zobrazení $\varphi : V \to V'$ takové, že

$$\varphi(\boldsymbol{u}_1) \;=\; \boldsymbol{v}'_1\;,\;\;\ldots\ldots\;\;,\;\varphi(\boldsymbol{u}_n) \;=\; \boldsymbol{v}'_n\,.$$

Důkaz.
Větu dokážeme postupně ve dvou krocích, a to tak, že nejprve dokážeme (a to konstruktivně) existenci hledaného lineárního zobrazení φ a potom dokážeme jednoznačnost tohoto zobrazení.

I. *důkaz existence lineárního zobrazení φ.*
Nechť $\boldsymbol{x} \in V$ je libovolný vektor, 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', pro které zřejmě platí (rozmyslete si podrobně proč), že $\varphi(\boldsymbol{u}_1) = \boldsymbol{v}'_1$, ... , $\varphi(\boldsymbol{u}_n) = \boldsymbol{v}'_n$. Zbývá tedy dokázat, že φ je lineárním zobrazením.

Nechť tedy $\boldsymbol{x}, \boldsymbol{y} \in V$, $t \in T$, přičemž:

$$\boldsymbol{x} = x_1 \cdot \boldsymbol{u}_1 + \cdots + x_n \cdot \boldsymbol{u}_n\,, \qquad\qquad \boldsymbol{y} = y_1 \cdot \boldsymbol{u}_1 + \cdots + y_n \cdot \boldsymbol{u}_n\,.$$

Potom :

$$\boldsymbol{x}+\boldsymbol{y} \;=\; (x_1+y_1)\cdot\boldsymbol{u}_1+\cdots+(x_n+y_n)\cdot\boldsymbol{u}_n\,, \qquad t\cdot\boldsymbol{x} \;=\; (tx_1)\cdot\boldsymbol{u}_1+\cdots+(tx_n)\boldsymbol{u}_n\,.$$

Podle definice zobrazení φ a po úpravě pak dostáváme, že

$$\varphi(\boldsymbol{x}+\boldsymbol{y}) \;=\; (x_1+y_1)\cdot\boldsymbol{v}'_1+\cdots+(x_n+y_n)\cdot\boldsymbol{v}'_n \;=$$

$$=\; (x_1\cdot\boldsymbol{v}'_1+\cdots+x_n\cdot\boldsymbol{v}'_n) \;+\; (y_1\cdot\boldsymbol{v}'_1+\cdots+y_n\cdot\boldsymbol{v}'_n) \;=\; \varphi(\boldsymbol{x})+\varphi(\boldsymbol{y})\,,$$

a podobným způsobem dostáváme, že

$$\varphi(t\cdot\boldsymbol{x}) \;=\; (tx_1)\cdot\boldsymbol{v}'_1+\cdots+(tx_n)\cdot\boldsymbol{v}'_n \;=\; t\cdot(x_1\cdot\boldsymbol{v}'_1+\cdots+x_n\cdot\boldsymbol{v}'_n) \;=\; t\cdot\varphi(\boldsymbol{x})\,.$$

Dokázali jsme tedy, že φ je lineární zobrazení s požadovanými vlastnostmi.

II. *důkaz jednoznačnosti lineárního zobrazení* φ.
Nechť φ je výše zkonstruované lineární zobrazení a nechť dále $\psi : V \to V'$ je lineární zobrazení takové, že $\psi(\boldsymbol{u}_1) = \boldsymbol{v}'_1,\ \ldots,\ \psi(\boldsymbol{u}_n) = \boldsymbol{v}'_n$. Budeme dokazovat, že je $\psi = \varphi$. K tomu zřejmě stačí dokázat, pro libovolné $\boldsymbol{x} \in V$ platí $\psi(\boldsymbol{x}) = \varphi(\boldsymbol{x})$.

Nechť tedy $\boldsymbol{x} \in V$ přičemž je $\boldsymbol{x} = x_1\cdot\boldsymbol{u}_1+\cdots+x_n\cdot\boldsymbol{u}_n$. Potom :

$$\psi(\boldsymbol{x}) = \psi(x_1\cdot\boldsymbol{u}_1+\cdots+x_n\cdot\boldsymbol{u}_n) = x_1\cdot\psi(\boldsymbol{u}_1)+\cdots+x_n\cdot\psi(\boldsymbol{u}_n) = x_1\cdot\boldsymbol{v}'_1+\cdots+x_n\cdot\boldsymbol{v}'_n = \varphi(\boldsymbol{x})\,.$$

Dokázali jsme tak, že zobrazení φ je určeno jednoznačně. ■

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 dokonce podprostory a popíší jejich základní vlastnosti.

Věta 1.5.
Nechť $\varphi : V \to V'$ je lineární zobrazení. Pak platí :

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 platí :

$$\varphi(\boldsymbol{u}+\boldsymbol{v}) = \varphi(\boldsymbol{u})+\varphi(\boldsymbol{v}) = \boldsymbol{o}'+\boldsymbol{o}' = \boldsymbol{o}'\,,$$

což znamená, že $\boldsymbol{u}+\boldsymbol{v} \in \operatorname{Ker}\varphi$.
Podobně se dokáže, že pro $\boldsymbol{u} \in \operatorname{Ker}\varphi$, $t \in T$ je $t\cdot\boldsymbol{u} \in \operatorname{Ker}\varphi$. Dohromady tedy dostáváme, že $\operatorname{Ker}\varphi$ je podprostorem ve V.

2: tvrzení je pouze speciálním případem věty 1.2. 1.. ■

Věta 1.6.
Nechť $\varphi : V \to V'$ je lineární zobrazení. Pak φ je injektivní $\iff$ $\operatorname{Ker}\varphi = \{\boldsymbol{o}\}$.

Důkaz.
„$\Rightarrow$“: Nechť φ je injektivní zobrazení. Dokážeme množinovou rovnost $\operatorname{Ker}\varphi = \{\boldsymbol{o}\}$. Inkluze „$\supseteq$“ je však zřejmá (protože $\varphi(\boldsymbol{o}) = \boldsymbol{o}'$), tzn. stačí dokázat inkluzi opačnou. Nechť tedy $\boldsymbol{x} \in \operatorname{Ker}\varphi$. Pak $\varphi(\boldsymbol{x}) = \boldsymbol{o}'$. Víme však, že je také $\varphi(\boldsymbol{o}) = \boldsymbol{o}'$, tzn. dostáváme tak, že $\varphi(\boldsymbol{x}) = \varphi(\boldsymbol{o})$. Zobrazení φ je však injektivní, a tedy $\boldsymbol{x} = \boldsymbol{o} \in \{\boldsymbol{o}\}$. Dokázali jsme tak, že $\operatorname{Ker}\varphi \subseteq \{\boldsymbol{o}\}$ a dohromady pak $\operatorname{Ker}\varphi = \{\boldsymbol{o}\}$.

