PRAKTICKÁ LINEÁRNÍ ALGEBRA A GEOMETRIE

Matici homomorfismu $f : V \to W$ vzhledem k bázím $B \subset V$ a $C \subset W$ budme zpravidla značit $[f]_{BC}$. V souladu s tímto značením budeme označovat $[\mathrm{Id}]_{B_2 B_1}$ matici přechodu od báze B_1 k bázi B_2. Symbolem $\mathbb{Z}_p$ budeme značit těleso celých čísel $\{0, 1, \dots, p-1\}$ se sčítáním a násobením modulo prvočíslo p.

Značení, které není komentováno, je shodné se značením učebnice profesora Bicana.

1. Lineární kódy

Definice. Každou neprázdnou množinu $\mathcal{C} \subseteq \mathbb{Z}_2^n$ nazveme *(binárním blokovým) kódem.* Řeknem, že $\mathcal{C}$ je *lineární kód* délky n a dimenze k, je-li $\mathcal{C}$ podprostorem vektorového prostoru $\mathbb{Z}_2^n$ nad tělesem $\mathbb{Z}_2$ a $\dim \mathcal{C} = k$.

Vektory libovolného kódu (délky n) budeme zpravidla nazývat *slovy* (délky n). Slovo budeme zapisovat jako posloupnost 0 a 1 bez závorek a oddělovacích čárek.

Definice. Nechť $\mathcal{C}$ je lineární kód délky n a dimenze k. Řekneme, že matice $\mathbf{C}$ typu (k, n) nad tělesem $\mathbb{Z}_2$ je *generující maticí* kódu $\mathcal{C}$, jestliže řádky matice $\mathbf{C}$ tvoří bázi lineárního kódu $\mathcal{C}$. Řekneme, že matice $\mathbf{D}$ typu $(n, n-k)$ nad tělesem $\mathbb{Z}_2$ je *kontrolní maticí* kódu $\mathcal{C}$, platí-li, že $\mathbf{v} \in \mathcal{C}$ právě tehdy, když $\mathbf{v}\,\mathbf{D} = \mathbf{0}$ (tj. $\mathcal{C}$ je právě množinou všech řešení homogenní soustavy rovnic s maticí $\mathbf{D}^\mathsf{T}$).

Příklad. Uveďme čtyři příklady lineárních kódů dimenze 2 a (nějakých) jim příslušných generujících a kontrolních matic:

1) $\mathcal{C}_1 = \{00, 01, 10, 11\}$, $\mathbf{C}_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ a kontrolní matice je prázdná.

2) $\mathcal{C}_2 = \{0000, 0101, 1010, 1111\}$, $\mathbf{C}_2 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ a $\mathbf{D}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$.

3) $\mathcal{C}_3 = \{000000, 010101, 101010, 111111\}$,

$$\mathbf{C}_3 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \text{ a } \mathbf{D}_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Date: 31.5.2010.

4) $\mathcal{C}_4 = \{000, 011, 101, 110\}$, $\mathbf{C}_4 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ a $\mathbf{D}_4 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$.

Lineární kódy $\mathcal{C}_2$ a $\mathcal{C}_3$ jsou takzvané opakovací kódy.

Definujeme-li (relativní) rychlost přenosu informace kódem $\mathcal{C}$ délky n jako číslo $\frac{1}{n}\log_2|\mathcal{C}|$, které je pro linární kód rovno hodnotě $\frac{\dim \mathcal{C}}{n}$, pak je první kód sice nejrychlejší, ale pokud při přenosu dojde k chybě, nedokážeme ji odhalit, protože chybně přijaté slovo bude rovněž kódovým slovem. Naproti tomu ve slově kódu $\mathcal{C}_2$ jsme schopni jednu chybu odhalit (například chyba na druhé souřadnici slova 1111 znamená, že přijmeme slovo 1011, které neleží v kódu $\mathcal{C}_2$), ovšem tuto chybu nedokážeme opravit (pokud dojde k chybě na čtvrté souřadnici slova 1010, přijmeme rovněž slovo 1011 a nemůžeme tudíž rozhodnout, které slovo kódu $\mathcal{C}_2$ bylo při přijetí 1011 původně vysláno, i když víme, že při přenosu došlo právě k jedné chybě). Podobně i kód $\mathcal{C}_4$ umožňuje rozpoznat jednu chybu při přenosu, ale neumožňuje její opravu. Tento kód je ovšem rychlejší než kód $\mathcal{C}_2$. Konečně kód $\mathcal{C}_3$ dokáže chybu nejen odhalit, ale i opravit. Víme-li (nebo předpokládáme-li), že došlo při přenosu slova právě k jedné chybě a uvědomíme-li si, že v každém slově kódu $\mathcal{C}_4$ se postupně třikrát zopakuje stejné slovo délky 2, pak jedna chyba znamená, že dvakrát přijmeme správné (pod)slovo a jednou nesprávné. Například při chybě ve slově 010101 na šesté souřadnici, přijmeme slovo 010100. Jestliže nesprávnou část slova nahradíme (dvakrát zopakovanou) správnou částí (tj. poslední dvě souřadnice 00 nahradíme slovem 01) dostaneme původně vyslané slovo.

Poznámka 1.1. *Nechť $\mathcal{C}$ je lineární kód délky n a dimenze k, $\mathbf{C}$ je jeho generující a $\mathbf{D}$ kontrolní matice. Mějme $\mathbf{P}$ regulární matici stupně k a $\mathbf{Q}$ regulární matici stupně $n-k$. Pak $\mathbf{PC}$ a $\mathbf{DQ}$ jsou rovněž generující a kontrolní maticí lineárního kódu $\mathcal{C}$.*

Důkaz. Označme $\mathcal{P}$ lineární kód s generující maticí $\mathbf{PC}$ a $\mathcal{Q}$ lineární kód s kontrolní maticí $\mathbf{DQ}$. Uvážíme-li, že řádky matice $\mathbf{PC}$ jsou lineární kombinací řádků matice $\mathbf{C}$, dostáváme $\mathcal{P} \subseteq \mathcal{C}$. Protože je dimenze kódů rovna hodnosti generujících matic a ty jsou konečné a stejné, je $\mathcal{P} = \mathcal{C}$.

Podobně množina všech řešení homogenní soustavy rovnic s maticí $\mathbf{Q}^T$ a $\mathbf{Q}^T\mathbf{D}^T$ jsou totožné, proto $\mathcal{Q} = \mathcal{C}$. □

Věta 1.2. *Nechť $\mathbf{C}$ je matice typu (k,n) a $\mathbf{D}$ matice typu $(n,n-k)$ obě nad tělesem $\mathbb{Z}_2$. Pak jsou následující tvrzení ekvivalentní:*

(1) *$\mathbf{C}$ a $\mathbf{D}$ jsou generující a kontrolní maticí nějakého lineárního kódu,*
(2) *$h(\mathbf{C}) = k$, $h(\mathbf{D}) = n-k$ a $\mathbf{CD} = \mathbf{0}$.*

Důkaz. (1) $\Rightarrow$ (2) Je-li $\mathbf{C}$ generující matice kódu, pak $k \leq n$ a $\mathbf{C}$ obsahuje v řádcích lineárně nezávislé vektory. Proto $h(\mathbf{C}) = k$. Kód $\mathcal{C}$ je právě množinou všech řešení homogenní soustavy rovnic s maticí $\mathbf{D}^{\mathrm{T}}$, proto $k = \dim \mathcal{C} = n - h(\mathbf{D}^{\mathrm{T}})$, tudíž $h(\mathbf{D}^{\mathrm{T}}) = h(\mathbf{D}) = n-k$. Konečně $\mathbf{v}\,\mathbf{D} = \mathbf{0}$ pro všechna slova kódu $\mathcal{C}$, tedy i pro všechny řádky matice $\mathbf{C}$, tj. $\mathbf{CD} = \mathbf{0}$.

(2) $\Rightarrow$ (1) Označme $\mathcal{C}$ podprostor $\mathbb{Z}_2^n$ generovaný řádky matice $\mathbf{C}$. Potom je přímo z definice $\mathcal{C}$ lineárním kódem s generující maticí $\mathbf{C}$. Libovolné slovo $\mathbf{v} \in \mathcal{C}$ dostaneme jako lineární kombinaci řádků matice $\mathbf{C}$, tedy $\mathbf{v} = \mathbf{x}\,\mathbf{C}$ pro vhodné $\mathbf{x} \in \mathbb{Z}_2^k$. Tedy $\mathbf{v}\,\mathbf{D} = \mathbf{x}\,\mathbf{CD} = \mathbf{0}$. Protože množina všech řešení homogenní soustavy

rovnic s maticí $\mathbf{D}^{\mathrm{T}}$ má dimenzi $n-(n-k)=k$, dostáváme, že $\mathbf{D}$ je kontrolní maticí kódu $\mathbf{C}$. $\square$

Definice. Nechť $\mathbf{u},\mathbf{v}\in\mathbb{Z}_2^n$. *(Hammingovou) vzdáleností* slov $\mathbf{u}$ a $\mathbf{v}$ budeme rozumět počet souřadnic, v nichž se obě slova liší. *(Hammingovou) váhou* slova $\mathbf{u}\in\mathbb{Z}_2^n$ nazveme počet souřadnic slova $\mathbf{u}$ rovných jedné. Vzdálenost slov $\mathbf{u}$ a $\mathbf{v}$ budeme značit $d(\mathbf{u},\mathbf{v})$ a váhu slova $\mathbf{u}$ označujme $wt(\mathbf{u})$. Konečně *(Hammingovou) vzdáleností* kódu $\mathcal{C}$ obsahujícího alespoň dvě slova budeme rozumět číslo $d(\mathcal{C})=\min\{d(\mathbf{u},\mathbf{v})|\ \mathbf{u},\mathbf{v}\in\mathcal{C},\mathbf{u}\neq\mathbf{v}\}$.

Poznámka 1.3. *Nechť* $\mathbf{u},\mathbf{v},\mathbf{w}\in\mathbb{Z}_2^n$.

(a) $d(\mathbf{u},\mathbf{v})=wt(\mathbf{u}+\mathbf{v})$,
(b) $wt(\mathbf{u})\leq n$,
(c) $d(\mathbf{u},\mathbf{v})=0$, *právě když* $\mathbf{u}=\mathbf{v}$,
(d) $d(\mathbf{u},\mathbf{v})=d(\mathbf{v},\mathbf{u})$,
(e) $wt(\mathbf{u}+\mathbf{v})\leq wt(\mathbf{u}+\mathbf{w})+wt(\mathbf{w}+\mathbf{v})$,
(f) $d(\mathbf{u},\mathbf{v})\leq d(\mathbf{u},\mathbf{w})+d(\mathbf{w},\mathbf{v})$.

Důkaz. Označme $\mathbf{u}=u_1\dots u_n$, $\mathbf{v}=v_1\dots v_n$ a $\mathbf{w}=w_1\dots w_n$, kde $u_i,v_i,w_i\in\mathbb{Z}_2$.

(a) Stačí si všimnout, že $u_i\neq v_i$, právě když $u_i+v_i=1$.

(b), (c), (d) Okamžitý důsledek definice.

(e) Jestliže $u_i+v_i\neq 0$, potom buď $u_i+w_i\neq 0$ nebo $w_i+v_i\neq 0$, a proto $\{i|\ u_i+v_i\neq 0\}\subseteq\{i|\ u_i+w_i\neq 0\}\cup\{i|\ w_i+v_i\neq 0\}$.

(f) Plyne z a) a e), tedy $d(\mathbf{u},\mathbf{v})=wt(\mathbf{u}+\mathbf{v})\leq wt(\mathbf{u}+\mathbf{w})+wt(\mathbf{w}+\mathbf{v})=d(\mathbf{u},\mathbf{w})+d(\mathbf{w},\mathbf{v})$. $\square$

Poznámka 1.4. *Buď $\mathcal{C}$ lineární kód obsahující alespoň dvě slova. Potom* $d(\mathcal{C})=min\{wt(\mathbf{u})|\ \mathbf{u}\in\mathcal{C},\mathbf{u}\neq\mathbf{0}\}$.

Důkaz. Zvolíme-li nenulové slovo $\mathbf{u}\in\mathcal{C}$, pro něž je $wt(\mathbf{u})$ minimální, pak $d(\mathcal{C})\leq d(\mathbf{u},\mathbf{0})=wt(\mathbf{u})$ díky 1.3(a). Vezmeme-li naopak dvě různá slova $\mathbf{v},\mathbf{w}\in\mathcal{C}$, pro která $d(\mathbf{v},\mathbf{w})=d(\mathcal{C})$, pak $\mathbf{0}\neq\mathbf{v}+\mathbf{w}\in\mathcal{C}$, a proto $wt(\mathbf{u})\leq wt(\mathbf{v}+\mathbf{w})=d(\mathbf{v},\mathbf{w})=d(\mathcal{C})$. $\square$

Protože lineární kód, který obsahuje jen jedno (tedy nulové) slovo, není prakticky ani teoreticky nijak zajímavý. Můžeme se v následujících úvahách omezit na nenulové lineární kódy.

Věta 1.5. *Nechť $\mathbf{D}$ je kontrolní matice lineárního kódu $\mathcal{C}$ dimenze n. Pak $d(\mathcal{C})=d$ právě tehdy, když existuje d lineárně závislých řádků matice $\mathbf{D}$ a každých $d-1$ řádků matice $\mathbf{D}$ je lineárně nezávislých.*

Důkaz. Vezměme nejprve nějaké slovo $\mathbf{v}\in\mathbb{Z}_2^n$. Všimněme si, že je $\mathbf{v}\,\mathbf{D}$ lineární kombinací právě $wt(\mathbf{v})$ řádků matice $\mathbf{D}$. Jestliže $d(\mathcal{C})=d$ a $\mathbf{v}\,\mathbf{D}=\mathbf{0}$ pro nenulové slovo $\mathbf{v}\in\mathbb{Z}_2^n$, pak podle definice kontrolní matice $\mathbf{v}\in\mathcal{C}$. Podle Poznámky 1.4 je $wt(\mathbf{v})\geq d$. Odtud plyne, že pro každé slovo $\mathbf{v}$ váhy $d-1$ platí, že $\mathbf{v}\,\mathbf{D}\neq\mathbf{0}$, a tudíž každých $d-1$ řádků matice $\mathbf{D}$ je lineárně nezávislých. Navíc podle Poznámky 1.4 existuje slovo $\mathbf{w}\in\mathcal{C}$ s váhou rovnou d, tedy $\mathbf{w}\,\mathbf{D}=\mathbf{0}$. Tím máme dokázáno, že d řádků matice $\mathbf{D}$ (právě těch, které odpovídají nenulovým souřadnicím ve slově $\mathbf{w}$) je lineárně závislých.

Naopak předpokládejme, že matice $\mathbf{D}$ obsahuje d lineárně závislých řádků a každých $d-1$ řádků matice $\mathbf{D}$ je lineárně nezávislých. Potom existuje slovo $\mathbf{w}$ váhy

d, pro něž $\mathbf{w}\,\mathbf{D} = \mathbf{0}$. Z definice kontrolní matice plyne, že $\mathbf{w} \in \mathcal{C}$, tedy $d(\mathcal{C}) \leq d$. Pokud je $wt(\mathbf{v}) < d$ pro nenulové slovo $\mathbf{v} \in \mathbb{Z}_2^n$, pak $\mathbf{v}\,\mathbf{D} \neq \mathbf{0}$, neboť žádných $d-1$ řádků matice $\mathbf{D}$ není lineárně závislých. Proto $d(\mathcal{C}) = d$. □

Definice. Mějme lineární kód $\mathcal{C}$ délky n. Řekneme, že kód $\mathcal{C}$ *dokáže odhalit t chyb*, pokud pro každé slovo $\mathbf{v} \in \mathcal{C}$ a pro každé nenulové slovo $\mathbf{e} \in \mathbb{Z}_2^n$ splňující podmínku $wt(\mathbf{e}) \leq t$ platí, že slovo $\mathbf{v} + \mathbf{e}$ neleží v kódu $\mathcal{C}$. Řekneme, že kód $\mathcal{C}$ *dokáže opravit t chyb*, pokud pro všechna navzájem různá slova $\mathbf{v}, \mathbf{w} \in \mathcal{C}$ a pro každé $\mathbf{e} \in \mathbb{Z}_2^n$ splňující podmínku $wt(\mathbf{e}) \leq t$ platí, že $d(\mathbf{v}, \mathbf{v}+\mathbf{e}) < d(\mathbf{v}+\mathbf{e}, \mathbf{w})$.

Symbol $\lfloor x \rfloor$ značí pro každé reálné číslo x jeho celou část, tj. $\lfloor x \rfloor \in \mathbb{Z}$ a $x - \lfloor x \rfloor \in \langle 0, 1)$.