„$\Leftarrow$“: Nechť je $\operatorname{Ker}\varphi = \{\boldsymbol{o}\}$. Dokážeme, že zobrazení φ je injektivním zobrazením. Nechť je tedy $\varphi(\boldsymbol{u}) = \varphi(\boldsymbol{v})$. Potom $\varphi(\boldsymbol{u}) - \varphi(\boldsymbol{v}) = \boldsymbol{o}'$ a užitím toho, že φ je lineární zobrazení dostáváme $\varphi(\boldsymbol{u} - \boldsymbol{v}) = \boldsymbol{o}'$. To však znamená, že $\boldsymbol{u} - \boldsymbol{v} \in \operatorname{Ker}\varphi$, odkud podle předpokladu plyne, že $\boldsymbol{u} - \boldsymbol{v} = \boldsymbol{o}$, tzn. $\boldsymbol{u} = \boldsymbol{v}$. Dokázali jsme tak, že zobrazení φ je injektivní. ■

Věta 1.7. (Věta o dimenzi jádra a obrazu lineárního zobrazení)
Nechť $\varphi : V \to V'$ je lineární zobrazení. Pak platí:

$$\dim(\operatorname{Ker}\varphi) + \dim(\operatorname{Im}\varphi) = \dim V .$$

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 $\boldsymbol{v}'_1, \dots, \boldsymbol{v}'_r$ je báze $\operatorname{Im}\varphi$. Pak existují vektory (obecně nikoliv jednoznačně!) $\boldsymbol{u}_1, \dots, \boldsymbol{u}_r \in V$ tak, že $\varphi(\boldsymbol{u}_1) = \boldsymbol{v}'_1, \dots, \varphi(\boldsymbol{u}_r) = \boldsymbol{v}'_r$.

Z věty 1.1.3. plyne, že vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_r$ jsou lineárně nezávislé, tzn. platí potom, že

$$\dim L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_r) = r = \dim(\operatorname{Im}\varphi) . \tag{1}$$

Dále:

I. *Ukážeme, že* $\operatorname{Ker}\varphi + L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_r) = V$.

Inkluze „$\subseteq$“ je však zřejmá, tzn. budeme dokazovat inkluzi opačnou. Nechť tedy $\boldsymbol{x} \in V$, libovolný. Pak $\varphi(\boldsymbol{x}) \in \operatorname{Im}\varphi$. Vyjádříme vektor $\varphi(\boldsymbol{x})$ pomocí báze $\operatorname{Im}\varphi$:

$$\varphi(\boldsymbol{x}) = c_1 \cdot \boldsymbol{v}'_1 + \cdots + c_r \cdot \boldsymbol{v}'_r , \qquad \text{kde } c_i \in T .$$

Uvažme nyní vektor $\boldsymbol{u} = c_1 \cdot \boldsymbol{u}_1 + \cdots + c_r \cdot \boldsymbol{u}_r$. Zřejmě je $\boldsymbol{u} \in L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_r)$ a dále:

$$\varphi(\boldsymbol{u}) = \varphi(c_1 \cdot \boldsymbol{u}_1 + \cdots + c_r \cdot \boldsymbol{u}_r) = c_1 \cdot \varphi(\boldsymbol{u}_1) + \cdots + c_r \cdot \varphi(\boldsymbol{u}_r) = c_1 \cdot \boldsymbol{v}'_1 + \cdots + c_r \cdot \boldsymbol{v}'_r = \varphi(\boldsymbol{x}),$$

odkud $\varphi(\boldsymbol{x}) - \varphi(\boldsymbol{u}) = \boldsymbol{o}'$, tzn. $\varphi(\boldsymbol{x} - \boldsymbol{u}) = \boldsymbol{o}'$, neboli $\boldsymbol{x} - \boldsymbol{u} \in \operatorname{Ker}\varphi$. Potom však:

$$\boldsymbol{x} = (\boldsymbol{x} - \boldsymbol{u}) + \boldsymbol{u} \in \operatorname{Ker}\varphi + L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_r),$$

II. *Ukážeme, že* $\operatorname{Ker}\varphi \cap L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_r) = \{\boldsymbol{o}\}$.

Zřejmě stačí dokazovat pouze inkluzi „$\subseteq$“. Nechť tedy $\boldsymbol{x} \in \operatorname{Ker}\varphi \cap L(\boldsymbol{u}_1, \dots, \boldsymbol{u}_r)$. Pak $\varphi(\boldsymbol{x}) = \boldsymbol{o}'$ a současně $\boldsymbol{x} = t_1 \cdot \boldsymbol{u}_1 + \cdots + t_r \cdot \boldsymbol{u}_r$, odkud dostáváme:

$$\boldsymbol{o}' = \varphi(\boldsymbol{x}) = t_1 \cdot \varphi(\boldsymbol{u}_1) + \cdots + t_r \cdot \varphi(\boldsymbol{u}_r) = t_1 \cdot \boldsymbol{v}'_1 + \cdots + t_r \cdot \boldsymbol{v}'_r.$$

Z lineární nezávislosti vektorů $\boldsymbol{v}'_1, \dots, \boldsymbol{v}'_r$ nyní plyne, že $t_1 = \cdots = t_r = 0$, a tedy po dosazení dostáváme $\boldsymbol{x} = \boldsymbol{o}$.

Z I. a II., užitím věty dimenzi o součtu a průniku podprostorů a vztahu (1) pak dostáváme:

$$\dim V \;=\; \dim\big(\operatorname{Ker}\varphi \,+\, L(\boldsymbol{u}_1,\dots,\boldsymbol{u}_r)\big) \;=$$

$$= \dim\operatorname{Ker}\varphi \,+\, \dim L(\boldsymbol{u}_1,\dots,\boldsymbol{u}_r) \,-\, \dim\big(\operatorname{Ker}\varphi \cap L(\boldsymbol{u}_1,\dots,\boldsymbol{u}_r)\big) \;=$$

$$=\; \dim\operatorname{Ker}\varphi + \dim\operatorname{Im}\varphi - 0 \;=\; \dim\operatorname{Ker}\varphi + \dim\operatorname{Im}\varphi$$

a věta tedy platí. ■

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.
Reflexivnost relace $\cong$ je zřejmá, neboť id_V je izomorfismus V na V, a tedy $V \cong V$.

Symetrie: nechť platí $V \cong V'$, tzn. existuje izomorfismus $\varphi : V \to V'$. Pak zobrazení $\varphi^{-1} : V' \to V$ je podle věty 1.3. 2. také izomorfizmus, což znamemá, že $V' \cong V$.

Tranzitivita relace $\cong$ plyne z vlastností bijekce a z věty 1.3. 1. ■

Věta 1.9.
Nechť $\varphi : V \to V'$ je izomorfismus a $\boldsymbol{u}_1,\dots,\boldsymbol{u}_k \in V$. Pak platí:

1. $\boldsymbol{u}_1,\dots,\boldsymbol{u}_k$ *jsou lineárně závislé* $\iff$ $\varphi(\boldsymbol{u}_1),\dots,\varphi(\boldsymbol{u}_k)$ *jsou lineárně závislé*
2. $\boldsymbol{u}_1,\dots,\boldsymbol{u}_k$ *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. na 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 stejné vlastnosti. V matematice se obvykle o takových algebraických strukturách 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. Ukáže se, že dva vektorové prostory jsou izomorfní právě když mají stejnou dimenzi.

Věta 1.10. (Věta o izomorfismu vektorových prostorů)
Nechť V, V' jsou vektorové prostory nad T. Pak:

$$V \cong V' \quad \Longleftrightarrow \quad \dim V = \dim V' .$$

Důkaz.
„$\Rightarrow$“: Plyne přímo z věty 1.9. 4..

„$\Leftarrow$“: Je-li $\dim V = \dim V' = 0$, pak oba prostory jsou nulovými vektorovými prostory a zřejmě je $V \cong V'$. Nechť tedy $\dim V = \dim V' = n$, kde $n \geq 1$ a nechť

$$\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n \text{ je báze } V \qquad \text{a} \qquad \boldsymbol{u}'_1, \ldots, \boldsymbol{u}'_n \text{ je báze } V' .$$

Nyní sestrojíme hledaný izomorfizmus prostoru V do prostoru V'. Nechť $\boldsymbol{x} \in V$, přičemž $\boldsymbol{x} = x_1 \cdot \boldsymbol{u}_1 + \cdots + x_n \cdot \boldsymbol{u}_n$ (víme, že toto vyjádření existuje, a to jediné). Položme:

$$\varphi(\boldsymbol{x}) = x_1 \cdot \boldsymbol{u}'_1 + \cdots + x_n \cdot \boldsymbol{u}'_n .$$

Pak zřejmě $\varphi : V \to V'$ je zobrazení, o kterém ukážeme, že je hledaným izomorfizmem.

I. *φ je bijektivní zobrazení.*
Libovolný vektor $\boldsymbol{x}' \in V'$, kde $\boldsymbol{x}' = t_1 \cdot \boldsymbol{u}'_1 + \cdots + t_n \cdot \boldsymbol{u}'_n$ má při zobrazení φ jediný vzor ve V, a to vektor $\boldsymbol{x} = t_1 \cdot \boldsymbol{u}_1 + \cdots + t_n \cdot \boldsymbol{u}_n$, což ihned plyne z definice zobrazení φ a z jednoznačnosti vyjádření vektorů pomocí báze. Tedy φ je bijektivní zobrazení.

II. *φ je lineární zobrazení.*
Nechť $\boldsymbol{x}, \boldsymbol{y} \in V$, $t \in T$, přičemž $\boldsymbol{x} = x_1 \cdot \boldsymbol{u}_1 + \cdots + x_n \cdot \boldsymbol{u}_n$, $\boldsymbol{y} = y_1 \cdot \boldsymbol{u}_1 + \cdots + y_n \cdot \boldsymbol{u}_n$.
Potom je $\boldsymbol{x} + \boldsymbol{y} = (x_1{+}y_1) \cdot \boldsymbol{u}_1 + \cdots + (x_n{+}y_n) \cdot \boldsymbol{u}_n$, $t \cdot \boldsymbol{x} = (tx_1) \cdot \boldsymbol{u}_1 + \cdots + (tx_n)\boldsymbol{u}_n$.
Podle definice zobrazení φ a po úpravě pak dostáváme:

$$\varphi(\boldsymbol{x} + \boldsymbol{y}) = (x_1{+}y_1) \cdot \boldsymbol{u}'_1 + \cdots + (x_n{+}y_n) \cdot \boldsymbol{u}'_n =$$

$$= (x_1\boldsymbol{u}'_1 + \cdots + x_n\boldsymbol{u}'_n) + (y_1\boldsymbol{u}'_1 + \cdots + y_n\boldsymbol{u}'_n) = \varphi(\boldsymbol{x}) + \varphi(\boldsymbol{y}) .$$

Analogickým způsobem (rozepište si podrobně sami) dostaneme, že $\varphi(t \cdot \boldsymbol{x}) = t \cdot \varphi(\boldsymbol{x})$. Tedy φ je lineární zobrazení.

Dohromady dostáváme, že φ je izomorfismus prostoru V na V' a je 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 $n = 1, 2, 3, \ldots$ 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 podstatného 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 speciálním případem lineárního zobrazení, a sice pro $V' = V$. Znamená to tedy, že všechny úvahy z předchozího paragrafu zůstávají v platnosti i pro lineární transformace a pro lineární transformace bude zřejmě platit ještě něco navíc.

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 o dimenzi jádra a obrazu lineárního zorazení je $\dim \operatorname{Im}\varphi = \dim V$. Protože však je $\operatorname{Im}\varphi \subseteq V$, musí být $\varphi(V) = V$. To však znamená, že φ je surjektivní zobrazení.

„$3 \Rightarrow 4$“: Nechť φ surjektivní zobrazení, tzn. $\varphi(V) = V$. Nechť nyní $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ je báze prostoru V. Podle věty 1.2. 2. jsou $\varphi(\boldsymbol{u}_1), \ldots, \varphi(\boldsymbol{u}_n)$ 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 $\varphi(\boldsymbol{u}_1), \ldots, \varphi(\boldsymbol{u}_n)$ je báze V.