Věta 1.6. *Mějme lineární kód $\mathcal{C}$ délky n a vzdálenosti d. Pak $\mathcal{C}$ dokáže odhalit $d-1$ chyb a opravit $\left\lfloor \frac{d-1}{2} \right\rfloor$ chyb. Navíc $\mathcal{C}$ nedokáže odhalit d chyb a opravit $\left\lfloor \frac{d-1}{2} \right\rfloor + 1$ chyb.*

Důkaz. Buď $\mathbf{e} \in \mathbb{Z}_2^n$ nenulové slovo váhy $wt(\mathbf{e}) \leq d-1$. Potom pro každé slovo $\mathbf{v} \in \mathcal{C}$ platí, že $d(\mathbf{v}+\mathbf{e}, \mathbf{v}) = wt(\mathbf{v}+\mathbf{v}+\mathbf{e}) = wt(\mathbf{e}) \leq d-1$. Protože minimální vzdálenost dvou různých slov kódu $\mathcal{C}$ je rovna d, slovo $\mathbf{v}+\mathbf{e}$ neleží v $\mathcal{C}$, a kód tudíž dokáže odhalit $d-1$ chyb. Protože $d(\mathcal{C}) = d$, existuje slovo $\mathbf{e} \in \mathcal{C}$ váhy $wt(\mathbf{e}) = d$. Zřejmě $\mathbf{0} \in \mathcal{C}$, a $d(\mathbf{0}, \mathbf{0}+\mathbf{e}) = d$, tedy kód nedokáže odhalit d chyb.

Vezměme nyní libovolné slovo $\mathbf{e} \in \mathbb{Z}_2^n$ váhy $wt(\mathbf{e}) \leq \left\lfloor \frac{d-1}{2} \right\rfloor \leq \frac{d-1}{2}$. To znamená, že $2wt(\mathbf{e}) + 1 \leq d$. Nechť $\mathbf{v}, \mathbf{w} \in \mathcal{C}$ jsou dvě různá slova. Potom $d \leq d(\mathbf{v}, \mathbf{w}) \leq d(\mathbf{v}, \mathbf{v}+\mathbf{e}) + d(\mathbf{v}+\mathbf{e}, \mathbf{w})$ podle Poznámky 1.3(f) a platí, že

$$d(\mathbf{v}, \mathbf{v}+\mathbf{e}) + d(\mathbf{v}+\mathbf{e}, \mathbf{w}) \geq d \geq 2 \cdot wt(\mathbf{e}) + 1 = 2 \cdot d(\mathbf{v}, \mathbf{v}+\mathbf{e}) + 1 > 2 \cdot d(\mathbf{v}, \mathbf{v}+\mathbf{e}).$$

Odtud už odečtením hodnoty $d(\mathbf{v}, \mathbf{v}+\mathbf{e})$ od obou krajních stran nerovnosti dostáváme, že $d(\mathbf{v}+\mathbf{e}, \mathbf{w}) > d(\mathbf{v}, \mathbf{v}+\mathbf{e})$, tedy lineární kód $\mathcal{C}$ dokáže opravit $\left\lfloor \frac{d-1}{2} \right\rfloor$ chyb.

Pro každou podmnožinu $P \subset \{1, 2, \ldots, n\}$ označme $e_1 e_2 \ldots e_n = \mathbf{e}_P \in \mathbb{Z}_2^n$ slovo, které má hodnotu $e_i = 1$ právě na souřadnicích $i \in P$ a jinde nulu. Zřejmě $wt(\mathbf{e}_P) = |P|$. Nyní zvolme nenulové slovo $\mathbf{v} \in \mathcal{C}$ váhy $wt(\mathbf{v}) = d$, jehož existenci nám zaručuje Poznámka 1.4 a označme $I = \{i |\ v_i = 1\}$ množinu všech souřadnic slova $\mathbf{v}$ rovných jedné. Potom $|I| = d$. Zvolme dále libovolnou podmnožinu J množiny I o $\left\lfloor \frac{d-1}{2} \right\rfloor + 1$ prvcích. Všimněme si, že $|J| > |I \setminus J|$. Konečně definujme slovo $\mathbf{e} = \mathbf{e}_J$. Nyní $d(\mathbf{0}, \mathbf{0}+\mathbf{e}) = wt(\mathbf{e}) = |J|$ a $d(\mathbf{0}+\mathbf{e}, \mathbf{v}) = wt(\mathbf{e}+\mathbf{v}) = wt(\mathbf{e}_{I \setminus J}) = |I \setminus J|$. Tím jsme dokázali, že $d(\mathbf{0}, \mathbf{0}+\mathbf{e}) > d(\mathbf{0}+\mathbf{e}, \mathbf{v})$ pro slova $\mathbf{0}, \mathbf{v} \in \mathcal{C}$ a $\mathbf{e} \in \mathbb{Z}_2^n$ váhy $wt(\mathbf{e}) = \left\lfloor \frac{d-1}{2} \right\rfloor + 1$, tedy kód $\mathcal{C}$ nedokáže opravit $\left\lfloor \frac{d-1}{2} \right\rfloor + 1$ chyb. □

Příklad. Hammingův kód délky $2^r - 1$ dimenze $2^r - r - 1$.

Nechť r je celé kladné číslo. Definujme matici typu $(2^r - 1, r)$

$$\mathbf{D}_r = \begin{pmatrix} 0 & \ldots & 0 & 0 & 1 \\ 0 & \ldots & 0 & 1 & 0 \\ 0 & \ldots & 0 & 1 & 1 \\ & \vdots & & & \\ 1 & \ldots & 1 & 1 & 0 \\ 1 & \ldots & 1 & 1 & 1 \end{pmatrix},$$

která na i-tém řádku obsahuje právě číslo $i < 2^r$ v binárním zápisu délky r. Snadno nahlédneme, že $h(\mathbf{D}_r) = r$ (například proto, že řádky příslušející číslu 2^i tvoří kanonickou bázi prostoru $\mathbb{Z}_2^r$). Navíc žádné dva řádky matice $\mathbf{D}_r$ nejsou lineárně závislé a naopak ke každými dvěma různým řádkům najdme v matici řádek (právě jejich součet), který je na nich lineárně závislý. Množinu všech řešení homogení soustavy rovnic s maticí $\mathbf{D}_r^{\mathsf{T}}$ označme $\mathcal{C}_r$. Zřejmě se jedná o lineární kód délky $2^r - 1$ a dimenze $2^r - 1 - h(\mathbf{D}_r^{\mathsf{T}}) = 2^r - r - 1$ s kontrolní maticí $\mathbf{D}_r^{\mathsf{T}}$ (tzv. Hammingův kód délky $2^r - 1$ dimenze $2^r - r - 1$). Podle Věty 1.5 je $d(\mathcal{C}_r) = 3$ a podle Věty 1.6 tudíž kód $\mathcal{C}_r$ dokáže odhalit nejvýše dvě chyby a opravit nejvýše jednu chybu.

Buď $\mathbf{v} \in$ přijaté slovo. Pokud $\mathbf{v}\,\mathbf{D}_r = \mathbf{0}$, jde samořejmě o kódové slovo. Jestliže $\mathbf{v}\,\mathbf{D}_r \neq \mathbf{0}$, došlo při přenosu k chybě. Předpokládáme, že došlo právě k jedné chybě. Protože matice $\mathbf{D}_r$ obsahuje na řádcích všechna nenulová slova $\mathbb{Z}_2^r$, existuje $i < 2^r$, pro něž $\mathbf{v}\,\mathbf{D}_r = \mathbf{e}_i\mathbf{D}_r$ (tedy $\mathbf{v}\,\mathbf{D}_r$ je právě i-tý řádek matice $\mathbf{D}_r$) a dále $(\mathbf{v} + \mathbf{e}_i)\mathbf{D}_r = \mathbf{v}\,\mathbf{D}_r + \mathbf{e}_i\mathbf{D}_r = \mathbf{0}$. To jednak znamená, že $\mathbf{v}\,\mathbf{D}_r$ je binární zápis čísla i, a také, že změníme-li (zleva) i-tou souřadnici slova $\mathbf{v}$, dostaneme kódové slovo $\mathbf{v} + \mathbf{e}_i$. Tedy slovo $\mathbf{v}\,\mathbf{D}_r$ udává v binárním zápisu číslo pozice, na níž došlo při přenosu k chybě. Zdůrazněme, že náš kód dokáže opravit jen jednu chybu a v případě, kdy dojde při přenosu k více chybám, jedna oprava sice změní přijaté slovo na slovo kódové, nepůjde ovšem o slovo, které bylo vysláno.

Prohlédněme si to na příkladě Hammingova kódu délky $7 = 2^3 - 1$ dimenze $4 = 2^3 - 3 - 1$:

$$\mathbf{D}_3 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

Generující maticí kódu $\mathcal{C}_r$ je například matice:

$$\mathbf{C}_3 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Pokud jsme kupříkladu přijali slovo 1101011, pak $1101011 \cdot \mathbf{D}_r = 110$. Binárnímu zápisu 110 odpovídá číslo 6, změňme tedy šestou cifru (z leva) ve slově 1101011 a dostaneme slovo 1101001, které už je kódovým slovem.

2. Bilineární a kvadratické formy

Definice. Nechť V je vektorový prostor nad tělesem T. Řekneme, že zobrazení $f : V \times V \to T$ je *bilineární forma*, platí-li pro všechny vektory $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ a skaláry $a, b \in T$ podmínky:

(1) $f(a \cdot \mathbf{u} + b \cdot \mathbf{v}, \mathbf{w}) = a \cdot f(\mathbf{u}, \mathbf{w}) + b \cdot f(\mathbf{v}, \mathbf{w})$,
(2) $f(\mathbf{w}, a \cdot \mathbf{u} + b \cdot \mathbf{v}) = a \cdot f(\mathbf{w}, \mathbf{u}) + b \cdot f(\mathbf{w}, \mathbf{v})$.

Poznámka 2.1. *Nechť V je vektorový prostor nad tělesem T a nechť f je zobrazení $f : V \times V \to T$. Definujme pro každý vektor $\mathbf{v} \in V$ zobrazení $f(\mathbf{v}, -) : V \to T$,* *které vektoru* $\mathbf{x} \in V$ *přiřadí hodnotu* $f(\mathbf{v}, \mathbf{x})$ *a obdobně definujme zobrazení* $f(-, \mathbf{v}) : V \to T$ *přiřazující vektoru* $\mathbf{x} \in V$ *hodnotu* $f(\mathbf{x}, \mathbf{v})$. *Pak je* f *bilineární forma právě tehdy, když* $f(\mathbf{v}, -)$ *i* $f(-, \mathbf{v})$ *jsou lineární formy pro všechny vektory* $\mathbf{v} \in V$.

Důkaz. Je-li f bilineární forma, a $\mathbf{v} \in V$ libovolný, pak bezprostředně z bodu (2) definice dostávám, že $f(\mathbf{v}, -)$ je lineární forma a podobně z podmínka (1) definice říká, že $f(-, \mathbf{v})$ je lineární forma.

Obráceně, z předpokladu, že $f(\mathbf{v}, -)$ je lineární forma pro všechna $\mathbf{v} \in V$ plyne druhá podmínka definice bilineární formy a symetricky z linearity $f(-, \mathbf{v})$ dostáváne první podmínku této definice. □

Příklad. 0) Zobrazení $0 : V \times V \to \mathbf{T}$ pro libovolný vektorový prostor nad tělesem T, které každé dvojici vektorů přiřadí nulu, je (tzv. *nulová*) bilineární forma.

1) Zobrazení $f : \mathbf{R}^3 \times \mathbf{R}^3 \to \mathbf{R}$ definované pro každou dvojici vektorů (x_1, x_2, x_3), $(y_1, y_2, y_3) \in \mathbf{R}^3$ předpisem $f((x_1, x_2, x_3), (y_1, y_2, y_3)) = 2x_1y_1 + 3x_1y_2 - x_1y_3 - 2x_3y_2$ je bilineární forma.

2) Vezměme nějakou čtvercovou matici A stupně n nad tělesem T. Pak zobrazení $g : T^n \times T^n \to T$ určené předpisem $g(\mathbf{v}, \mathbf{w}) = \mathbf{v}\, A\, \mathbf{w}^{\mathrm{T}}$ je bilineární formou.

3) Nechť $a, b \in \mathbf{R}$ a p, q jsou dva reálné polynomy. Potom zobrazení $H(p, q) = p(a) \cdot q(b)$ tvoří bilineární formu na (reálném vektorovém) prostoru všech reálných polynomů.

4) Buď $a < b$ dvě reálná čísla a $\mathbb{C}_0(\langle a, b\rangle)$ vektorový prostor všech spojitých reálných funkcí na intervalu $\langle a, b\rangle$. Pak zobrazení $I_{ab} : \mathbb{C}_0(\langle a, b\rangle) \times \mathbb{C}_0(\langle a, b\rangle) \to \mathbf{R}$ dané předpisem $I_{ab}(f, g) = \int_a^b fg$ je bilineární formou.

Definice. Nechť je V konečně dimenzionální vektorový prostor nad tělesem T, $(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n)$ jeho báze a $f : V \times V \to T$ bilineární forma. Matici $[f]_{(\mathbf{u}_i)} = (a_{ij})$ nazveme *maticí bilineárního zobrazení* f *vzhledem k bázi* $(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n)$, pokud $a_{ij} = f(\mathbf{u}_i, \mathbf{u}_j)$, kde $i, j \le n$.

Věta 2.2. *Buď* V *vektorový prostor nad tělesem* T, f *bilineární forma na* V, $(\mathbf{u}_1, \ldots, \mathbf{u}_n)$ *báze* V *a* $[f]_{(\mathbf{u}_i)}$ *její matice vzhledem k bázi* $(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n)$. *Potom* $f(\mathbf{v}, \mathbf{w}) = \{\mathbf{v}\}_{(\mathbf{u}_i)}[f]_{(\mathbf{u}_i)}\{\mathbf{w}\}^{\mathrm{T}}_{(\mathbf{u}_i)}$ *pro každé dva vektory* $\mathbf{v}, \mathbf{w} \in V$.

Důkaz. Nechť $\{\mathbf{v}\}_{(\mathbf{u}_i)} = (a_1, a_2, \ldots, a_n)$ a $\{\mathbf{w}\}_{(\mathbf{u}_i)} = (b_1, b_2, \ldots, b_n)$, tedy $\mathbf{v} = \sum_{i=1}^n a_i\, \mathbf{u}_i$ a $\mathbf{w} = \sum_{j=1}^n b_j\, \mathbf{u}_j$. Potom podle definice bilineární formy dostáváme, že

$$f(\mathbf{v}, \mathbf{w}) = f(\sum_{i=1}^n a_i\, \mathbf{u}_i, \sum_{j=1}^n b_j\, \mathbf{u}_j) = \sum_{i=1}^n \sum_{j=1}^n f(a_i\, \mathbf{u}_i, b_j\, \mathbf{u}_j) = \sum_{i=1}^n \sum_{j=1}^n a_i \cdot b_j \cdot f(\mathbf{u}_i, \mathbf{u}_j).$$

Nyní už snadno nahlédneme, že příslušný maticový součin nám dá stejný výsledek, tedy že $f(\mathbf{v}, \mathbf{w}) = \{\mathbf{v}\}_{(\mathbf{u}_i)}[f]_{(\mathbf{u}_i)}\{\mathbf{w}\}^{\mathrm{T}}_{(\mathbf{u}_i)}$. □

Věta 2.3. *Mějme vektorový prostor* V *konečné dimenze nad tělesem* T *a nějakou bilineární formu* $f : V \times V \to T$. *Nechť* B *a* C *jsou dvě báze prostoru* V *a* $[\mathrm{Id}]_{CB}$ *matice přechodu od báze* B *k bázi* C. *Potom* $[f]_C = [\mathrm{Id}]^{\mathrm{T}}_{CB}[f]_B[\mathrm{Id}]_{CB}$.