„$4 \Rightarrow 5$“: Nechť platí 4. a nechť $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k \in V$ jsou lineárně nezávislé vektory. Ale lineárně nezávislé vektory z V lze doplnit na bázi prostoru V, například $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k, \boldsymbol{v}_{k+1}, \ldots, \boldsymbol{v}_n$. Podle 4. jsou vektory $\varphi(u_1), \ldots \varphi(u_k), \varphi(v_{k+1}), \ldots, \varphi(v_n)$ bází prostoru V, tzn. jsou lineárně nezávislé. Potom také vektory $\varphi(\boldsymbol{u}_1), \ldots, \varphi(\boldsymbol{u}_k)$ jsou lineárně nezávislé.

„$5 \Rightarrow 1$“: Nechť platí 5. Nejprve dokážeme, že je $\operatorname{Ker}\varphi = \{\boldsymbol{o}\}$. Je-li však $\boldsymbol{x} \neq \boldsymbol{o}$, pak je vektor $\boldsymbol{x}$ lineárně nezávislý, a tedy podle 5 je $\varphi(\boldsymbol{x})$ také lineárně nezávislý, což znamená, že $\varphi(\boldsymbol{x}) \neq \boldsymbol{o}$. Dokázali jsme tak, že $\operatorname{Ker}\varphi = \{\boldsymbol{o}\}$.

Je-li $\operatorname{Ker}\varphi = \{\boldsymbol{o}\}$, pak z věty 1.6. plyne, že zobrazení φ je injektivní. Dále pak, stejným způsobem jako v důkazu implikace „$1 \Rightarrow 2$“ dokážeme, že zobrazení φ je surjektivní.

Dohromady dostáváme, že φ je bijektivní lineární transformace, tzn. automorfismus. ∎

Definice.
Nechť φ je lineární transformace prostoru V. Nechť $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ je pevná báze prostoru V a platí:

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

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* $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$.

Poznámka.
Vidíme, že matice A je čtvercovou maticí řádu n (kde $n = \dim V$), která je utvořena tak, že souřadnice vektoru $\varphi(\boldsymbol{u}_j)$ v bázi $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ jsou napsány do j-tého sloupce matice A $(j = 1, \ldots, n)$. Tyto souřadnice jsou určeny jednoznačně, což znamená, že i matice A je určena jednoznačně.

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.

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
$$(\varphi + \psi)(\boldsymbol{u}) = \varphi(\boldsymbol{u}) + \psi(\boldsymbol{u}) \qquad \text{pro } \forall\, \boldsymbol{u} \in V$$
se nazývá *součet lineárních transformací* φ a ψ

2. $\varphi \circ \psi : V \to V$ definované
$$(\varphi \circ \psi)(\boldsymbol{u}) = \varphi\big(\psi(\boldsymbol{u})\big) \qquad \text{pro } \forall\, \boldsymbol{u} \in V$$
se nazývá *součin lineárních transformací* φ a ψ

3. $t \cdot \varphi : V \to V$ definované
$$(t \cdot \varphi)(\boldsymbol{u}) = t \cdot \big(\varphi(\boldsymbol{u})\big) \qquad \text{pro } \forall\, \boldsymbol{u} \in V$$
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 platí:

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

$$\omega : V \to V\,, \quad \text{definovaná: } \omega(\boldsymbol{u}) = \boldsymbol{o} \text{ pro } \forall\, \boldsymbol{u} \in V)\,,$$

resp. opačným prvkem k $\varphi \in \mathcal{L}(V)$ je lineární transformace

$$\varrho : V \to V\,, \quad \text{definovaná: } \varrho(\boldsymbol{u}) = -\varphi(\boldsymbol{u}) \text{ pro } \forall\, \boldsymbol{u} \in V\,.$$

3: Dokáže se opět rozepsáním, s využitím 2. Jedničkou tohoto okruhu je zřejmě identická transformace id_V.
4: Dokáže se užitím 2 a bezprostředním ověřením axiomů vektorového prostoru. ■

Věta 2.3.
Nechť φ, ψ jsou lineární transformace prostoru V, $\dim V = n \geq 1$*. Nechť maticí lineární transformace φ v bázi $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ je matice A a nechť maticí lineární transformace ψ v bázi $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ je matice B. Potom:*

1. *maticí lineární transformace $\varphi + \psi$ v bázi $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ je matice $A + B$*
2. *maticí lineární transformace $\varphi \circ \psi$ v bázi $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ je matice $A \cdot B$*
3. *maticí lineární transformace $t \cdot \varphi$ v bázi $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ je matice $t \cdot A$.*

Důkaz.
Nechť $A = (a_{ij})$, $B = (b_{ij})$, $i, j = 1, \dots, n$. Při tomto označení pak platí:

$$\varphi(\boldsymbol{u}_j) = \sum_{r=1}^{n} a_{rj} \cdot \boldsymbol{u}_r\,, \qquad \psi(\boldsymbol{u}_j) = \sum_{r=1}^{n} b_{rj} \cdot \boldsymbol{u}_r \qquad \text{pro } j = 1, \dots, n.$$

Potom:
1: Pro $j = 1, \dots, n$ je

$$(\varphi + \psi)(\boldsymbol{u}_j) = \varphi(\boldsymbol{u}_j) + \psi(\boldsymbol{u}_j) = \sum_{r=1}^{n} a_{rj} \cdot \boldsymbol{u}_r + \sum_{r=1}^{n} b_{rj} \cdot \boldsymbol{u}_r = \sum_{r=1}^{n} (a_{rj} + b_{rj}) \cdot \boldsymbol{u}_r$$

a tedy maticí lineární transformace $\varphi + \psi$ v bázi $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ je matice $(a_{ij} + b_{ij}) = A + B$.

2: Označme $A \cdot B = (c_{ij})$, tzn. $c_{ij} = \sum_{k=1}^{n} a_{ik} \cdot b_{kj}$ pro $i, j = 1, \dots, n$. Potom

$$(\varphi \circ \psi)(\boldsymbol{u}_j) = \varphi\left(\sum_{r=1}^{n} b_{rj} \cdot \boldsymbol{u}_r\right) = \sum_{r=1}^{n} b_{rj} \cdot \varphi(\boldsymbol{u}_r) =$$

$$\sum_{r=1}^{n} b_{rj} \cdot \sum_{s=1}^{n} a_{sr} \cdot \boldsymbol{u}_s = \sum_{s=1}^{n} \left(\sum_{r=1}^{n} a_{sr} b_{rj}\right) \cdot \boldsymbol{u}_s = \sum_{s=1}^{n} c_{sj} \cdot \boldsymbol{u}_s\,,$$

odkud plyne, že maticí lineární transformace $\varphi \circ \psi$ v bázi $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ je matice $A \cdot B$.

3: Pro $j = 1, \ldots, n$ je

$$(t \cdot \varphi)(\boldsymbol{u}_j) = t \cdot \varphi(\boldsymbol{u}_j) = t \cdot \sum_{r=1}^{n} a_{rj} \cdot \boldsymbol{u}_r = \sum_{r=1}^{n} (t \cdot a_{rj}) \cdot \boldsymbol{u}_r \,,$$

a tedy maticí lineární transformace $t \cdot \varphi$ v bázi $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ je matice $(t \cdot a_{ij}) = t \cdot A$. ■

Věta 2.4.
Nechť V je vektorový prostor nad T, $\dim V = n \geq 1$. *Pak platí:*

1. *grupa* $(\mathcal{L}(V), +)$ *je izomorfní s grupou* $(\mathrm{Mat}_{nn}(T), +)$
2. *okruh* $(\mathcal{L}(V), +, \circ)$ *je izomorfní s okruhem* $(\mathrm{Mat}_{nn}(T), +, \cdot)$
3. *vektorový prostor* $\mathcal{L}(V)$ *je izomorfní s vektorovým prostorem* $\mathrm{Mat}_{nn}(T)$.

Důkaz.
Nechť $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ 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 $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$. Nyní dokážeme, že:

I. F je bijektivní zobrazení.

Nechť $A \in \mathrm{Mat}_{nn}(T)$ libovolná. Označme $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ vektory z V, jejichž souřadnicemi v bázi $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ jsou po řadě sloupce matice A. Podle základní věty o lineárních zobrazeních existuje jediná lineární transformace φ prostoru V s vlastností

$$\varphi(\boldsymbol{u}_1) = \boldsymbol{v}_1,\ \ldots,\ \varphi(\boldsymbol{u}_n) = \boldsymbol{v}_n\,.$$

Ale maticí lineární transformace φ v bázi $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ 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 homomorfizmus grup, resp. homomorfizmus okruhů, resp. lineární zobrazení.

Důkaz provedeme pro poslední případ, ve zbývajících případech se postupuje analogicky (proveďte si podrobně sami).
Nechť tedy $\varphi, \psi \in \mathcal{L}(V)$, $t \in T$ libovolné, přičemž $F(\varphi) = A$, $F(\psi) = B$. Pak podle věty 2.3. 1., resp. podle věty 2.3. 3. je

$$F(\varphi + \psi) = A + B = F(\varphi) + F(\psi)\,, \quad \textit{resp.} \quad F(t \cdot \varphi) = t \cdot A = t \cdot F(\varphi)\,.$$

Dokázali jsme tak, že F je lineární zobrazení.

Dohromady, F je izomorfismus vektorových prostorů, neboli $\mathcal{L}(V) \cong \mathrm{Mat}_{nn}(T)$. ■

Poznamenejme, že z předchozí věty okamžitě plyne, že okruh $(\mathcal{L}(V), +, \circ)$ je pro $n \geq 2$ nekomutativní (proč?) a dále, že dimenze vektorového prostoru $\mathcal{L}(V)$ je n^2 (proč?).

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) právě když existuje regulární matice S tak, že $B = S^{-1} \cdot A \cdot S$.

Důkaz.
„$\Rightarrow$“: Nechť $A = (a_{ij})$ je matice lineární transformace φ v bázi $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ a nechť $B = (b_{ij})$ je matice téže lineární transformace φ v bázi $\boldsymbol{u}'_1, \dots, \boldsymbol{u}'_n$.

Dále nechť $S = (s_{ij})$ je matice přechodu od báze $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ k bázi $\boldsymbol{u}'_1, \dots, \boldsymbol{u}'_n$, tzn. S je regulární matice a platí:

$$\boldsymbol{u}'_j = \sum_{i=1}^{n} s_{ij} \cdot \boldsymbol{u}_j \qquad \text{pro } j = 1, \dots, n\,.$$

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 $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$) dostáváme, že:

$$\sum_{k=1}^{n} s_{ik} b_{kj} \;=\; \sum_{k=1}^{n} a_{ik} s_{kj} \qquad \text{pro } i, j = 1, \dots, n\,,$$

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 $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ je pevná báze vektorového prostoru V. Pak (podle důkazu věty 2.4.) existuje jediná lineární transformace φ prostoru V taková, že A je maticí φ v bázi $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$.

Dále, S je regulární matice, tzn. existuje (jediná) báze $\boldsymbol{u}'_1, \dots, \boldsymbol{u}'_n$ prostoru V taková, že S je matice přechodu od báze $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ k bázi $\boldsymbol{u}'_1, \dots, \boldsymbol{u}'_n$.

Konečně, podle předpokladu je $S \cdot B = A \cdot S$, neboli

$$\sum_{k=1}^{n} s_{ik} b_{kj} = \sum_{k=1}^{n} a_{ik} s_{kj} \qquad \text{pro } i, j = 1, \dots, n\,.$$

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 $j = 1, \dots, n$, což však znamená, že B je maticí lineární transformace φ v bázi $\boldsymbol{u}'_1, \dots, \boldsymbol{u}'_n$. Tedy matice A, B jsou maticemi téže lineární transformace prostoru V. $\blacksquare$

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.
Reflexivita: pro libovolnou matici $A \in \mathrm{Mat}_{nn}(T)$ zřejmě platí, že $A = E_n^{-1} \cdot A \cdot E_n$, kde E_n je jednotková matice řádu n. Je tedy $A \sim A$.

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 $B \sim A$.