Důkaz. Podle Věty 2.2 platí pro každé dva vektory $\mathbf{v}, \mathbf{w} \in V$, že

$$f(\mathbf{v}, \mathbf{w}) = \{\mathbf{v}\}_B[f]_B\{\mathbf{w}\}^{\mathrm{T}}_B = \{\mathbf{v}\}_C[f]_C\{\mathbf{w}\}^{\mathrm{T}}_C.$$

Připomeňme, že $\{\mathbf{w}\}^{\mathrm{T}}_B = [\mathrm{Id}]_{CB}\{\mathbf{w}\}^{\mathrm{T}}_C$ a $\{\mathbf{v}\}_B = \{\mathbf{v}\}_C[\mathrm{Id}]^{\mathrm{T}}_{CB}$. Tak dostáváme pro každé dva vektory $\mathbf{v}, \mathbf{w} \in V$ rovnost

$$\{\mathbf{v}\}_C[f]_C\{\mathbf{w}\}^{\mathrm{T}}_C = \{\mathbf{v}\}_C[\mathrm{Id}]^{\mathrm{T}}_{CB}[f]_B[\mathrm{Id}]_{CB}\{\mathbf{w}\}^{\mathrm{T}}_C.$$

Budeme-li za $\mathbf{v}$ a $\mathbf{w}$ volit vektory báze C, pak souřadnicové vektory $\{\mathbf{v}\}_C$ a $\{\mathbf{w}\}_C$ budou tvořit příslušné vektory $\mathbf{e}_i$ a $\mathbf{e}_j$ kanonické báze prostoru T^n. Víme-li, že $\mathbf{e}_i \cdot (a_{kl}) \cdot \mathbf{e}_j = a_{ij}$ pro libovolnou čtvercovou matici (a_{kl}) stupně n a

$$\mathbf{e}_i[f]_C\mathbf{e}_j = \mathbf{e}_i([\mathrm{Id}]_{CB}^{\mathsf{T}}[f]_B[\mathrm{Id}]_{CB})\mathbf{e}_j,$$

pak se matice $[f]_C$ a $[\mathrm{Id}]_{CB}^{\mathsf{T}}[f]_B[\mathrm{Id}]_{CB}$ shodují, což jsme měli dokázat. □

Poznámka 2.4. *Pro každou bázi B vektorového prostoru V dimenze n a každou čtvercovou matici $\mathbf{A}$ stupně n existuje právě jedna bilineární forma, pro níž $\mathbf{A} = [f]_B$.*

Důkaz. Definujeme-li $f(\mathbf{u},\mathbf{v}) = \{\mathbf{u}\}_B\mathbf{A}\{\mathbf{v}\}_B^{\mathsf{T}}$, pak z definice vidíme, že je f bilineární forma s maticí $[f]_B = \mathbf{A}$. Z Věty 2.2 potom plyne jednoznačnost. □

Poznámka 2.5. *Označme $B(V)$ množinu všech bilineárních forem na vektorovém prostoru V nad tělesem T. Buď $f, g \in B(V)$ a $t \in T$. Definujme na $B(V)$ násobení skalárem a sčítání následujícícm způsobem:*

$$(t \cdot f)(\mathbf{v},\mathbf{w}) = t \cdot (f(\mathbf{v},\mathbf{w})), \quad (f+g)(\mathbf{v},\mathbf{w}) = f(\mathbf{v},\mathbf{w}) + g(\mathbf{v},\mathbf{w})$$

pro všechna $\mathbf{v},\mathbf{w} \in V$. Potom množina všech bilineárních forem $B(V)$ spolu se zavedeným násobením skalárem a sčítáním tvoří vektorový prostor nad tělesem T. Je-li prostor V konečné dimenze $n = \dim(V)$, je zobrazení $f \to [f]_B$ pro každou bázi prostoru V izomorfismem $B(V)$ a vektorového prostoru všech čtvercových matic stupně n nad tělesem T.

Důkaz. Postupujeme podle definice vektorového prostoru. Zvolme libovolně $f, g, h \in B(V)$ a $r, s \in T$. Nejprve si všimněme, že $f + g$ a af jsou podle 2.1 bilineární formy, protože zobrazení $\mathbf{u} \to (f+g)(\mathbf{v},\mathbf{u})$, $\mathbf{u} \to (f+g)(\mathbf{u},\mathbf{v})$, $\mathbf{u} \to (af)(\mathbf{v},\mathbf{u})$ a $\mathbf{u} \to (af)(\mathbf{u},\mathbf{v})$ jsou lineární formy

Z komutativity a asociativity počítání v tělese T, máme pro všechna $\mathbf{v},\mathbf{w} \in V$

$$(f+g)(\mathbf{v},\mathbf{w}) = f(\mathbf{v},\mathbf{w}) + g(\mathbf{v},\mathbf{w}) = g(\mathbf{v},\mathbf{w}) + f(\mathbf{v},\mathbf{w}) = (g+f)(\mathbf{v},\mathbf{w}),$$

$$(f+(g+h))(\mathbf{v},\mathbf{w}) = f(\mathbf{v},\mathbf{w}) + g(\mathbf{v},\mathbf{w}) + h(\mathbf{v},\mathbf{w}) = ((f+g)+h)(\mathbf{v},\mathbf{w}).$$

Snadno uvážíme, že nulová bilineární forma 0 (tj. $0(\mathbf{v},\mathbf{w}) = 0$) je neutrální vzhledem ke sčítání, t.j. $f + 0 = f$ pro všechna $f \in B(V)$. Stejně přímočaře využijeme distributivitu a asociativitu počítání v tělese, abychom ověřili, že

$$(r\cdot(f+g))(\mathbf{v},\mathbf{w}) = r\cdot(f(\mathbf{v},\mathbf{w})+g(\mathbf{v},\mathbf{w})) = r\cdot f(\mathbf{v},\mathbf{w})+r\cdot g(\mathbf{v},\mathbf{w}) = (rf+rg)(\mathbf{v},\mathbf{w}),$$

$$((r+s)\cdot f)(\mathbf{v},\mathbf{w}) = (r+s)\cdot f(\mathbf{v},\mathbf{w})) = r\cdot f(\mathbf{v},\mathbf{w}) + s\cdot f(\mathbf{v},\mathbf{w}) = (rf+sf)(\mathbf{v},\mathbf{w}),$$

$$((r\cdot s)\cdot f)(\mathbf{v},\mathbf{w}) = (r\cdot s)\cdot f(\mathbf{v},\mathbf{w})) = r\cdot(s\cdot f(\mathbf{v},\mathbf{w})) = (r\cdot(s\cdot f))(\mathbf{v},\mathbf{w}).$$

pro každé $\mathbf{v},\mathbf{w} \in V$. Konečně podmínka $1 \cdot f = f$ platí zjevně.

Je-li $n = \dim(V)$, označme $M_n(T)$ vektorový prostor čtvercových matic stupně n nad tělesem T. Buď B báze prostoru V a definujeme zobrazení $\varphi : B(V) \to M_n(T)$ předpisem $\varphi(f) = [\mathrm{Id}]_B$. Díky 2.4 je φ zobrazení na a podle 2.2 je prosté. Z 2.2 a definice operací na $B(V)$ navíc pro každé $f, g \in B(V)$ a $t \in T$ plyne, že $[f+g]_B = [f]_B + [g]_B$ a $[t \cdot f]_B = t \cdot [f]_B$, tedy φ je izomorfismus. □

Definice. Řekneme, že je bilineární formu f na vektorovém prostoru V *symetrická*, jestliže $f(\mathbf{v},\mathbf{w}) = f(\mathbf{w},\mathbf{v})$ pro všechna $\mathbf{v},\mathbf{w} \in V$, a *antisymetrická*, jestliže $f(\mathbf{v},\mathbf{w}) = -f(\mathbf{w},\mathbf{v})$ pro všechna $\mathbf{v},\mathbf{w} \in V$.

Poznámka 2.6. *Pro bilineární formu f na vektorovém prostoru V konečné dimenze n jsou následující tvrzení ekvivalentní:*

(1) *f je (anti)symetrická,*
(2) *existuje taková báze B prostoru V, že $[f]_B$ je (anti)symetrická matice,*
(3) *pro každou bázi B prostoru V je $[f]_B$ je (anti)symetrická matice.*

Důkaz. (1)⇒(3) Je-li symetrická (resp. antisymetrická) a $B = (\mathbf{b}_i)$ libovolná báze V, pak $f(\mathbf{b}_i, \mathbf{b}_j) = f(\mathbf{b}_j, \mathbf{b}_i)$ (resp. $f(\mathbf{b}_i, \mathbf{b}_j) = -f(\mathbf{b}_j, \mathbf{b}_i)$) pro všechna $i, j \leq n$, tedy podle definice je matice $[f]_B$ symetrická (resp. antisymetrická).

(3)⇒(2) Zjevné.

(2)⇒(1) Zvolme bázi B, pro níž je $[f]_B$ je symetrická (resp. antisymetrická) matice, potom pro libovolné $\mathbf{v}, \mathbf{w} \in V$ díky Větě 2.2 máme $f(\mathbf{v}, \mathbf{w}) = \{\mathbf{v}\}_B[f]_B\{\mathbf{w}\}_B^{\mathsf{T}} = (\{\mathbf{v}\}_B[f]_B\{\mathbf{w}\}_B^{\mathsf{T}})^{\mathsf{T}} = \{\mathbf{w}\}_B[f]_B^{\mathsf{T}}\{\mathbf{v}\}_B^{\mathsf{T}} = \{\mathbf{w}\}_B[f]_B\{\mathbf{v}\}_B^{\mathsf{T}} = f(\mathbf{w}, \mathbf{v})$ (resp. $f(\mathbf{v}, \mathbf{w}) = \{\mathbf{w}\}_B[f]_B^{\mathsf{T}}\{\mathbf{v}\}_B^{\mathsf{T}} = -\{\mathbf{w}\}_B[f]_B\{\mathbf{v}\}_B^{\mathsf{T}} = -f(\mathbf{w}, \mathbf{v})$) pro všechna $\mathbf{v}, \mathbf{w} \in V$, tedy f je symetrická (resp. antisymetrická). □

Poznámka 2.7. *Označme $BS(V)$ resp. $BA(V)$ množinu všech symetrických resp. antisymetrických bilineárních forem na prostoru V nad tělesem T. Potom $BS(V)$ i $BA(V)$ jsou podprostory vektorového prostoru všech bilineárních forem $B(V)$. Jestliže* $\mathrm{char}(T) \neq 2$, *pak $BS(V) \cap BA(V) = \{0\}$.*

Důkaz. Zvolme bázi B prostoru. Díky 2.5 máme $[f + g]_B = [f]_B + [g]_B$ a $[tf]_B = t[f]_B$ pro každé $f, g \in B(V)$ a $t \in T$, navíc $f \in BS(V)$, právě když je matice $[f]_B$ symetrická a $f \in BA(V)$, právě když je matice $[f]_B$ antisymetrická podle 2.6. Tedy stačí uvážit, že součet a násobek skalárem (anti)symetrických matic je opět (anti)symetrická matice, což zjevně platí.

Předpokládejme $f \in BS(V) \cap BA(V)$. Potom podle definice $f(\mathbf{v}, \mathbf{w}) = f(\mathbf{w}, \mathbf{v}) = -f(\mathbf{v}, \mathbf{w})$, tedy $f(\mathbf{v}, \mathbf{w}) + f(\mathbf{v}, \mathbf{w}) = 0$ pro každé $\mathbf{v}, \mathbf{w} \in V$. Jestliže $\mathrm{char}(T) \neq 2$, pak $f = 0$. □

Věta 2.8. *Je-li V vektorový prostor nad tělesem T a* $\mathrm{char}(T) \neq 2$, *potom lze každou bilineární formu f na V jednoznačně zapsat ve tvaru $f = f_s + f_a$, kde f_s je symetrická a f_a antisymetrická bilineární forma.*

Důkaz. Položme $f_s(\mathbf{u}, \mathbf{v}) = \frac{1}{2}(f(\mathbf{u}, \mathbf{v}) + f(\mathbf{v}, \mathbf{u}))$ a $f_a(\mathbf{u}, \mathbf{v}) = \frac{1}{2}(f(\mathbf{u}, \mathbf{v}) - f(\mathbf{v}, \mathbf{u}))$. Zřejmě $f = f_s + f_a$ a a f_s je symetrická a f_a antisymetrická bilineární forma. Mějme nyní nějaký jiný rozklad bilineární formy $f = g_s + g_a$ na symetrickou a antisymetrickou část. Pak $f_s + f_a = g_s + g_a$, a proto $f_s - g_s = g_a - f_a$. Podle Poznámky 2.7 je $f_s - g_s \in BS(V)$ a $g_a - f_a \in BA(V)$, a proto a $f_s - g_s = \mathbf{0} = g_a - f_a$. Tudíž $f_s = g_s$ a $f_a = g_a$, čímž jsme dokázali jednoznačnost volby rozkladu f na symetrickou a antisymetrickou část. □

Příklad. Nad libovolným tělesem T charakteristiky 2 platí, že $a = -a$ pro každé $a \in T$, což znamená, že bilineární forma je nad takovým tělesem symetrická právě tehdy, když je antisymetrická. Vezmeme-li tedy bilineární formu g na vektorovém prostoru $\mathbb{Z}_2^2$ nad tělesem $\mathbb{Z}_2$ danou předpisem $g((x_1, x_2), (y_1, y_2)) = x_1 y_2$ zřejmě nejde o symetrickou (a proto ani antisymetrickou) formu. Protože platí, že

$$BS(\mathbb{Z}_2^2) = BA(\mathbb{Z}_2^2) = BS(\mathbb{Z}_2^2) + BA(\mathbb{Z}_2^2) \neq \mathbb{Z}_2^2,$$

nelze bilineární formu g rozložit na symetrickou a antisymetrickou část.

Příklad. Buď f bilineární forma na vektorovém prostoru $\mathbb{Z}_5^3$ nad tělesem $\mathbb{Z}_5$ a $[f]_B = \begin{pmatrix} 1 & 2 & 4 \\ 2 & 0 & 3 \\ 2 & 1 & 1 \end{pmatrix}$ pro nějakou bázi B prostoru $\mathbb{Z}_5^3$. Uvědomíme-li si , že přiřazení $f \to [f]_B$ je podle Poznámky 2.5 izomorfismus, můžeme předpis obsažený v důkazu Věty 2.8 pro rozklad bilineární formy na symetrickou a antisymetrickou část snadno vyjádřit pomocí matic:

$$[f_s]_B = \frac{1}{2}([f]_B + [f]_B^{\mathtt{T}}) = \frac{1}{2} \cdot \left(\begin{pmatrix} 1 & 2 & 4 \\ 2 & 0 & 3 \\ 2 & 1 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 2 & 2 \\ 2 & 0 & 1 \\ 4 & 3 & 1 \end{pmatrix} \right) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 0 & 2 \\ 3 & 2 & 1 \end{pmatrix}$$

$$[f_a]_B = \frac{1}{2}([f]_B - [f]_B^{\mathtt{T}}) = \frac{1}{2} \cdot \left(\begin{pmatrix} 1 & 2 & 4 \\ 2 & 0 & 3 \\ 2 & 1 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 2 & 2 \\ 2 & 0 & 1 \\ 4 & 3 & 1 \end{pmatrix} \right) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 4 & 4 & 0 \end{pmatrix}$$

Definice. Buď f bilineární forma na vektorovém prostoru V. Řekneme, že báze B prostoru V je *polární bází* bilineární formy f, jestliže $f(\mathbf{u}, \mathbf{v}) = 0$ pro všechna $\mathbf{u}, \mathbf{v} \in B$, $\mathbf{u} \neq \mathbf{v}$.

Poznámka 2.9. *B je polární báze bilineární formy f na konečně dimenzionálním prostoru, právě když je $[f]_B$ diagonální matice.*

Důkaz. Plyne okamžitě z definice. □

Jsou-li a, b dva prvky obecného tělesa a $b \neq 0$, budeme místo $a \cdot b^{-1}$ psát $\frac{a}{b}$.

Věta 2.10. *Buď f nenulová symetrická bilineární forma na vektorovém prostoru V nad tělesem T. Jestliže* $\mathrm{char}(T) \neq 2$, *existuje vektor $\mathbf{u} \in V$, pro nějž $f(\mathbf{u}, \mathbf{u}) \neq 0$.*

Důkaz. Protože f je nenulová symetrická bilineární forma, existují vektory $\mathbf{v}, \mathbf{w} \in V$, pro něž $f(\mathbf{v}, \mathbf{w}) \neq 0$. Jakmile $f(\mathbf{v}, \mathbf{v}) \neq 0$ nebo $f(\mathbf{w}, \mathbf{w}) \neq 0$ jsme hotovi. V opačném případě $f(\mathbf{v}+\mathbf{w}, \mathbf{v}+\mathbf{w}) = f(\mathbf{v}, \mathbf{v}) + f(\mathbf{v}, \mathbf{w}) + f(\mathbf{w}, \mathbf{v}) + f(\mathbf{w}, \mathbf{w}) = 2f(\mathbf{v}, \mathbf{w}) \neq 0$ neboť $\mathrm{char}(T) \neq 2$. □

Věta 2.11. *Nechť V je vektorový prostor nad tělesem T konečné dimenze a nechť f je bilineární forma na V. Jestliže* $\mathrm{char}(T) \neq 2$, *pak f je symetrická právě tehdy, když existuje nějaká polární báze f.*

Důkaz. ($\Rightarrow$) Přímou implikaci budeme dokazovat indukcí podle $n = \dim(V)$, přičemž využijeme Poznámku 2.9. Jestliže $\dim(V) = 1$, není co dokazovat, protože každá čtvercová matice stupně 1 je diagonální (tj. triviálně splňuje podmínku, že má všude mimo diagonálu nuly).