Tranzitivita: nechť $A \sim B$ a $B \sim C$, tzn. existují regulární matice S, Q tak, že

$$B = S^{-1} \cdot A \cdot S \qquad \text{a} \qquad C = Q^{-1} \cdot B \cdot Q\,.$$

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. Potom 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:

1. *matice A, B mají stejné determinanty, tj. $|A| = |B|$*
2. *matice A, B mají stejnou hodnost, tj. $h(A) = h(B)$*
3. *matice A, B mají 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:

$$|B| = |S^{-1} \cdot A \cdot S| = \frac{1}{|S|} \cdot |A| \cdot |S| = |A|.$$

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:

$$|B - \lambda E_n| \; = \; |S^{-1} \cdot A \cdot S - S^{-1} \cdot (\lambda E_n) \cdot S| \; =$$

$$= \; |S^{-1} \cdot (A - \lambda E_n) \cdot S| \; = \; \frac{1}{|S|} \cdot |A - \lambda E_n| \cdot |S| \; = \; |A - \lambda E_n| \, .$$

■

Poznámka.
Poznamenejme, 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 například matice

$$E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{a} \qquad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

pak zřejmě

$$|E_2| = |B| \quad \text{a} \quad h(E_2) = h(B) \quad \text{a} \quad |E_2 - \lambda E_2| = |B - \lambda E_2| \, ,$$

ale matice E_2 a B evidentně nejsou podobné, protože pro každou regulární matici S řádu dva 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 platí:

$$\dim \mathrm{Im}\, \varphi \; = \; h(A) \, ,$$

Důkaz.
Nechť A je matice lineární transformace φ v bázi $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$. 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 $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ 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 $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$, 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 dostáváme, že $\dim \operatorname{Im} \varphi = h(A)$. ■

§3. Vlastní vektory a vlastní hodnoty

Definice.
Nechť φ je lineární transformace vektorového prostoru V. Podprostor U vektorového prostoru V se nazývá *invariantní podprostor vzhledem k* φ, je-li:

$$\varphi(U) \subseteq U\,, \qquad \text{tzn. pro libovolný vektor } \boldsymbol{x} \in U \text{ platí } \varphi(\boldsymbol{x}) \in U.$$

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 U 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 U 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 $U = \{(x, 0) \mid x \in \mathbb{R}\}$ a dále uvažme dvě lineární transformace φ a ψ prostoru $\mathbb{R}^2$ definované:

$$\varphi\big((x_1, x_2)\big) = (x_1 + x_2, 0) \qquad \text{a} \qquad \psi\big((x_1, x_2)\big) = (x_2, x_1)$$

pro každé $(x_1, x_2) \in \mathbb{R}^2$. Lehce se ověří, že U je invariantní podprostor vzhledem k φ, zatímco tentýž podprostor U není invariantním podprostorem vzhledem k ψ (neboť například $(1, 0) \in U$, ale $\psi\big((1, 0)\big) = (0, 1) \notin U$).

Poznámka.
V příkladu 3.1. jsou uvedeny speciální, triviální případy. Uvědomme si, že obecně podprostor U 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 $\boldsymbol{u} \in \operatorname{Ker}\varphi$. Pak $\varphi(\boldsymbol{u}) = \boldsymbol{o} \in \operatorname{Ker}\varphi$, a tedy $\operatorname{Ker}\varphi$ je invariantní vzhledem k φ. Dále nechť $\boldsymbol{u} \in \operatorname{Im}\varphi$. Zřejmě je $\boldsymbol{u} \in V$. 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 $U_1, \ldots, U_k$ jsou podprostory ve V, které jsou invariantní vzhledem k φ. Pak průnik $(U_1 \cap \cdots \cap U_k)$ a součet $(U_1 + \cdots + U_k)$ jsou invariantní podprostory vzhledem k φ.

Důkaz.
Víme, že $(U_1 \cap \dots \cap U_k)$, resp. $(U_1 + \dots + U_k)$ jsou podprostory ve V. Dodážeme, že se v obou případech jedná o invariantní podprostory vzhledem k φ.

a) Nechť $\boldsymbol{u} \in U_1 \cap \dots \cap U_k$ libovolný. Pak $\boldsymbol{u} \in U_i$ a podle předpokladu $\varphi(\boldsymbol{u}) \in U_i$ pro každé $i = 1, \dots, k$. Tedy $\varphi(\boldsymbol{u}) \in U_1 \cap \dots \cap U_k$, což znamená, že $U_1 \cap \dots \cap U_k$ je invariantní podprostor vzhledem k φ.

b) Nechť $\boldsymbol{u} \in U_1 + \dots + U_k$, tzn. $\boldsymbol{u} = \boldsymbol{u}_1 + \dots + \boldsymbol{u}_k$, kde $\boldsymbol{u}_i \in U_i$. Pak:

$$\varphi(\boldsymbol{u}) = \varphi(\boldsymbol{u}_1 + \dots + \boldsymbol{u}_k) = \varphi(\boldsymbol{u}_1) + \dots + \varphi(\boldsymbol{u}_k) \in U_1 + \dots + U_k\,,$$

neboť podle předpokladu $\varphi(\boldsymbol{u}_i) \in U_i$. Tedy $U_1 + \dots + U_k$ 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 U ve vektorovém prostoru V (nad T) je generován jedním nenulovým vektorem $\boldsymbol{u} \in V$, tzn. je pak:

$$U = L(\boldsymbol{u}) = \{t \cdot \boldsymbol{u} \mid t \in T\}\,.$$

Máme-li navíc dánu lineární transformaci φ prostoru V, pak zřejmě podprostor $U = L(\boldsymbol{u})$ 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 U 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 lineární transformace φ, příslušným vlastní hodnotě λ, pak také každý nenulový vektor $\boldsymbol{v} \in L(\boldsymbol{u})$, tj. každý nenulový násobek vektoru $\boldsymbol{u}$, je také vlastním vektorem lineární transformace φ, příslušným téže vlastní hodnotě λ.

Příklad 3.3.
Nechť V je libovolný pevný vektorový prostor nad T. Dále nechť:
1. $\mathrm{id}_V : V \to V$ 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. $\omega : V \to V$ je nulová lineární transformace prostoru V.
Pak každý nenulový vektor z V je vlastním vektorem transformace ω příslušným vlastní hodnotě $\lambda = 0$ (což je opět jediná vlastní hodnota ω).
3. $\varphi : V \to V$ je libovolná lineární transformace prostoru V.
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 lineární transformace δ, příslušnými vlastní hodnotě $\lambda = 0$ a že žádné jiné vlastní hodnoty a vlastní vektory lineární transformace 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 lineární transformace φ*
2. *je-li $\lambda \in T$ vlastní hodnota φ, pak vlastní vektory φ příslušné λ jsou právě všechny nenulové vektory z podprostoru* $\operatorname{Ker}(\varphi - \lambda \cdot \mathrm{id}_V)$.

Důkaz.
Nejprve dokážeme 2. část věty a potom 1. část věty.