Předpokládejme, že tvrzení platí pro každou symetrickou bilineární formu na libovolném prostoru dimenze n a dokažme tvrzení pro prostory dimenze $n+1$. Pokud je f nulová, je každá báze V polární vzhledem k f. Je-li f nenulová symetrická bilineární forma na prostoru V dimenze $n+1$, pak podle Věty 2.10 existuje takový vektor $\mathbf{u}_0$, že $f(\mathbf{u}_0, \mathbf{u}_0) \neq 0$. Vektor můžeme doplnit na bázi $\mathbf{u}_0, \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n$ celého vektorového prostoru V. Nyní položme $\mathbf{w}_i = \mathbf{v}_i - \frac{f(\mathbf{u}_0, \mathbf{v}_i)}{f(\mathbf{u}_0, \mathbf{u}_0)} \mathbf{u}_0$ pro každé $i = 1, 2, \dots, n$ a označme $W = \langle \mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_n \rangle$. Nyní zřejmě

$$f(\mathbf{u}_0, \mathbf{w}_i) = f(\mathbf{u}_0, \mathbf{v}_i - \frac{f(\mathbf{u}_0, \mathbf{v}_i)}{f(\mathbf{u}_0, \mathbf{u}_0)} \mathbf{u}_0) = f(\mathbf{u}_0, \mathbf{v}_i) - \frac{f(\mathbf{u}_0, \mathbf{v}_i)}{f(\mathbf{u}_0, \mathbf{u}_0)} f(\mathbf{u}_0, \mathbf{u}_0) = 0$$

pro každé $i = 1, 2, \dots, n$, a proto $f(\mathbf{u}_0, \mathbf{w}) = 0$ pro každé $\mathbf{w} \in W$. Protože f omezená na podprostor W tvoří rovněž symetrickou bilineární formu a protože $\dim W = n$, existuje podle indukčního předpokladu nějaká polární báze W vzhledem k f, označme ji $(\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n)$. Tedy $f(\mathbf{u}_i, \mathbf{u}_j) = 0$ pro všechna $i \neq j$, $i, j = 1, 2, \dots, n$. Navíc víme, že $f(\mathbf{u}_0, \mathbf{u}_i) = f(\mathbf{u}_i, \mathbf{u}_0) = 0$ pro $i = 1, 2, \dots, n$, tedy jsme našli bázi $(\mathbf{u}_0, \mathbf{u}_1, \dots, \mathbf{u}_n)$ prostoru V polární vzhledem k f.

($\Leftarrow$) Protože je matice f vzhledem k polární bázi zjevně symetrická, je f podle Poznámky 2.6 symetrickou bilineární formou. □

Příklad (Výpočet polární báze)**.** (1) Mějme f symetrickou bilineární formu na prostoru $\mathbb{Z}_7^3$ danou předpisem $f((x_1, x_2, x_3), (y_1, y_2, y_3)) = 2x_1y_1 + x_1y_3 + x_3y_1 + 2x_2y_3 + 2x_3y_2$. Matice $[f]_{K_3} = \begin{pmatrix} 2 & 0 & 1 \\ 0 & 0 & 2 \\ 1 & 2 & 0 \end{pmatrix}$ je maticí bilineární formy f vzhledem ke kanonické bázi K_3. Symetrickou elementární úpravou nazývejme dvojici elemntárních úprav stejného typu na řádky a zároveň jim odpovídající sloupce matice. Tedy vyměníme-li řádky i a j, vyměníme zároveň i sloupce i a j, jestliže i-tý řádek vynásobíme nenulovým skalárem a, zároveň vynásobíme i i-tý sloupec týmž skalárem a konečně, pokud přičteme k i-tému řádku a-násobek j-tého řádku, přičteme zároveň k i-tému sloupci a-násobek j-tého sloupce.

Uvědomíme-li si, že matice bilineární formy upravená symetrickými úpravami, je maticí téže bilineární formy vzhledem k jisté nové bázi, zkusíme matici upravovat tak, aby postupně odpovídala maticím f vzhledem k bázím, které se vyskytují v důkazu Věty 2.11. Nejprve symetrickými elementárními úpravami vynulujeme všechny hodnoty na prvním řádku a prvním sloupci matice $[f]_{K_3}$ kromě diagonální pozice $(1, 1)$. Potom postupně nulujeme hodnoty mimo diagonálu v dalších řádcích a sloupcích. Narazíme-li na diagonále (na pozici (i, i)) na hodnotu 0, obdobně jako je tomu ve Větě 2.10, kterou používáme v důkazu Věty 2.11, buď najdeme nenulovou hodnotu na pozici (j, j) pro $j > i$ a poté vyměněnou i-tého a j-tého řádku i sloupce dostaneme na pozici (i, i) nenulovou hodnotu nebo, neexistuje-li takový prvek diagonály, přičteme k i-tému řádku takový j-tý řádek, který má na místě i-té souřadnice nenulovou hodnotu a zároveň přičteme k i-tému sloupci j-tý sloupec. Postupně tak vytvoříme diagonální matici:

$$[f]_{K_3} = \begin{pmatrix} 2 & 0 & 1 \\ 0 & 0 & 2 \\ 1 & 2 & 0 \end{pmatrix} \sim_s \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 2 & 3 \end{pmatrix} \sim_s \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 2 \\ 0 & 2 & 0 \end{pmatrix} \sim_s \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Budeme-li zaznamenávat do matice provedené řádkové úpravy dostaneme podle Věty 2.3 matici $[\mathrm{Id}]_{BK_3}^{\mathsf{T}}$, kde B je báze vůči níž má f diagonální matici, kterou jsme získali výše uvedenými úpravami. Tedy

$$([f]_{K_3}|\mathbf{E}) = \left(\begin{array}{ccc|ccc} 2 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 1 & 0 \\ 1 & 2 & 0 & 0 & 0 & 1 \end{array}\right) \sim_s \left(\begin{array}{ccc|ccc} 2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 1 & 0 \\ 0 & 2 & 3 & 3 & 0 & 1 \end{array}\right) \sim_s$$

$$\sim_s \left(\begin{array}{ccc|ccc} 2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 3 & 2 & 3 & 0 & 1 \\ 0 & 2 & 0 & 0 & 1 & 0 \end{array}\right) \sim_s \left(\begin{array}{ccc|ccc} 2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 3 & 0 & 3 & 0 & 1 \\ 0 & 0 & 1 & 5 & 1 & 4 \end{array}\right) = ([f]_B|[\mathrm{Id}]_{BK_3}^{\mathsf{T}})$$

Dostali jsme matici přechodu od kanonické k polární bázi $[\mathrm{Id}]_{BK_3} = \begin{pmatrix} 1 & 3 & 5 \\ 0 & 0 & 1 \\ 0 & 1 & 4 \end{pmatrix}$, a proto je báze $((1,0,0),\ (3,0,1),\ (5,1,4))$ polární bází bilineární formy f.

To snadno ověříme zkouškou:

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

(2) Uvažujme symetrickou bilineární formu g na reálném vektorovém prostoru $\mathbb{R}^2$ s maticí $[g]_{K_2} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ vzhledem ke kanonické bázi K_2. Stejnou metodou jako v (1) najdeme její polární bázi. Všimněme si, že hodnota $g(\mathbf{e}_i, \mathbf{e}_i) = 0$ pro $i = 1, 2$, tedy nám při symetrických úvahách nestačí přehodit řádek a sloupec matice, nýbrž musíme přičíst druhý řádek i sloupec k prvnímu:

$$([g]_{K_2}|\mathbf{E}) = \left(\begin{array}{cc|cc} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right) \sim_s \left(\begin{array}{cc|cc} 2 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{array}\right) \sim_s \left(\begin{array}{cc|cc} 2 & 0 & 1 & 1 \\ 0 & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{array}\right).$$

Našli jsme tedy matici přechodu od kanonické bázi k polární, tedy hledanou polární bází je například posloupnost vektorů $((1,1), (-\frac{1}{2}, \frac{1}{2})$

Definice. Buď f bilineární forma na vektorovém prostoru V. *Levým* (resp. *pravým*) *vrcholem* bilineární formy f nazveme množinu $V_l(f) = \{\mathbf{u} \in V|\ \forall\, \mathbf{v} \in V : f(\mathbf{u}, \mathbf{v}) = 0\}$ (resp. $V_p(f) = \{\mathbf{u} \in V|\ \forall\, \mathbf{v} \in V : f(\mathbf{v}, \mathbf{u}) = 0\}$).

Poznámka 2.12. *Je-li f bilineární forma na vektorovém prostoru V, pak $V_l(f)$ a $V_p(f)$ tvoří podprostory prostoru V.*

Důkaz. Podle 2.1 jsou $f(-, \mathbf{v})$ a $f(\mathbf{v}, -)$ lineární formy, tedy jádra $\operatorname{Ker} f(-, \mathbf{v})$ i $\operatorname{Ker} f(\mathbf{v}, -)$ jsou podprostory prostoru V. Z definice vrcholů vidíme, že $V_l(f) = \bigcap_{\mathbf{v} \in V} \operatorname{Ker} f(-, \mathbf{v})$ a $V_p(f) = \bigcap_{\mathbf{v} \in V} \operatorname{Ker} f(\mathbf{v}, -)$, proto $V_l(f)$ a $V_p(f)$ jsou rovněž podprostory. □

Poznámka 2.13. *Mějme na konečně dimenzionálním vektorovém prostoru V mad tělesem T bilineární formu f a buď B báze V. Potom množina souřadnic vzhledem k bázi B vektorů levého vrcholu $\{\{\mathbf{u}\}_B|\ \mathbf{u} \in V_l(f)\}$ (resp. pravého vrcholu $\{\{\mathbf{u}\}_B|\ \mathbf{u} \in V_p(f)\}$) je rovna právě množině všech řešení homogenní soustavy rovnic s maticí $[f]_B^{\mathsf{T}}$ (resp. $[f]_B$).*

Důkaz. Položme $n = \dim V$ a $S_l = \{\mathbf{x} \in T^n|\ [f]_B^{\mathsf{T}} \cdot \mathbf{x}^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}}\}$. Jestliže $\mathbf{u} \in V_l(f)$, pak díky 2.2 máme $0 = f(\mathbf{u}, \mathbf{v}) = \{\mathbf{u}\}_B [f]_B \{\mathbf{v}\}_B^{\mathsf{T}}$ pro každé $\mathbf{v} \in V$, tedy transponujeme-li rovnost a omezíme-li se na vektory báze $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$, dostaneme

$$\mathbf{e}_i \cdot [f]_B^{\mathsf{T}} \cdot \{\mathbf{u}\}_B^{\mathsf{T}} = \{\mathbf{b}_i\}_B \cdot [f]_B^{\mathsf{T}} \cdot \{\mathbf{u}\}_B^{\mathsf{T}} = 0,$$

proto $[f]_B^{\mathsf{T}} \cdot \{\mathbf{u}\}_B^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}}$, tedy $\{\mathbf{u}\}_B \in S_l$. Vezmeme-li naopak vektor $\mathbf{u} \in V$, pro který $\{\mathbf{u}\}_B \in S_l$, pak pomocí 2.2 pro každé $a_1, \ldots, a_n \in T$ spočítáme, že

$$f(\mathbf{u}, \sum_{i=1}^{n} a_i \mathbf{b}_i) \sum_{i=1}^{n} \{\mathbf{b}_i\}_B \cdot [f]_B^{\mathsf{T}} \cdot \{\mathbf{u}\}_B^{\mathsf{T}} = \sum_{i=1}^{n} \mathbf{e}_i \cdot [f]_B^{\mathsf{T}} \cdot \{\mathbf{u}\}_B^{\mathsf{T}} = 0.$$

Tím jsme ověřili, že $f(\mathbf{u},\mathbf{v}) = 0$ pro každý vektor $\mathbf{v} \in V$.

Argument pro pravý vrchol je symetrický. □

Důsledek 2.14. *Je-li f bilineární forma na konečnědimenzionálním vektorovém prostoru V, pak* $\dim(V_l(f)) = \dim(V_p(f)) = \dim(V) - h([f]_B)$ *pro každou bázi B prostoru V.*

Definice. *Nulitou* $n(f)$ bilineární formy f na vektorovém prostoru V nazveme číslo $\dim(V_l(f))$. Jestliže $n(f) = 0$ mluvíme o *regulární* bilineární formě f.

Poznámka 2.15. *$V_l(f) = V_p(f)$ pro každou symetrickou bilineární formu f.*

Důkaz. Plyne okamžitě z definice. □

Definice. Buď f symetrická bilineární forma na vektorovém prostoru V. Pak podprostor $V(f) = V_l(f) = V_p(f)$ nazveme *vrcholem* symetrické bilineární formy f.

Věta 2.16. *Nechť f je symetrická bilineární forma na konečně dimenzionálním vektorovém prostoru V a B polární báze f. Právě všechny vektory $\mathbf{u} \in B$ splňující podmínku $f(\mathbf{u},\mathbf{u}) = 0$ tvoří bázi vrcholu $V(f)$.*

Důkaz. Označme $B = (\mathbf{u}_1, \mathbf{u}_2, \ldots \mathbf{u}_n)$ vektory polární báze V vzhledem k f. Zřejmě platí, že $f(\mathbf{u}_i, \mathbf{u}_j) = 0$ pro každé $i \neq j$. Pokud navíc $f(\mathbf{u}_i, \mathbf{u}_i) = 0$ pro nějaké $i \leq n$, leží vektor $\mathbf{u}_i$ ve vrcholu $V(f)$. Připomeňme, že nulita (tedy dimenze $V(f)$) je podle Poznámky 2.13 rovna hodnotě $n - h([f]_B)$ a dále si uvědomme, že hodnost diagonální matice $h([f]_B)$ je rovna právě počtu nenulových hodnot na diagonále, tedy naopak $n - h([f]_B)$ je počet nulových hodnot na diagonále matice $[f]_B$. Vezmeme-li všechny vektory $\mathbf{u}_i$, pro něž $f(\mathbf{u}_i, \mathbf{u}_i) = 0$ (tedy právě i-tá hodnota na diagonále matice $[f]_B$ je rovna nule), dostaneme $n - h([f]_B)$ lineárně nezávislých vektorů, které všechny leží ve vrcholu $V(f)$. Protože $\dim(V(f)) = n - h([f]_B)$ podle Poznámky 2.14, musí už nutně jít o bázi celého podprostoru $V(f)$. □

Definice. Mějme bilineární formu f na vektorovém prostoru V nad tělesem T. Zobrazení $f_2 : V \to T$ dané předpisem $f_2(\mathbf{v}) = f(\mathbf{v},\mathbf{v})$ pro každý vektor $\mathbf{v} \in V$ nazveme *kvadratickou formou* vytvořenou bilineární formou f.

Poznámka 2.17. *Pro každou antisymetrickou bilineární formu g nad tělesem T charakteristiky* $\mathrm{char}(T) \neq 2$ *je $g_2 = 0$.*

Důkaz. Protože $g(\mathbf{v},\mathbf{v}) = -g(\mathbf{v},\mathbf{v})$, je $g_2(\mathbf{v}) = g(\mathbf{v},\mathbf{v}) = 0$ pro každé $\mathbf{v} \in V$. □

Poznámka 2.18. *Buď f bilineární forma na vektorovém prostoru V nad tělesem T,* $\mathrm{char}(T) \neq 2$ *a buď $f = f_s + f_a$ rozklad na symetrickou a antisymetrickou část podle Věty 2.8. Pak* $f_s(\mathbf{v},\mathbf{w}) = \frac{1}{2}(f_2(\mathbf{v}+\mathbf{w}) - f_2(\mathbf{v}) - f_2(\mathbf{w}))$.

Důkaz. Protože $(f_s + f_a)_2 = (f_s)_2 + (f_a)_2 = (f_s)_2$ podle 2.17 můžeme bez újmy na obecnosti předpokládat, že $f = f_s$ je symetrická bilineární forma. Potom přímočaře počítáme

$$f_2(\mathbf{v}+\mathbf{w}) - f_2(\mathbf{v}) - f_2(\mathbf{w}) = f(\mathbf{v}+\mathbf{w}, \mathbf{v}+\mathbf{w}) - f(\mathbf{v},\mathbf{v}) - f(\mathbf{w},\mathbf{w}) =$$

$$= f(\mathbf{v},\mathbf{v}) + f(\mathbf{v},\mathbf{w}) + f(\mathbf{w},\mathbf{v}) + f(\mathbf{w},\mathbf{w}) - f(\mathbf{v},\mathbf{v}) - f(\mathbf{w},\mathbf{w}) = 2f(\mathbf{v},\mathbf{w}).$$

□

Věta 2.19. *Pro každou kvadratickou formu f_2 na vektorovém prostor nad tělesem chrakteristiky různé od 2 vytvořenou bilineární formou f existuje právě jedna symetrická bilineární forma g tak, že $f_2(\mathbf{u}) = g_2(\mathbf{u})$ pro všechna $\mathbf{u} \in V$. Přitom $g = f_s$.*

Důkaz. Z Poznámky 2.17 okamžitě plyne, že $f_2(\mathbf{u}) = f_s(\mathbf{u},\mathbf{u}) + f_a(\mathbf{u},\mathbf{u}) = f_s(\mathbf{u},\mathbf{u})$, tedy $f_2(\mathbf{u}) = (f_s)_2(\mathbf{u})$. Máme-li symetrickou bilineární formu g splňující podmínku, že $f_2(\mathbf{u}) = g_2(\mathbf{u})$, potom $g(\mathbf{v},\mathbf{w}) = g_s(\mathbf{v},\mathbf{w}) = \frac{1}{2}(g_2(\mathbf{v}+\mathbf{w}) - g_2(\mathbf{v}) - g_2(\mathbf{w})) = \frac{1}{2}(f_2(\mathbf{v}+\mathbf{w}) - f_2(\mathbf{v}) - f_2(\mathbf{w})) = f_s(\mathbf{v},\mathbf{w})$ podle Poznámky 2.18, čímž máme ověřenu jednoznačnost. □

Příklad. Uvažujme zobrazení $h_2 : \mathbf{R}^2 \to \mathbf{R}$ dané předpisem $h_2(x_1,x_2) = x_1^2 + 4x_1y_2 + 3x_2^2$. Uvědomíme si, že jde o kvadratickou formu. Protože můžeme dané zobrazení vyjádřit ve tvaru $h_2(x_1,x_2) = (x_1,x_2)\cdot\begin{pmatrix}1&2\\2&3\end{pmatrix}\cdot\begin{pmatrix}x_1\\x_2\end{pmatrix}$, tedy $h_2(x_1,x_2) = h((x_1,x_2),(x_1,x_2))$ pro symetrickou bilineární formu h s maticí $[h]_{K_2} = \begin{pmatrix}1&2\\2&3\end{pmatrix}$ vzhledem ke kanonické bázi, je h_2 podle definice kvadratická forma.

Definice. *Maticí, polární bází a vrcholem kvadratické formy* f_2 budeme nad tělesem s charakteristikou různou od 2 rozumět matici, polární bázi a vrchol příslušné symetrické bilineární formy f_s. Dále řekneme, že kvadratická forma f_2 je *regulární*, f_s je-li regulární bilineární forma.

Příklad (Výpočet polární báze pomocí vrcholu)**.** (1) Buď h symetrická bilineární forma na vektorovém prostoru $\mathbf{Z}_7^5$ daná podmínkou $h(\mathbf{e}_i,\mathbf{e}_j) = 2$ pro všechna $i,j = 1,\dots,n$ Najdeme nejprve nějakou bázi vrcholu a poté nějakou polární bázi h.

Z podmínky, jíž je zadána bilineární forma h je zřejmé, že matice h zhledem ke kanonické bázi se skládá ze samých dvojek, tedy $[h]_{K_5} = \begin{pmatrix}2&2&2&2&2\\2&2&2&2&2\\2&2&2&2&2\\2&2&2&2&2\\2&2&2&2&2\end{pmatrix}$.
Hledáme-li vrchol, stačí díky 2.13 vyřešit homogenní soustavu rovnic s maticí $[h]_{K_5}$. Například posloupnost $M = ((6,1,0,0,0),(6,0,1,0,0),(6,0,0,1,0),\ (6,0,0,0,1))$ je báze vrcholu h. Podle definice vrcholu je $f(\mathbf{m},\mathbf{v}) = 0$ pro každé $\mathbf{m} \in M$ a $\mathbf{v} \in \mathbf{Z}_7^5$. Vzhledem k tomu, že je hodnost dané bilineární formy (tj. hodnost kterékoli její matice) rovna jedné, stačí nám v tomto případě najít libovolný doplněk posloupnosti M na bázi $\mathbf{Z}_7^5$ a takto doplněná posloupnost vektorů bude polární bází. Tedy například posloupnost $N = ((6,1,0,0,0),(6,0,1,0,0),(6,0,0,1,0),(6,0,0,0,1),(1,0,0,0,0))$ je polární báze h a matice h vzhledem k N je $\begin{pmatrix}0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&2\end{pmatrix}$.

(2) Označme f symetrickou bilineární formu na $\mathbf{Z}_5^3$, která vytváří kvadratickou formu f_2 danou vztahem $f_2(x_1,x_2,x_3) = 3x_1^2 + x_1x_2 + 2x_2^2 + 3x_2x_3 + 4x_3^2$. Najdeme polární bázi f (a tedy i f_2). Nejprve přímočaře určíme matici $[f]_{K_3} = \begin{pmatrix}3&3&0\\3&2&4\\0&4&4\end{pmatrix}$

a díky 2.13 spočítáme vrchol $V(f)$ jako řešení homogenní soustavy a maticí $[f]_{K_3}$. Protože

$$[f]_{K_3} = \begin{pmatrix} 3 & 3 & 0 \\ 3 & 2 & 4 \\ 0 & 4 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 \\ 0 & 4 & 4 \\ 0 & 0 & 0 \end{pmatrix}$$

tvoří bázi vrcholu vektor $(1,4,1)$. Nyní doplníme vektor $\mathbf{p}_1 = (1,4,1)$ na bázi celého $\mathbf{Z}_5^3$ například vektory $\mathbf{e}_1$ a $\mathbf{e}_2$ kanonické báze. Snadno určíme matici $[\widetilde{f}]_N = \begin{pmatrix} 3 & 3 \\ 3 & 2 \end{pmatrix}$ bilineární formy $\widetilde{f}$, která je restrikcí f na podprostor $U = \langle \mathbf{e}_1, \mathbf{e}_2 \rangle$, vzhledem k bázi $N = (\mathbf{e}_1, \mathbf{e}_2)$. Dále počítáme v souřadnicích vzhledem k N.

Nyní budeme hledat polární bázi $\widetilde{f}$. Nejprve poznamenejme, že určitě existuje vektor $\mathbf{p}_2$, pro který $\widetilde{f}_2(\mathbf{p}_2) \neq 0$ (a k jeho nalezení nám opět může pomoci 2.10). Protože $\widetilde{f}_2(\mathbf{e}_1) = 3 \neq 0$ položme $\mathbf{p}_2 = \mathbf{e}_1$. Nyní hledáme vektor $\mathbf{p}_3 \in U$, pro který $\widetilde{f}(\mathbf{p}_2, \mathbf{p}_3) = 0$. Využijeme-li 2.2, potřebujeme vyřešit homogenní soustavu rovnic s maticí

$$\{\mathbf{p}_2\}_B \cdot [\widetilde{f}]_N = (1,0) \cdot \begin{pmatrix} 3 & 3 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 3 & 3 \end{pmatrix}.$$

Vidíme, že soustavu řeší $\{\mathbf{p}_3\}_B = (4,1)$, tedy $\mathbf{p}_3 = (4,1,0)$ a $\widetilde{f}_2(\mathbf{p}_2) = (4,1) \cdot [\widetilde{f}]_N \cdot (4,1)^T = 4$. Našli jsme polární bázi $P = ((1,4,1),(1,0,0),(4,1,0))$ formy f s maticí vůči této bázi $[f]_P = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{pmatrix}$.

Věta 2.20 (Zákon setrvačnosti kvadratických forem)**.** *Buď f_2 kvadratická forma na reálném konečně dimenzionálním vektorovém prostoru V a buď B a C dvě polární báze kvadratické formy f_2. Pak platí, že*

(a) *počet vektorů $\mathbf{w}$, pro něž je $f_2(\mathbf{w}) = 0$, je v bázích B a C stejný, tedy $n(f_2) = |\{\mathbf{u} \in B | f_2(\mathbf{u}) = 0\}| = |\{\mathbf{v} \in C | f_2(\mathbf{v}) = 0\}|$,*
(b) *počet vektorů $\mathbf{w}$, pro něž je $f_2(\mathbf{w})$ kladné, je v bázích B a C stejný, tedy $p(f_2) = |\{\mathbf{u} \in B | f_2(\mathbf{u}) > 0\}| = |\{\mathbf{v} \in C | f_2(\mathbf{v}) > 0\}|$,*
(c) *počet vektorů $\mathbf{w}$, pro něž je $f_2(\mathbf{w})$ záporné, je v bázích B a C stejný, tedy $q(f_2) = |\{\mathbf{u} \in B | f_2(\mathbf{u}) < 0\}| = |\{\mathbf{v} \in C | f_2(\mathbf{v}) < 0\}|$.*

Navíc $n(f_2) + p(f_2) + q(f_2) = \dim(V)$

Důkaz. Označme p_B, q_B, p_C a q_C po řadě počet vektorů báze B s kladnou a se zápornou hodnotou f_2 a báze C s kladnou a se zápornou hodnotou f_2. Poznamenejme, že bod a) plyne okamžitě z Věty 2.16. Dále zřejmě platí rovnosti $n(f_2) + p_B + q_B = \dim(V) = n(f_2) + p_C + q_C$. Označme nyní $\mathbf{u}_1, \ldots, \mathbf{u}_{p_B}$ všechny bázické vektory báze B, pro které je $f_2(\mathbf{u}_i)$ kladné a $\mathbf{v}_1, \ldots, \mathbf{v}_k$ všechny bázické vektory báze C, pro které $f_2(\mathbf{v}_i) \leq 0$, kde $k = n(f_2) + q_C$. Všimněme si, že $f_2(\mathbf{u}) > 0$ pro každý nenulový vektor $\mathbf{u} \in \langle \mathbf{u}_1, \ldots, \mathbf{u}_{p_B} \rangle$ a že $f_2(\mathbf{u}) \leq 0$ pro každý vektor $\mathbf{u} \in \langle \mathbf{v}_1, \ldots, \mathbf{v}_k \rangle$. To znamená, že $\langle \mathbf{u}_1, \ldots, \mathbf{u}_{p_B} \rangle \cap \langle \mathbf{v}_1, \ldots, \mathbf{v}_k \rangle = \{\mathbf{0}\}$ a posloupnost vektorů $\mathbf{u}_1, \ldots, \mathbf{u}_{p_B}, \mathbf{v}_1, \ldots, \mathbf{v}_k$ je tudíž lineárně nezávislá. Proto $p_B + k = p_B + n(f_2) + q_C \leq \dim(V) = n(f_2) + p_C + q_C$ a odtud dostáváme, že $p_B \leq p_C$. Symetrickou úvahou pro ty vektory C, na nichž je f_2 kladná, a ty vektory B, na nichž je f_2 nulová nebo záporná, dostaneme, že $p_C \leq p_B$. Tedy $p_B = p_C$, a proto i $q_B = q_C$. □

Důsledek 2.21. *Buď f_2 kvadratická forma na reálném konečnědimenzionálním vektorovém prostoru V. Pak matice $[f_2]_B$ a $[f_2]_C$ obsahují na diagonále pro každou dvojici polárních bází $B, C \in V$ stejné množství nul, kladných čísel s záporných čísel.*

Definice. Buď f_2 kvadratická forma na reálném konečnědimenzionálním vektorovém prostoru. Vezměme nulitu $n(f_2)$ kvadratické formy f_2 a dále čísla $p(f_2)$ a $q(f_2)$ z Věty 2.20. Pak uspořádanou trojici $(n(f_2), p(f_2), q(f_2))$ nazveme *signaturou* kvadratické formy f_2 a bilineární formy f.

Důsledek 2.22 (klasické znění Zákona setrvačnosti kvadratických forem)**.** *Buď f_2 kvadratická forma na reálném konečnědimenzionálním vektorovém prostoru, pak její signatura $(n(f_2), p(f_2), q(f_2))$ nezávisí na volbě polární báze a $n(f_2)+p(f_2)+q(f_2) = \dim(V)$.*

Poznámka 2.23. *Buď f_2 kvadratická forma na reálném konečně dimenzionálním vektorovém prostoru V. Pak existuje taková polární báze B, že $f_2(\mathbf{v}) \in \{-1, 0, 1\}$ pro každý vektor $\mathbf{v} \in B$.*

Důkaz. Zvolme nějakou polární bázi $B = (\mathbf{b}_1, \dots, \mathbf{b}_n)$ kvadratické formy f_2, která existuje podle Věty 2.11. Položíme-li $\mathbf{b}'_i = \mathbf{b}_i$, jestliže $f_2(\mathbf{b}_i) = 0$ a $\mathbf{b}'_i = \frac{1}{\sqrt{|f_2(\mathbf{b}_i)|}} \cdot \mathbf{b}_i$ v případě, že $f_2(\mathbf{b}_i) \neq 0$, pak vidíme, že posloupnost $B = (\mathbf{b}'_1, \dots, \mathbf{b}'_n)$ je báze splňující podmínku $f_2(\mathbf{b}'_i) \in \{-1, 0, 1\}$. □

Poznámka 2.24. *Nechť V a W jsou dva reálné konečně dimenzionální vektorové prostory, f_2 kvadratická forma na V a g_2 kvadratická forma na W. Mají-li f_2 a g_2 stejnou signaturu, existuje takový izomorfismus $\varphi : V \to W$, že $f_2(\mathbf{v}) = g_2(\varphi(\mathbf{v}))$ pro každý vektor $\mathbf{v} \in V$.*

Důkaz. Protože mají V a W stejnou signaturu (n, p, q), mají i stejnou dimenzi $n+p+q$. Navíc podle 2.23 můžeme zvolit bázi $B = \{\mathbf{b}_1, \dots, \mathbf{b}_n\}$ prostoru V a bázi $C = (\mathbf{c}_1, \dots, \mathbf{c}_n)$ prostoru W, pro něž platí $f_2(\mathbf{b}_i) = 0 = g_2(\mathbf{c}_i)$ pro $i = 1, \dots n$, $f_2(\mathbf{b}_i) = 1 = g_2(\mathbf{c}_i)$ pro $i = n+1, \dots n+p$ a $f_2(\mathbf{b}_i) = -1 = g_2(\mathbf{c}_i)$ pro $i > n+p$. Rozšíříme-li nyní zobrazení $\varphi(\mathbf{b}_i) = \mathbf{c}_i$ na homomorfismus vektorových prostorů V a W, pak jde zjevně o izomorfismus a platí, že

$$f_2(\sum_{i=1}^{n+p+q} a_i\mathbf{b}_i) = \sum_{i=n+1}^{n+p} a_i^2 - \sum_{i=n+p+1}^{n+p+q} a_i^2 = g_2(\sum_{i=1}^{n+p+q} a_i\mathbf{c}_i) = g_2(\varphi(\sum_{i=1}^{n+p+q} a_i\mathbf{b}_i)).$$

□

Věta 2.25 (Klasifikace kvadratických forem)**.** *Nechť f_2 je kvadratická forma na reálném konečně dimenzionálním vektorovém prostoru V, f_s jí příslušná symetrická bilineární forma a $(n(f_2), p(f_2), q(f_2))$ signatura f.*

(1) *Jestliže $q(f_2) = 0$ a $n(f_2) = 0$, pak $f_2(\mathbf{v}) > 0$ pro každý nenulový vektor $\mathbf{v} \in V$ (říkáme, že f_2 resp. f_s je* pozitivně definitní*),*
(2) *jestliže $q(f_2) = 0$ a $n(f_2) > 0$, pak $f_2(\mathbf{v}) \geq 0$ pro každý vektor $\mathbf{v} \in V$ (říkáme, že f_2 resp. f_s je* pozitivně semidefinitní*),*
(3) *jestliže $p(f_2) = 0$ a $n(f_2) = 0$, pak $f_2(\mathbf{v}) < 0$ pro každý nenulový vektor $\mathbf{v} \in V$ (říkáme, že f_2 resp. f_s je* negativně definitní*),*
(4) *jestliže $p(f_2) = 0$ a $n(f_2) > 0$, pak $f_2(\mathbf{v}) \leq 0$ pro každý vektor $\mathbf{v} \in V$ (říkáme, že f_2 resp. f_s je* negativně semidefinitní*),*

(5) *jestliže* $p(f_2) >$ *a* $q(f_2) > 0$, *pak existuje* $\mathbf{v} \in V \setminus V(f_2)$, *pro které* $f_2(\mathbf{v}) = 0$ *(říkáme, že* f_2 *resp.* f_s *je* indefinitní*).*

Důkaz. Zvolme nějakou polární bázi $(\mathbf{u}_1, \dots, \mathbf{u}_n)$ symetrické bilineární formy f_s, která existuje podle Věty 2.11. Nechť $\mathbf{v} \in V$ je libovolný nenulový vektor, potom $\mathbf{v} = \sum_{i=1}^n a_i\, \mathbf{u}_i$ pro vhodné skaláry $a_i \in \mathbf{R}$, z nichž alespoň jedno a_i je nenulové.