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:

$$\boldsymbol{u} \neq \boldsymbol{o} \quad \wedge \quad (\varphi - \lambda \cdot \mathrm{id}_V)(\boldsymbol{u}) = \boldsymbol{o}. \tag{2}$$

Množina vektorů splňujících (2) je však rovna množině všech nenulových vektorů z podprostoru $\operatorname{Ker}(\varphi - \lambda \cdot \mathrm{id}_V)$ vektorového prostoru V.

1: Z právě dokázaného a z vět 2.8. a 1.7. plyne:

$$\begin{aligned} &\lambda \text{ je vlastní hodnota } \varphi \iff \lambda \in T \ \wedge\ \operatorname{Ker}(\varphi - \lambda \cdot \mathrm{id}_V) \neq \{\boldsymbol{o}\} \iff \\ &\iff \lambda \in T \wedge \text{matice lineární transformace } (\varphi - \lambda \cdot \mathrm{id}_V) \text{ je singulární.} \end{aligned}$$

Je-li A maticí lineární transformace φ (v pevné bázi prostoru V), pak zřejmě $(A - \lambda \cdot E_n)$ je maticí lineární transformace $(\varphi - \lambda \cdot \mathrm{id}_V)$ v téže bázi. Tedy pak:

$$\lambda \text{ je vlastní hodnota } \varphi \iff \lambda \in T \ \wedge\ |A - \lambda \cdot E_n| = 0\,,$$

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:

$$\begin{aligned} (a_{11} - \lambda)x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= 0 \\ a_{21}x_1 + (a_{22} - \lambda)x_2 + \cdots + a_{2n}x_n &= 0 \\ &\vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + (a_{nn} - \lambda)x_n &= 0 \end{aligned} \tag{3}$$

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). ■

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 $\lambda_1, \dots, \lambda_n$ (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 $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ jsou vlastní vektory lineární transformace φ příslušné navzájem různým vlastním hodnotám $\lambda_1, \dots, \lambda_k$. Z posloupnosti vektorů $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ vybereme libovolnou maximální lineárně nezávislou posloupnost. Bez újmy na obecnosti lze předpokládat, že ji tvoří například prvních r vektorů, tj. $\boldsymbol{u}_1, \dots, \boldsymbol{u}_r$. 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 $\boldsymbol{u}_1, \dots, \boldsymbol{u}_r$ však plyne, že $t_i \cdot (\lambda_{r+1} - \lambda_i) = 0$ pro $i = 1, \dots, r$. Podle předpokladu věty je však $\lambda_{r+1} - \lambda_i \neq 0$, a tedy musí být $t_i = 0$ pro $i = 1, \dots, r$. 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. ■

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. ■

§4. Ortogonální zobrazení, ortogonální matice

V tomto paragrafu se vrátíme k euklidovským vektorovým prostorům a budeme studovat vzájemné vztahy mezi nimi. Použijeme k tomu lineárních zobrazení, 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:

$$\boldsymbol{u} \cdot \boldsymbol{v} = \varphi(\boldsymbol{u}) \cdot \varphi(\boldsymbol{v}) \qquad \text{pro každé } \boldsymbol{u}, \boldsymbol{v} \in V\,.$$

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 speciálně $V' = V$, pak se ortogonální zobrazení φ nazývá *ortogonální transformace euklidovského prostoru V.*

Podmínku „zachování skalárního součinu“ z předchozí definice je možné pro lineární zobrazení 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: $\quad \varphi(\boldsymbol{u}_i) \cdot \varphi(\boldsymbol{u}_i) = \|\varphi(\boldsymbol{u}_i)\|^2 = \|\boldsymbol{u}_i\|^2 = 1$

– 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 plyne, že $\varphi(\boldsymbol{u}_i) \cdot \varphi(\boldsymbol{u}_j) = 0$.

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 výrok 1 zřejmě platí. 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

$$\boldsymbol{u} = u_1 \cdot \boldsymbol{e}_1 + u_2 \cdot \boldsymbol{e}_2 \qquad \text{a} \qquad \boldsymbol{v} = v_1 \cdot \boldsymbol{e}_1 + v_2 \cdot \boldsymbol{e}_2\,.$$

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

$$\boldsymbol{u} = t \cdot \boldsymbol{e} \qquad \text{a} \qquad \boldsymbol{v} = s \cdot \boldsymbol{e}\,.$$

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. ■

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. Dokážeme postupně obě implikace.

„$\Rightarrow$“: 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 oba nulovými euklidovskými prostory a jsou tedy zřejmě izomorfní.

Nechť tedy $n \geq 1$ a nechť:

$$\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n \text{ je ortonormální báze } V \qquad \text{a} \qquad \boldsymbol{e}'_1, \ldots, \boldsymbol{e}'_n \text{ je ortonormální báze } V'\,.$$

Nechť $\boldsymbol{u} \in V$ je libovolný vektor, přičemž: $\boldsymbol{u} = u_1 \cdot \boldsymbol{e}_1 + \cdots + u_n \cdot \boldsymbol{e}_n$.
Položme nyní:

$$\varphi(\boldsymbol{u}) = u_1 \cdot \boldsymbol{e}'_1 + \cdots + u_n \cdot \boldsymbol{e}'_n\,.$$

Pak φ je zřejmě zobrazení prostoru V do V', o němž se rozepsáním lehce ověří, že je bijektivní a že je lineárním zobrazením (proveďte si sami!). 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 dostáváme, že φ je izomorfismus euklidovského prostoru V na V'. ■

Podmínka zachovávání skalárního součinu, požadovaná v definici ortogonálního zobrazení φ je poměrně velmi silná. Následující věta ukáže, že tato podmínka vynutí injektivnost zobrazení φ.

Věta 4.3.
Nechť V, V' jsou euklidovské prostory a nechť $\varphi : V \to V'$ je ortogonální zobrazení. Pak φ je injektivní zobrazení.

Důkaz.
Injektivnost zobrazení φ budeme tentokrát dokazovat pomocí věty 1.6., tzn. budeme dokazovat, že jádro $\operatorname{Ker}\varphi = \{\boldsymbol{o}\}$. Přitom zřejmě stačí dokázat inkluzi „$\subseteq$“.