(2) Pokud $q(f_2) = 0$, pak $f_2(\mathbf{u}_i) \geq 0$ pro všechna $i = 1, \dots, n$. Tedy

$$f_2(\mathbf{v}) = f_s(\mathbf{v}, \mathbf{v}) = f_s(\sum_{i=1}^n a_i\, \mathbf{u}_i, \sum_{j=1}^n a_j\, \mathbf{u}_j) = \sum_{i,j\leq 1} a_i a_j f(\mathbf{u}_i, \mathbf{u}_j) = \sum_{i=1}^n a_i^2 f(\mathbf{u}_i, \mathbf{u}_i) \geq 0.$$

(1) Pokud navíc $n(f_2) = 0$, je $f_2(\mathbf{u}_i) > 0$ pro všechna $i = 1, \dots, n$, a proto $f_2(\mathbf{v}) = \sum_{i=1}^n a_i^2 f(\mathbf{u}_i, \mathbf{u}_i) > 0$

Body (3) a (4) se dokazují obdobně

(5) Podle 2.23 existuje polární báze $(\mathbf{v}_1, \dots, \mathbf{v}_n)$ a dva různé indexy i a j, pro které $f_2(\mathbf{v}_i) = 1$ a $f_2(\mathbf{v}_j) = -1$. Nyní stačí položit $\mathbf{v} = \mathbf{v}_i + \mathbf{v}_j$. Zřejmě $\mathbf{v} \neq 0$ a $f_2(\mathbf{v}) = f_s(\mathbf{v}, \mathbf{v}) = f_s(\mathbf{v}_i + \mathbf{v}_j, \mathbf{v}_i + \mathbf{v}_j) = f_s(\mathbf{v}_i, \mathbf{v}_i) + f_s(\mathbf{v}_j, \mathbf{v}_j) = 1 - 1 = 0.$ □

3. Skalární součin

V celé této kapitole je těleso T buď tělesem **reálných** nebo **komplexních** čísel. Jestliže $c = a + bi$ je komplexní číslo, kde $a, b \in \mathbf{R}$, budeme značit $\overline{c} = a - bi$ číslo komplexně sdružené. Je-li $c \in \mathbf{R}$, zřejmě $\overline{c} = c$.

Definice. *Skalárním součinem* na vektorovém prostoru V nad tělesem T ($= \mathbf{R}$ nebo $\mathbf{C}$) nazveme zobrazení $g : V \times V \to T$ splňující pro všechny vektory $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ a skaláry $a, b \in T$ podmínky:

(1) $g(\mathbf{u}, a \cdot \mathbf{v} + b \cdot \mathbf{w}) = a \cdot g(\mathbf{u}, \mathbf{v}) + b \cdot g(\mathbf{u}, \mathbf{w})$,
(2) $g(\mathbf{u}, \mathbf{v}) = \overline{g(\mathbf{v}, \mathbf{u})}$,
(3) $g(\mathbf{u}, \mathbf{u}) \in \mathbf{R}$ a $g(\mathbf{u}, \mathbf{u}) \geq 0$, navíc $g(\mathbf{u}, \mathbf{u}) = 0$, právě když $\mathbf{u} = \mathbf{0}$.

Dvojici (V, g) nazveme (reálným nebo komplexním) *unitárním prostorem.*

Poznámka 3.1. *Pro všechny vektory* $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ *a skaláry* $a, b \in T$ *na unitárním prostoru* (V, g) *platí:*

(a) $g(a \cdot \mathbf{v} + b \cdot \mathbf{w}, \mathbf{u}) = \overline{a} \cdot g(\mathbf{v}, \mathbf{u}) + \overline{b} \cdot g(\mathbf{w}, \mathbf{u})$,
(b) $g(a \cdot \mathbf{u}, a \cdot \mathbf{u}) = |a|^2 g(\mathbf{u}, \mathbf{u})$,
(c) $g(\mathbf{u}, \mathbf{0}) = g(\mathbf{0}, \mathbf{u}) = 0$.

Důkaz. (a) Použijeme-li body (1) a (2) definice, pak

$$g(a\cdot\mathbf{v} + b\cdot\mathbf{w}, \mathbf{u}) = \overline{g(\mathbf{u}, a\cdot\mathbf{v} + b\cdot\mathbf{w})} = \overline{a}\cdot\overline{g(\mathbf{u}, \mathbf{v})} + \overline{b}\cdot\overline{g(\mathbf{u}, \mathbf{w})} = \overline{a}\cdot g(\mathbf{v}, \mathbf{u}) + \overline{b}\cdot g(\mathbf{w}, \mathbf{u}).$$

(b) Z (a) a bodu (1) definice plyne, že $g(a \cdot \mathbf{u}, a \cdot \mathbf{u}) = a\overline{a}g(\mathbf{u}, \mathbf{u}) = |a|^2 g(\mathbf{u}, \mathbf{u})$.

(c) Z (a) plyne $g(\mathbf{u}, \mathbf{0}) = g(\mathbf{u}, 0\,\mathbf{0}) = 0g(\mathbf{u}, \mathbf{0}) = 0$. Druhou rovnost dostaneme stejným postupem přímo z definice. □

Věta 3.2. *Buď* V *reálný vektorový prostor konečné dimenze a* g *zobrazeni* $V \times V \to \mathbf{R}$*. Pak* g *je skalárním součinem právě tehdy, když* g *je pozitivně definitní symetrickou bilineární formou na* V*.*

Důkaz. ($\Rightarrow$) Podle definice je skalární součin g lineární v druhé složce a podle Poznámky 3.1 a) je nad reálným tělesem lineární i v první složce, tedy jde o bilineární formu. Dále bod (2) definice říká, že skalární součin na reálném vektorovém prostoru je symetrická bilineární forma. Konečně podle bodu (3) definice je g pozitivně definitní.

($\Leftarrow$) Pozitivně definitní symetrická bilineární forma na reálném vektorovém prostoru zřejmě splňuje všechny tři axiomy definice skalárního součinu. $\square$

Příklad. 1) Zobrazení $\omega : T^n \times T^n \to T$ definované pro každou dvojici vektorů $\mathbf{x}, \mathbf{y} \in \mathbf{R}^n$ předpisem $\omega(\mathbf{x}, \mathbf{y}) = \overline{\mathbf{x}}\mathbf{y}^{\mathsf{T}}$ je (takzvaným *standardním*) skalárním součinem.

2) Mějme nějakou bázi B konečně dimenzionálního vektorového prostoru V. Zobrazení $g_B : V \times V \to T$ definované předpisem $g_B(\mathbf{v}, \mathbf{w}) = \overline{\{\mathbf{v}\}_B}\{\mathbf{w}\}_B^{\mathsf{T}}$ pro všechny vektory $\mathbf{v}, \mathbf{w} \in V$ je skalární součin.

3) Symetrická bilineární forma $I_{ab}(f, g) = \int_a^b fg$ na reálném vektorovém prostoru $\mathbb{C}_0(\langle a, b\rangle)$ (viz příklad 4) bilineárních forem) je zřejmě pozitivně definitní, tedy jde o skalární součin.

Definice. Nechť (V, g) je unitární prostor, potom zobrazení $\|-\|_g : V \to \mathbf{R}$ určené předpisem $\|\mathbf{v}\|_g = \sqrt{g(\mathbf{v}, \mathbf{v})}$ nazveme *normou* danou skalárním součinem g.

Poznámka 3.3. *Pro všechny vektory $\mathbf{u}, \mathbf{v} \in V$ a skaláry $a \in T$ na unitárním prostoru (V, g) platí:*

(a) $\|\mathbf{v}\|_g \geq 0$ *a* $\|\mathbf{v}\|_g = 0$ *právě když* $\mathbf{v} = \mathbf{0}$*,*
(b) $\|a\mathbf{v}\|_g = |a| \cdot \|\mathbf{v}\|_g$*,*

Důkaz. (a) dostáváme bezprostředně z bodu (3) definice skalárního součinu a (b) plyne z 3.1(b) $\square$

Věta 3.4. *Nechť (V, g) je unitární prostor. Potom pro všechny vektory $\mathbf{u}, \mathbf{v} \in V$ platí:*

(a) $|g(\mathbf{u}, \mathbf{v})| \leq \|\mathbf{u}\|_g \|\mathbf{v}\|_g$ *(Cachyho-Schwarzova nerovnost),*
(b) $\|\mathbf{u}+\mathbf{v}\|_g \leq \|\mathbf{u}\|_g + \|\mathbf{v}\|_g$ *(Trojúhelníková nerovnost).*

Důkaz. a) Je-li $\mathbf{u} = \mathbf{0}$, tvrzení zřejmě platí. Předpokládejme, že $\mathbf{u} \neq \mathbf{0}$, a označme $c = \frac{g(\mathbf{u},\mathbf{v})}{\|\mathbf{u}\|_g^2}$. S využitím definice a Poznámky 3.1 dostaneme:

$$0 \leq g(c\mathbf{u} - \mathbf{v}, c\mathbf{u} - \mathbf{v}) = \overline{c}c \cdot g(\mathbf{u}, \mathbf{u}) - c \cdot g(\mathbf{v}, \mathbf{u}) - \overline{c} \cdot g(\mathbf{u}, \mathbf{v}) + g(\mathbf{v}, \mathbf{v}) =$$
$$= \frac{|g(\mathbf{u}, \mathbf{v})|^2}{\|\mathbf{u}\|_g^4} \cdot \|\mathbf{u}\|_g^2 - 2\frac{|g(\mathbf{u}, \mathbf{v})|^2}{\|\mathbf{u}\|_g^2} + \|\mathbf{v}\|_g^2 = \|\mathbf{v}\|_g^2 - \frac{|g(\mathbf{u}, \mathbf{v})|^2}{\|\mathbf{u}\|_g^2}.$$

Proto $|g(\mathbf{u}, \mathbf{v})|^2 \leq \|\mathbf{u}\|_g^2 \|\mathbf{v}\|_g^2$ a $|g(\mathbf{u}, \mathbf{v})| \leq \|\mathbf{u}\|_g \|\mathbf{v}\|_g$.

b) Uvědomíme-li si, že $\mathrm{Re}(g(\mathbf{u}, \mathbf{v})) \leq |g(\mathbf{u}, \mathbf{v})| \leq \|\mathbf{u}\|_g \|\mathbf{v}\|_g$, kde Re označuje reálnou část komplexního čísla, snadno spočítáme, že

$$\|\mathbf{u}+\mathbf{v}\|_g^2 = \|\mathbf{u}\|_g^2 + 2 \cdot \mathrm{Re}(g(\mathbf{u}, \mathbf{v})) + \|\mathbf{v}\|_g^2 \leq$$
$$\leq \|\mathbf{v}\|_g^2 + 2\|\mathbf{u}\|_g \|\mathbf{v}\|_g + \|\mathbf{v}\|_g^2 = (\|\mathbf{u}\|_g + \|\mathbf{v}\|_g)^2.$$

Tedy $\|\mathbf{u}+\mathbf{v}\|_g \leq \|\mathbf{u}\|_g + \|\mathbf{v}\|_g$. $\square$

Příklad (Geometrie na reálném unitárním prostoru)**.** Na reálném unitárním prostoru (V, g) můžeme měřit úhly a vzdálenosti vektorů následujícím způsobem: řekneme, že dva vektory $\mathbf{u}$ a $\mathbf{v}$ svírají úhel α, pokud

$$cos\alpha = \frac{g(\mathbf{u}, \mathbf{v})}{\|\mathbf{u}\|_g \|\mathbf{v}\|_g},$$

a vzdálenost dvou vektorů $\mathbf{u}$ a $\mathbf{v}$ definujeme jako hodnotu $\|\mathbf{u}-\mathbf{v}\|_g$. Poznamenejme, že podle Věty 3.4(a) je úhel dobře definován (tj. $cos\alpha \in \langle -1, 1\rangle$) a dva vektory $\mathbf{u}$ a $\mathbf{v}$ jsou kolmé právě tehdy, když $g(\mathbf{u}, \mathbf{v}) = 0$. Podle Poznámky 3.3 a) je velikost nenulového vektoru kladná a Věta 3.3(b) říká, že platí trojúhelníkoví nerovnost.

Definice. Nechť (V, g) je konečně dimenzionální unitární prostor a $(\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n)$ je nějaká báze V. Matici $[g]_{(\mathbf{u}_i)} = (a_{ij})$ nazveme *maticí skalárního součinu g vzhledem k bázi* $(\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n)$, jestliže $a_{ij} = g(\mathbf{u}_i, \mathbf{u}_j)$, kde $i, j \le n$.

Poznámka 3.5. *Buď (V, g) unitární prostor a B nějaká konečná báze V. Potom $[g]_B = \overline{[g]_B^{\mathsf{T}}}$, dále $[g]_C = \overline{[\mathrm{Id}]_{CB}}^{\mathsf{T}}[g]_B[\mathrm{Id}]_{CB}$ a $g(\mathbf{v}, \mathbf{w}) = \overline{\{\mathbf{v}\}_B}[g]_B\{\mathbf{w}\}_B^{\mathsf{T}}$ pro každé dva vektory $\mathbf{v}, \mathbf{w} \in V$.*

Důkaz. Obdoba tvrzení 2.2 a 2.3. Označme si vektory báze $B = (\mathbf{u}_1, \dots, \mathbf{u}_n)$ a nechť $\mathbf{v} = \sum_{i=1}^n a_i\, \mathbf{u}_i$ a $\mathbf{w} = \sum_{j=1}^n b_j\, \mathbf{u}_j$. Potom podle definice a díky 3.1(a) dostáváme, že

$$g(\mathbf{v}, \mathbf{w}) = g(a_i\, \mathbf{u}_i, \sum_{j=1}^n b_j\, \mathbf{u}_j) = \sum_{i=1}^n \sum_{j=1}^n \overline{a_i} \cdot b_j \cdot g(\mathbf{u}_i, \mathbf{u}_j) = \overline{\{\mathbf{v}\}_B}[g]_B\{\mathbf{w}\}_B^{\mathsf{T}}.$$

Podmínka $[g]_B = \overline{[g]_B^{\mathsf{T}}}$ plyne z bodu (2) definice skalárního součinu. Konečně rovnost $[g]_C = \overline{[\mathrm{Id}]_{CB}}^{\mathsf{T}}[g]_B[\mathrm{Id}]_{CB}$ se dokáže stejnou úvahou jako 2.3 s využitím právě ověřené rovnosti $g(\mathbf{v}, \mathbf{w}) = \overline{\{\mathbf{v}\}_B}[g]_B\{\mathbf{w}\}_B^{\mathsf{T}}$. □

Definice. Nechť je (V, g) unitární prostor. Řekneme, že je posloupnost vektorů $B \subset V$ je *ortogonální*, pokud $g(\mathbf{u}, \mathbf{v}) = 0$ pro každou dvojici vektorů $\mathbf{u}, \mathbf{v} \in B$, $\mathbf{u} \ne \mathbf{v}$. Ortogonální posloupnost $B \subset V$ nazveme *ortonormální*, jestliže navíc $g(\mathbf{u}, \mathbf{u}) = 1$ pro každý vektor $\mathbf{u} \in B$.

Věta 3.6 (Pythagorova věta)**.** *Jsou-li dva vektory $\mathbf{u}$ a $\mathbf{v}$ unitárního prostoru (V, g) ortogonální, pak $\|\mathbf{u}+\mathbf{v}\|_g^2 = \|\mathbf{u}\|_g^2 + \|\mathbf{v}\|_g^2$.*

V reálném vektorovém prostoru platí i opačná implikace.

Důkaz. Stačí uvážit rovnost

$$\|\mathbf{u}+\mathbf{v}\|_g^2 = \|\mathbf{u}\|_g^2 + 2 \cdot \mathrm{Re}(g(\mathbf{u}, \mathbf{v})) + \|\mathbf{v}\|_g^2$$

z důkazu Věty 3.4. □

Poznámka 3.7. *Každá ortonormální posloupnost vektorů unitárního prostoru je lineárně nezávislá.*

Důkaz. Úvahu stačí provést pro konečné posloupnosti. Je-li $(\mathbf{u}_1, \dots, \mathbf{u}_n)$ ortonormální posloupnost vektorů unitárního prostoru (V, g) a předpokládáme-li pro posloupnost skalárů $a_1, \dots a_n$, že $\sum_{i=1}^n a_i\, \mathbf{u}_i = \mathbf{0}$, potom

$$0 = g(\mathbf{u}_j, \mathbf{0}) = g(\mathbf{u}_j, \sum_{i=1}^n a_i\, \mathbf{u}_i) = \sum_{i=1}^n a_i g(\mathbf{u}_j, \mathbf{u}_i) = a_j$$

pro všechna $j = 1, \dots, n$, tedy $(\mathbf{u}_1, \dots, \mathbf{u}_n)$ je lineárně nezávislá. □

Věta 3.8. *Nechť $(\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n)$ je báze unitárního prostoru (V, g). Potom existuje $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$ ortonormální báze V splňující podmínku $\langle \mathbf{u}_1, \dots, \mathbf{u}_i\rangle = \langle \mathbf{v}_1, \dots, \mathbf{v}_i\rangle$ pro všechna $i = 1, 2, \dots, n$.*

Důkaz. Při hledání ortonormální báze s požadovanými vlastnostmi postupujme indukcí.

Protože $\mathbf{u}_1$ je bázický vektor, $\mathbf{u}_1 \neq \mathbf{0}$, a proto $\| \mathbf{u}_1 \|_g \neq 0$ podle Poznámky 3.2. Položme $\mathbf{v}_1 = \frac{\mathbf{u}_1}{\| \mathbf{u}_1 \|_g}$. Potom $g(\mathbf{v}_1, \mathbf{v}_1) = 1$ a $\langle \mathbf{u}_1 \rangle = \langle \mathbf{v}_1 \rangle$.

Mějme definovánu ortonormální posloupnost vektorů $\mathbf{v}_1, \dots, \mathbf{v}_{i-1}$, která splňuje podmínku $\langle \mathbf{u}_1, \dots, \mathbf{u}_{i-1} \rangle = \langle \mathbf{v}_1, \dots, \mathbf{v}_{i-1} \rangle$. Nyní nejprve definujme vektor

$$\mathbf{v}_i' = \mathbf{u}_i - \sum_{j=1}^{i-1} g(\mathbf{v}_j, \mathbf{u}_i)\, \mathbf{v}_j\,.$$

Zřejmě platí, že $\langle \mathbf{u}_1, \dots, \mathbf{u}_{i-1}, \mathbf{u}_i \rangle = \langle \mathbf{v}_1, \dots, \mathbf{v}_{i-1}, \mathbf{u}_i \rangle = \langle \mathbf{v}_1, \dots, \mathbf{v}_{i-1}, \mathbf{v}_i' \rangle$. Odtud také plyne, že posloupnost $\mathbf{v}_1, \dots, \mathbf{v}_{i-1}, \mathbf{v}_i'$ generuje podprostor dimenze i, tedy jde o lineárně nezávislou posloupnost. Proto $\mathbf{v}_i' \neq \mathbf{0}$ a $\| \mathbf{v}_i' \|_g \neq 0$. Dále

$$g(\mathbf{v}_k, \mathbf{v}_i') = g(\mathbf{v}_k, \mathbf{u}_i) - \sum_{j=1}^{i-1} g(\mathbf{v}_j, \mathbf{u}_i) g(\mathbf{v}_k, \mathbf{v}_j) = g(\mathbf{v}_k, \mathbf{u}_i) - g(\mathbf{v}_k, \mathbf{u}_i) = 0$$

pro každé $k = 1, \dots, i-1$. Když nyní položíme $\mathbf{v}_i = \frac{\mathbf{v}_i'}{\| \mathbf{v}_i' \|_g}$, dostáváme $\| \mathbf{v}_i \|_g = 1$, tedy $\mathbf{v}_1, \dots, \mathbf{v}_i$ bude ortonormální posloupností vektorů. Konečně $\langle \mathbf{u}_1, \dots, \mathbf{u}_i \rangle = \langle \mathbf{v}_1, \dots, \mathbf{v}_i' \rangle = \langle \mathbf{v}_1, \dots, \mathbf{v}_i \rangle$. □

Příklad (klasická Gramova-Schmidtova ortogonalizace)**.** Shrňme postup, kterým jsme v důkazu předchozí věty získali z báze $(\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n)$ unitárního prostoru (V, g) ortonormální bázi $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$:

V prvním kroku jsme položili $\mathbf{v}_1 = \frac{\mathbf{u}_1}{\| \mathbf{u}_1 \|_g}$.

V i-tém kroku jsme nejprve hledali vektor ve tvaru $\mathbf{v}_i' = \mathbf{u}_i - \sum_{j=1}^{i-1} c_j\, \mathbf{v}_j$, který by byl kolmý na všechny předchozí vektory $\mathbf{v}_k$, tj. $g(\mathbf{v}_k, \mathbf{v}_i') = 0$ pro všechna $k = 1, \dots, i-1$. Odtud snadno odvodíme, že $c_j = g(\mathbf{v}_j, \mathbf{u}_i)$ a $\mathbf{v}_i' = \mathbf{u}_i - \sum_{j=1}^{i-1} g(\mathbf{v}_j, \mathbf{u}_i)\, \mathbf{v}_j$. Konečně $\mathbf{v}_i = \frac{\mathbf{v}_i'}{\| \mathbf{v}_i' \|_g}$.

Vezměme si bázi $((1,1,0),\ (0,1,1),\ (1,1,1))$ reálného vektorového prostoru $\mathbf{R}^3$ se standardním skalárním součinem ω. Najdeme výše uvedeným postupem ortonormální bázi: $(\mathbf{v}_i)$.

1. $\mathbf{v}_1 = \frac{(1,1,0)}{\|(1,1,0)\|_\omega} = \frac{1}{\sqrt{2}}(1,1,0)$.
2. $\mathbf{v}_2' = (0,1,1) - \omega(\frac{1}{\sqrt{2}}(1,1,0), (0,1,1)) \cdot \frac{1}{\sqrt{2}}(1,1,0) = \frac{1}{2}(-1,1,2)$. Proto $\mathbf{v}_2 = \frac{1}{\sqrt{6}}(-1,1,2)$.
3. Předně $\omega(\frac{1}{\sqrt{2}}(1,1,0), (1,1,1)) = \sqrt{2}$ a $\omega(\frac{1}{\sqrt{6}}(-1,1,2), (1,1,1)) = \frac{2}{\sqrt{6}}$, proto $\mathbf{v}_3' = (1,1,1) - \sqrt{2} \cdot \frac{1}{\sqrt{2}}(1,1,0) - \frac{2}{\sqrt{6}} \frac{1}{\sqrt{6}}(-1,1,2) = \frac{1}{3}(1,-1,1)$. Konečně $\mathbf{v}_3 = \frac{1}{\sqrt{3}}(1,-1,1)$.

Příklad (modifikovaná Gramova-Schmidtova ortogonalizace)**.** V prvním kroku modifikovaného Gramova-Schmidtova algoritmu rovněž položme $\mathbf{v}_1 = \frac{\mathbf{u}_1}{\| \mathbf{u}_1 \|_g}$ a dále přiřaďme $\mathbf{u}_k \to \mathbf{v}_k'$ pro všechna $k = 2, \dots, n$.

V i-tém kroku algoritmu potom postupně nahradíme vektory $\mathbf{v}_k'$ pro všechna $k = i, i+1, \dots, n$ vektorem $\mathbf{v}_k' - g(\mathbf{v}_{i-1}, \mathbf{v}_k')\, \mathbf{v}_{i-1}$. Nakonec položíme $\mathbf{v}_i = \frac{\mathbf{v}_i'}{\| \mathbf{v}_i' \|_g}$.

Chceme-li vytvořit ortonormální bázi z báze $((1,1,0),\ (0,1,1),\ (1,1,1))$ unitárního prostoru $(\mathbf{R}^3, \omega)$ modifikovaným Gramovým-Schmidtovým algoritmem, dostáváme:

1. $\mathbf{v}_1 = \frac{1}{\sqrt{2}}(1,1,0)$, $\mathbf{v}_2' = (0,1,1)$ a $\mathbf{v}_3' = (1,1,1)$.
2. $\mathbf{v}_2' = \frac{1}{2}(-1,1,2)$, $\mathbf{v}_3' = (1,1,1) - \sqrt{2}\cdot\frac{1}{\sqrt{2}}(1,1,0) = (0,0,1)$ a normujeme $\mathbf{v}_2 = \frac{1}{\sqrt{6}}(-1,1,2)$.
3. $\mathbf{v}_3' = (0,0,1) - \frac{2}{\sqrt{6}}\frac{1}{\sqrt{6}}(-1,1,2) = \frac{1}{3}(1,-1,1)$ a $\mathbf{v}_3 = \frac{1}{\sqrt{3}}(1,-1,1)$.

Výsledek modifikovaného algoitmu je stejný jako v případě klasického algoritmu, změnili jsme jen uspořádání úprav.

Poznámka 3.9. *Buď (V,g) unitární prostor konečné dimenze a $(\mathbf{v}_1,\mathbf{v}_2,\dots,\mathbf{v}_n)$ ortonormální báze V. Pak $\mathbf{v} = \sum_{i=1}^n g(\mathbf{v}_i,\mathbf{v})\,\mathbf{v}_i$ pro každý vektor $\mathbf{v}\in V$.*

Důkaz. Předpokládejme, že $\{\mathbf{v}\}_{(\mathbf{v}_i)} = (a_1,\dots,a_n)$, tedy $\mathbf{v} = \sum_{i=1}^n a_i\,\mathbf{v}_i$, potom $g(\mathbf{v}_j,\mathbf{v}) = g(\mathbf{v}_j,\sum_{i=1}^n a_i\,\mathbf{u}_i) = \sum_{i=1}^n a_i g(\mathbf{u}_j,\mathbf{u}_i) = a_j$ pro všechna $j=1,\dots,n$. □

Příklad. Uvažujem ortonormální bázi $M = (\frac{1}{\sqrt{2}}(1,1,0), \frac{1}{\sqrt{6}}(-1,1,2), \frac{1}{\sqrt{3}}(1,-1,1))$ reálného unitárního prostoru $(\mathbf{R}^3,\omega)$. S využitím 3.9 snadno spočítáme souřadnice $\{(1,2,3)\}_M = (a_1,a_2,a_3)$, kde $a_1 = \omega(\frac{1}{\sqrt{2}}(1,1,0),(1,2,3)) = \frac{3}{\sqrt{2}}$, dále $a_2 = \omega(\frac{1}{\sqrt{6}}(-1,1,2),(1,2,3)) = \frac{7}{\sqrt{6}}$ a $a_3 = \omega(\frac{1}{\sqrt{3}}(1,-1,1),(1,2,3)) = \frac{4}{\sqrt{3}}$, tedy

$$\{(1,2,3)\}_M = (\frac{3}{\sqrt{2}},\frac{7}{\sqrt{6}},\frac{4}{\sqrt{3}}).$$

Poznámka 3.10. *Buď (V,g) konečně dimenzionální unitární prostor. Pak báze $B\subset V$ je ortonormální právě tehdy, když $[g]_B$ je jednotková matice.*

Důkaz. Okamžitý důsledek definic pojmů. □

Definice. Nechť (V,g) a (V',g') jsou dva unitární prostory nad stejným tělesem (tj. buď nad $\mathbf{R}$ nebo $\mathbf{C}$). Řekneme, že homomorfismus $\varphi: V\to V'$ je *unitární zobrazení*, jestliže $g(\mathbf{v},\mathbf{w}) = g'(\varphi(\mathbf{v}),\varphi(\mathbf{w}))$ pro každou dvojici vektorů $\mathbf{v},\mathbf{w}\in V$.

Poznámka 3.11. *Každé unitární zobrazení je prosté.*

Důkaz. Buď $\varphi: V\to V'$ unitární zobrazení unitárních prostorů (V,g) a (V',g') a vezměme $\mathbf{v}\in\operatorname{Ker}\varphi$. Potom $0 = g'(\varphi(\mathbf{v}),\varphi(\mathbf{v})) = g(\mathbf{v},\mathbf{v})$, tedy podle definice skalárního součinu je $\mathbf{v}=\mathbf{0}$. Dokázali jsme, že $\operatorname{Ker}\varphi = \{\mathbf{0}\}$. □

Věta 3.12. *Nechť (V,g) je unitární prostor konečné dimenze (zopakujme, že nad tělesem $T=\mathbf{R}$ nebo $\mathbf{C}$) a B je ortonormální báze V, položme $n=\dim(V)$. Pak zobrazení $\varphi: V\to T^n$ dané předpisem $\varphi(\mathbf{u}) = \{\mathbf{u}\}_B$ je unitární zobrazení na prostor (T^n,ω).*

Důkaz. Zobrazení φ je zřejmě izomorfismus. Dále díky 3.5 máme rovnost $g(\mathbf{v},\mathbf{w}) = \overline{\{\mathbf{v}\}}_B[g]_B\{\mathbf{w}\}_B^{\mathsf{T}}$ pro každé dva vektory $\mathbf{v},\mathbf{w}\in V$. Ovšem matice $[g]_B$ je podle 3.10 jednotková, proto $g(\mathbf{v},\mathbf{w}) = \overline{\{\mathbf{v}\}}_B\{\mathbf{w}\}_B^{\mathsf{T}} = \omega(\varphi(\mathbf{v}),\varphi(\mathbf{w}))$, tedy φ je unitární zobrazení. □

Definice. Buď (V,g) unitární prostor a buď M nějaká podmnožina V. Množinu $M^\perp = \{\mathbf{v}\in V \mid \forall\mathbf{u}\in M:\ g(\mathbf{u},\mathbf{v})=0\}$ nazveme *ortogonálním doplňkem* množiny M v unitárním prostoru (V,g).

Poznámka 3.13. *Nechť (V,g) je unitární prostor a M podmnožina V. Potom $M^\perp$ je podprostor V a platí, že $\langle M\rangle^\perp = M^\perp$*

Důkaz. Předně si všimněme, že $\mathbf{0} \in M^\perp$ protože $g(\mathbf{v}, \mathbf{0})$ pro každý vektor $\mathbf{v} \in V$. Zvolme $\mathbf{v}, \mathbf{w} \in M^\perp$ a skalár $r \in T$. Pak pro každé $\mathbf{u} \in M$ je $g(\mathbf{u}, \mathbf{v}+\mathbf{w}) = g(\mathbf{u}, \mathbf{v}) + g(\mathbf{u}, \mathbf{w}) = 0$ a $g(\mathbf{u}, r \cdot \mathbf{v}) = r \cdot g(\mathbf{u}, \mathbf{v}) = 0$, tedy $\mathbf{v}+\mathbf{w}, r \cdot \mathbf{v} \in M^\perp$.

Zjevně platí $\langle M \rangle^\perp \subseteq M^\perp$. Zvolme naopak $\mathbf{v} \in M^\perp$ a libovolné $\mathbf{u} \in \langle M \rangle$. Potom existují takové prvky $\mathbf{u}_i \in\in M$ a $a_i \in T$, $i = 1, \dots, n$, že $\mathbf{u} = \sum_{i=1}^n a_i \mathbf{u}_i$, a proto podle 3.1(a)

$$g(\mathbf{u}, \mathbf{v}) = g(\sum_{i=1}^n a_i \mathbf{u}_i, \mathbf{v}) = \sum_{i=1}^n \overline{a_i} g(\mathbf{u}_i, \mathbf{v}) = \sum_{i=1}^n \overline{a_i} \cdot 0 = 0.$$

Tím jsem ověřili, že $\mathbf{v} \in \langle M \rangle^\perp$, a proto $\langle M \rangle^\perp = M^\perp$. □

Věta 3.14. *Nechť (V, g) je unitární prostor a U jeho podprostor konečné dimenze. Potom $U \cap U^\perp = \{\mathbf{0}\}$ a $U + U^\perp = V$.*

Důkaz. Pokud $\mathbf{u} \in U \cap U^\perp$, zřejmě $g(\mathbf{u}, \mathbf{u}) = 0$, tedy podle definice $\mathbf{u} = \mathbf{0}$. Tím jsme ověřili, že $U \cap U^\perp = \{\mathbf{0}\}$.