Nechť tedy $\boldsymbol{x} \in \operatorname{Ker}\varphi$, 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 tak, že $\operatorname{Ker}\varphi = \{\boldsymbol{o}\}$, odkud podle věty 1.6. plyne, že φ je injektivní zobrazení. ∎

Ve zbývající části tohoto paragrafu se budeme zabývat ortogonálními transformacemi daného euklidovského prostoru V. Je-li speciálně $V = \{\boldsymbol{o}\}$ 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 věty 4.3. a věty 2.1.

2: Podle právě dokázaného bodu 1. je φ bijektivním lineárním zobrazením. Potom podle věty 1.3. 2. je $\varphi^{-1} : V \to V$ izomorfizmem vektorového prostoru V, tzn. φ^{-1} je bijektivním lineárním zobrazením. Zbývá tedy dokázat, že φ^{-1} splňuje podmínku z definice ortogonálního zobrazení, tj. „zachovává skalární součin“.

Nechť $\boldsymbol{u}, \boldsymbol{v} \in V$ libovolné. Označme $\varphi^{-1}(\boldsymbol{u}) = \boldsymbol{a}$, $\varphi^{-1}(\boldsymbol{v}) = \boldsymbol{b}$. Potom je $\varphi(\boldsymbol{a}) = \boldsymbol{u}$, $\varphi(\boldsymbol{b}) = \boldsymbol{v}$ a platí (s využitím faktu, že φ je ortogonálním zobrazením):

$$\boldsymbol{u} \cdot \boldsymbol{v} \;=\; \varphi(\boldsymbol{a}) \cdot \varphi(\boldsymbol{b}) \;=\; \boldsymbol{a} \cdot \boldsymbol{b} \;=\; \varphi^{-1}(\boldsymbol{u}) \cdot \varphi^{-1}(\boldsymbol{v})\,,$$

tzn. dostáváme, že φ^{-1} je ortogonální transformace euklidovského prostoru V.

3: Nechť λ je vlastní hodnota ortogonální transformace 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 $\lambda = \pm 1$. ∎

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, speciálně například 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 3.8., kapitoly 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: tvrzení dokážeme užitím 2. části předchozí věty. Platí:

$$(A \cdot B) \cdot (A \cdot B)' \;=\; A \cdot (B \cdot B') \cdot A' \;=\; A \cdot E_n \cdot A' \;=\; A \cdot A' \;=\; E_n,$$

odkud podle věty 4.5. dostáváme, že $A \cdot B$ je ortogonální maticí.

2: ověříme definici ortogonální matice pro matici A^{-1}. S využitím věty 3.9. 4., kapitoly II. dostáváme:

$$(A^{-1})^{-1} \;=\; (A')^{-1} \;=\; (A^{-1})'$$

což znamená, že matice A^{-1} je ortogonální.

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 ihned plyne, že $|A| = \pm 1$. ∎

Důsledek.
Množina všech ortogonálních matic řádu n s operací násobení matic je grupou, která je pro $n \geq 2$ nekomutativní.

Důkaz.
První část důsledku plyne z předchozí věty, uvědomíme-li si navíc, že násobení matic je asociativní a že jednotková matice E_n je ortogonální.

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

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

Potom zřejmě matice A, B jsou ortogonální, a platí $A \cdot B \neq B \cdot A$ (ověřte si sami výpočtem – počítejte přitom prvek v prvním řádku a n-tém sloupci obou součinů matic). Tedy uvažovaná grupa je pro $n \geq 2$ nekomutativní. ■

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 $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ je ortonormální báze prostoru V a nechť $A = (a_{ij})$ je matice lineární transformace φ v této bázi $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$. Dokážeme postupně obě implikace.

„$\Rightarrow$“: Nechť φ je ortogonální transformace euklidovského prostoru V. Pak podle věty 4.1. vektory $\varphi(\boldsymbol{e}_1), \dots, \varphi(\boldsymbol{e}_n)$ tvoří ortonormální bázi prostoru V. Označme $A' \cdot A = B = (b_{ij})$. Pak platí:

$$\varphi(\boldsymbol{e}_i) \cdot \varphi(\boldsymbol{e}_j) = (a_{1i} \cdot \boldsymbol{e}_1 + \cdots + a_{ni} \cdot \boldsymbol{e}_n) \cdot (a_{1j} \cdot \boldsymbol{e}_1 + \cdots + a_{nj} \cdot \boldsymbol{e}_n) = \sum_{k=1}^{n} a_{ki} \cdot a_{kj} = b_{ij},$$

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 pak matice A ortogonální.

„$\Leftarrow$“: Nechť matice A je ortogonální, tzn. platí (dle věty 4.5. 3.):

$$\sum_{k=1}^{n} a_{ki} \cdot a_{kj} = \begin{cases} 1 & \text{pro } i = j \\ 0 & \text{pro } i \neq j \end{cases} \tag{1}$$

Nechť dále $\boldsymbol{u} \in V$ libovolný, přičemž $\boldsymbol{u} = \sum_{i=1}^{n} u_i \cdot \boldsymbol{e}_i$. Potom je: $\|\boldsymbol{u}\|^2 = \boldsymbol{u} \cdot \boldsymbol{u} = \sum_{i=1}^{n} u_i^2$.

Dále je:

$$\varphi(\boldsymbol{u}) = \sum_{i=1}^{n} u_i \cdot \varphi(\boldsymbol{e}_i) = \sum_{i=1}^{n} u_i \cdot \sum_{k=1}^{n} a_{ki} \cdot \boldsymbol{e}_k = \sum_{k=1}^{n} \left(\sum_{i=1}^{n} a_{ki} u_i \right) \cdot \boldsymbol{e}_k,$$

odkud rozepsáním a úpravou (užitím ortonormálnosti vektorů $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$) dostáváme:

$$\|\varphi(\boldsymbol{u})\|^2 = \varphi(\boldsymbol{u}) \cdot \varphi(\boldsymbol{u}) = \quad \dots \quad = \sum_{i=1}^{n} \sum_{j=1}^{n} \left(\sum_{k=1}^{n} a_{ki} a_{kj} \right) u_i u_j ,$$

tzn. po dosazení z (1) je pak: $\|\varphi(\boldsymbol{u})\|^2 = \sum_{i=1}^{n} u_i^2$.

Dohromady potom dostáváme, že $\|\boldsymbol{u}\|^2 = \|\varphi(\boldsymbol{u})\|^2$, neboli $\|\boldsymbol{u}\| = \|\varphi(\boldsymbol{u})\|$, což znamená, že φ je ortogonální transformace. ■

Obsah