Poznamenejme, že zobrazení g omezené na množinu $U \times U$ je skalárním součinem na konečně dimenzionálním prostoru U. Vezměme nějakou ortonormální bázi $(\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k)$ podprostoru U, kterou nám zaručuje Věta 3.8. Nechť $\mathbf{v} \in V$. Položme $\mathbf{u} = \sum_{i=1}^k g(\mathbf{u}_i, \mathbf{v}) \mathbf{u}_i$ a $\mathbf{u}^\perp = \mathbf{v} - \mathbf{u}$. Zřejmě $\mathbf{u} \in U$. Dále $g(\mathbf{u}_i, \mathbf{u}^\perp) = g(\mathbf{u}_i, \mathbf{v}) - g(\mathbf{u}_i, \mathbf{v}) = 0$, tedy $\mathbf{u}^\perp \in U^\perp$ podle 3.13. Tedy každý vektor z V leží v prostoru $U + U^\perp$, což znamená, že $U + U^\perp = V$. □

Poznámka 3.15. *Mějme (V, g) unitární prostor a U jeho podprostor konečné dimenze. Potom pro každý vektor $\mathbf{v} \in V$ existuje právě jeden vektor $P_U(\mathbf{v}) \in U$ a právě jeden vektor $P_U^\perp(\mathbf{v}) \in U^\perp$ tak, že $\mathbf{v} = P_U(\mathbf{v}) + P_U^\perp(\mathbf{v})$. Navíc obě zobrazení $P_U : V \to U$ i $P_U^\perp : V \to U^\perp$ jsou homomorfismy na (tj. epimorfismy), $P_U(\mathbf{u}) = \mathbf{u}$ pro každý vektor $\mathbf{u} \in U$ a $P_U^\perp(\mathbf{v}) = \mathbf{v}$ pro každý vektor $\mathbf{v} \in U^\perp$.*

Důkaz. Zvolme $\mathbf{v}, \mathbf{w} \in V$ a $r \in T$. Existence a vektorů $P_U(\mathbf{v}) \in U$ a $P_U^\perp(\mathbf{v}) \in U^\perp$, pro něž $\mathbf{v} = P_U(\mathbf{v}) + P_U^\perp(\mathbf{v})$ plyne z 3.14. Navíc vezmeme-li $\mathbf{u} \in U$ a $\mathbf{u}^\perp \in U^\perp$, pro něž $\mathbf{v} = \mathbf{u} + \mathbf{u}^\perp$, pak $P_U(\mathbf{v}) - \mathbf{u} = \mathbf{u}^\perp - P_U^\perp(\mathbf{v}) \in U \cap U^\perp = \{\mathbf{0}\}$. Opět díky 3.14 tedy dostáváme jednoznačnost volby $P_U(\mathbf{v})$ a $P_U^\perp(\mathbf{v})$. Konečně

$$P_U(\mathbf{v}) + P_U^\perp(\mathbf{v}) + P_U(\mathbf{w}) + P_U^\perp(\mathbf{w}) = \mathbf{v} + \mathbf{w} = P_U(\mathbf{v} + \mathbf{w}) + P_U^\perp(\mathbf{v} + \mathbf{w}),$$

$$P_U(r \cdot \mathbf{v}) + P_U^\perp(r \cdot \mathbf{v}) = r \cdot \mathbf{v} = r \cdot (P_U(\mathbf{v}) + P_U^\perp(\mathbf{v})) = r \cdot P_U(\mathbf{v}) + r \cdot P_U^\perp(\mathbf{v}).$$

Z jednoznačnosti rozkladu a díky tomu, že U i $U^\perp$ jsou podprostory, tedy $P_U(\mathbf{v}) + P_U(\mathbf{w}), r \cdot (P_U(\mathbf{v}) \in U$ a $P_U^\perp(\mathbf{v}) + P_U^\perp(\mathbf{w}), r \cdot (P_U^\perp(\mathbf{v}) \in U^\perp$, dostáváme

$$P_U(\mathbf{v}) + P_U(\mathbf{w}) = P_U(\mathbf{v} + \mathbf{w}), \quad P_U^\perp(\mathbf{v}) + P_U^\perp(\mathbf{w}) = P_U^\perp(\mathbf{v} + \mathbf{w}),$$

$$P_U(r \cdot \mathbf{v}) = r \cdot P_U(\mathbf{v}), \quad P_U^\perp(r \cdot \mathbf{v}) = r \cdot P_U^\perp(\mathbf{v}),$$

tedy zobrazení P_U i $P_U^\perp$ jsou homomorfismy a podmínky $P_U(\mathbf{u}) = \mathbf{u}$ pro každý vektor $\mathbf{u} \in U$ a $P_U^\perp(\mathbf{v}) = \mathbf{v}$ pro každý vektor $\mathbf{v} \in U^\perp$, které platí díky jednoznačnosti rozkladu, říkají, že jde o homomorfimsy na. □

Definice. Homomorfismus P_U z předchozí poznámky se nazývá *ortogonální projekcí* prostoru V na podprostor U.

Příklad. Máme-li nějaký podprostor $U = \langle \mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k \rangle$ unitárního prostoru (V, g) a budeme-li chtít najít ortogonální projekci libovolného vektoru $\mathbf{v} \in V$, nemusíme nutně hledat ortogonální bázi U, tak jak to vyžaduje postup důkazu Věty 3.14. Můžeme pozorování, které využívá důkaz 3.14, aplikovat i na původní generující množinu $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k$, tj. vyjádříme si hledanou ortogonální projekci ve tvaru $\mathbf{u} = \sum_{j=1}^{k} x_j\, \mathbf{u}_j$ a uvědomíme si, že vektor $\mathbf{u}^\perp = \mathbf{v} - \mathbf{u}$ musí být kolmý na všechny generátory $\mathbf{u}_i$, tedy $g(\mathbf{u}_i, \mathbf{v} - \mathbf{u}) = 0$ pro $i = 1, \dots k$. Dosaďme a upravujme:

$$0 = g(\mathbf{u}_i, \mathbf{v} - \mathbf{u}) = g(\mathbf{u}_i, \mathbf{v} - \sum_{i=j}^{k} x_j\, \mathbf{u}_j) = g(\mathbf{u}_i, \mathbf{v}) - \sum_{i=j}^{k} x_j g(\mathbf{u}_i, \mathbf{u}_j)$$

Dostaneme tak obecně nehomogenní soustavu rovnic:

$$\sum_{j=1}^{k} g(\mathbf{u}_i, \mathbf{u}_j) x_j = g(\mathbf{u}_i, \mathbf{v}).$$

Matici levých stran $(g(\mathbf{u}_i, \mathbf{u}_j))$ se zpravidla říká Gramova matice (všimněme si, že se jedná právě o matici skalárního součinu g umezeného na podprostor U vzhledem k bázi $(\mathbf{u}_1, \dots, \mathbf{u}_k)$).

Poznámka 3.15 nám říká, že existuje řešení dané soustavy rovnic (tj. existuje příslušná ortogonální projekce). Pokud je posloupnost $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k$ navíc lineárně nezávislá (tj. jde o bázi U) je řešení dané soustavy právě jedno. Hledanou projekcí je lineární kombinace $\mathbf{u} = \sum_{j=1}^{k} x_j\, \mathbf{u}_j$.

Vezměme si například podprostor $U = \langle (1, 2, 1, -1),\ (1, 1, 0, 1) \rangle$ reálného unitárního porostoru se standardním skalárním součinem $(\mathbf{R}^4, \omega)$. Hledejme ortogonální projekci vektoru $(-1, 1, 0, 4)$. K tomu potřebujeme nejprve určit souřadnice x_1, x_2 ortogonální projekce $\mathbf{u} = x_1 \cdot (1, 2, 1, -1) + x_2 \cdot (1, 1, 0, 1)$. Řešíme tedy nehomogenní soustavu rovnic s maticí:

$$\left(\begin{array}{cc|c} 7 & 2 & -3 \\ 2 & 3 & 4 \end{array}\right).$$

Snadno zjistíme, že $x_1 = -1$ a $x_2 = 2$, proto $P_U(\mathbf{v}) = \mathbf{u} = (1, 0, -1, 3)$. Pro kontrolu ještě ověřme, zda je vektor $\mathbf{v} - \mathbf{u} = (-2, 1, 1, 1)$ skutečně kolmý na podprostor U. Zřejmě $\omega((-2, 1, 1, 1), (1, 2, 1, -1)) = 0$ a $\omega((-2, 1, 1, 1), (1, 1, 0, 1)) = 0$.

Věta 3.16. *Je-li (V, g) unitární prostor, U jeho podprostor konečné dimenze a $\mathbf{v} \in V$, pak $\|\, \mathbf{v} - P_U(\mathbf{v})\|_g < \|\, \mathbf{v} - \mathbf{u}\,\|_g$ pro každý vektor $\mathbf{u} \in U$, $\mathbf{u} \neq P_U(\mathbf{v})$.*

Důkaz. Stačí využít Větu 3.6, pro ortogonální dvojici vektorů $P_U(\mathbf{v}) - \mathbf{u} \in U$ a $\mathbf{v} - P_U(\mathbf{v}) = P_U^\perp(\mathbf{v}) \in U^\perp$:

$$\|\, \mathbf{v} - P_U(\mathbf{v})\|_g^2 + \|P_U(\mathbf{v}) - \mathbf{u}\,\|_g^2 = \|\, \mathbf{v} - P_U(\mathbf{v}) + P_U(\mathbf{v}) - \mathbf{u}\,\|_g^2 = \|\, \mathbf{v} - \mathbf{u}\,\|_g^2.$$

Z předpokladu $\mathbf{u} \neq P_U(\mathbf{v})$, díky 3.3 plyne, že (a) $\|P_U(\mathbf{v}) - \mathbf{u}\,\|_g > 0$, a proto $\|\, \mathbf{v} - P_U(\mathbf{v})\|_g^2 < \|\, \mathbf{v} - P_U(\mathbf{v})\|_g^2 + \|P_U(\mathbf{v}) - \mathbf{u}\,\|_g^2$. Dostáváme, že $\|\, \mathbf{v} - P_U(\mathbf{v})\|_g^2 < \|\, \mathbf{v} - \mathbf{u}\,\|_g^2$, a závěr získáme po odmocnění. □

Příklad (Metoda nejmenších čtverců)**.** Buď $A\mathbf{x}^{\mathrm{T}} = \mathbf{y}^{\mathrm{T}}$ nehomogenní soustava m rovnic o n neznámých nad tělesem $T = \mathbf{R}$ nebo $\mathbf{C}$ a označme $\mathbf{a}_i$ sloupce matice $\mathbf{A}$ zapsané do řádků, tj. $\mathbf{A} = (\mathbf{a}_1^{\mathrm{T}} | \mathbf{a}_2^{\mathrm{T}} | \dots | \mathbf{a}_n^{\mathrm{T}})$. Pokud soustava nemá řešení, potom $\mathbf{y} \notin \langle \mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n \rangle$. Soustavu můžeme v takovém případě vyřešit pouze "přibližně", tj. musíme vzít nějaký nový vektor pravých stran $\mathbf{y}'$, který by už ležel v podprostoru $U = \langle \mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n \rangle$. Uvažujeme-li na prostoru T^n standardní skalární součin

ω, je podle Poznámky 3.17 $P_U(\mathbf{y})$ nejbližší (ve smyslu vzdálenosti, kterou jsme pomocí normy zavedli v této kapitole) vektor k vektoru $\mathbf{y}$ ležící v podprostoru U. Řešení nové soustavy rovnic $\mathbf{A}\mathbf{x}^{\mathrm{T}} = P_U(\mathbf{y})^{\mathrm{T}}$ nazveme přibližným řešením nalezené metodou nejmenších čtverců. Při samotném počítání postupujeme obdobně jako v předchozím příkladu.

Mějme soustavu rovnic:

$$\begin{array}{llll} x_1 & +2x_2 & & = 0 \\ 2x_1 & +x_2 & +2x_3 & = 0 \\ x_1 & -2x_2 & +x_3 & = 10 \\ x_1 & +2x_2 & +2x_3 & = 7 \\ & x_2 & -x_3 & = 3 \end{array}$$

Snadno nahlédneme, že soustava nemá řešení. Budeme hledat přibližné řešení metodou nejmenších čtverců. Máme vektor pravých stran $\mathbf{y} = (1, 4, 6, 2, -1)$ a vektory levých stran $\mathbf{a}_1 = (1, 2, 1, 1, 0)$, $\mathbf{a}_2 = (2, 1, -2, 2, 1)$ a $\mathbf{a}_3 = (0, 2, 1, 2, -1)$. Hledáme x_i tak, aby $P_{\langle \mathbf{a}_i \rangle}(\mathbf{y}) = \sum_{i=1}^{3} x_i \mathbf{a}_i$. To vede stejně jako v případě ortogonální projekce k soustavě rovnic s maticí

$$\left(\begin{array}{ccc|c} \omega(\mathbf{a}_1, \mathbf{a}_1) & \omega(\mathbf{a}_1, \mathbf{a}_2) & \omega(\mathbf{a}_1, \mathbf{a}_3) & \omega(\mathbf{a}_1, \mathbf{y}) \\ \omega(\mathbf{a}_2, \mathbf{a}_1) & \omega(\mathbf{a}_2, \mathbf{a}_2) & \omega(\mathbf{a}_2, \mathbf{a}_3) & \omega(\mathbf{a}_2, \mathbf{y}) \\ \omega(\mathbf{a}_3, \mathbf{a}_1) & \omega(\mathbf{a}_3, \mathbf{a}_2) & \omega(\mathbf{a}_3, \mathbf{a}_3) & \omega(\mathbf{a}_3, \mathbf{y}) \end{array}\right).$$

Dosadíme a hledáme řešení soustavy rovnic s maticí

$$\left(\begin{array}{ccc|c} 7 & 4 & 7 & 17 \\ 4 & 14 & 3 & -3 \\ 7 & 3 & 10 & 21 \end{array}\right).$$

Zbývá nám dopočítat, že $x_1 = 2$, $x_2 = -1$ a $x_3 = 1$.

4. Vlastní čísla a vlastní vektory

Podobně jako nad reálnými nebo komplexními čísly budeme nad každým tělesem T pokládat za polynom zobrazení $p : T \to T$, které libovolnému prvku $t \in T$ přiřadí hodnotu $p(t) = \sum_{i=0}^{n} a_i t^i$, pro nějaké pevně zvolené skaláry $a_0, \ldots, a_n \in T$. Kořenem polynomu budeme rozumět každé číslo $t_0 \in T$, pro které $p(t_0) = 0$. Všimněme si, že polynomy lze sčítat a násobit a výsledkem těchto operací je opět polynom.

Definice. Nechť $\mathbf{A}$ je čtvercová matice stupně n nad tělesem T a $\mathbf{E}$ je jednotková matice stupně n. *Vlastním číslem matice* $\mathbf{A}$ nazveme každé $\lambda \in T$, pro nějž bude matice $\mathbf{A} - \lambda\mathbf{E}$ singulární. Každé nenulové řešení $\mathbf{v}_\lambda \in T^n$ homogenní soustavy rovnic s maticí $\mathbf{A} - \lambda\mathbf{E}$ potom budeme nazývat *vlastním vektorem* příslušným vlastnímu číslu λ. Množině $\sigma(\mathbf{A})$ všech vlastních čísel matice budeme říkat *spektrum* matice $\mathbf{A}$. Konečně *charakteristickým polynomem* matice $\mathbf{A}$ nazveme polynom $p(\lambda) = \det(\mathbf{A} - \lambda\mathbf{E})$.

Poznámka 4.1. *Buď $\mathbf{A}$ čtvercová matice stupně n nad tělesem T. Pak je λ vlastní číslo matice $\mathbf{A}$ a $\mathbf{v}_\lambda \in T^n$ jemu příslušný vlastní vektor právě tehdy, když $\mathbf{v}_\lambda \neq \mathbf{0}$ a $\mathbf{A}\,\mathbf{v}_\lambda^{\mathrm{T}} = \lambda\,\mathbf{v}_\lambda^{\mathrm{T}}$.*

Důkaz. Je-li λ vlastní číslo matice $\mathbf{A}$ a $\mathbf{v}_\lambda \in T^n$ příslušný vlastní vektor, tedy $\mathbf{v}_\lambda$ je řešení homogenní soustavy rovnic se čtvercovou singulární maticí $\mathbf{A} - \lambda\mathbf{E}$, pak

$(\mathbf{A} - \lambda\mathbf{E}) \cdot \mathbf{v}_\lambda^\mathsf{T} = \mathbf{0}^\mathsf{T}$, proto $\mathbf{A}\,\mathbf{v}_\lambda^\mathsf{T} = \lambda\mathbf{E} \cdot \mathbf{v}_\lambda^\mathsf{T} = \lambda\,\mathbf{v}_\lambda^\mathsf{T}$. Naopak, jestliže $\mathbf{A}\,\mathbf{v}_\lambda^\mathsf{T} = \lambda\,\mathbf{v}_\lambda^\mathsf{T}$, pak $(\mathbf{A} - \lambda\mathbf{E}) \cdot \mathbf{v}_\lambda^\mathsf{T} = \mathbf{0}^\mathsf{T}$, proto matice $\mathbf{A} - \lambda\mathbf{E}$ musí být singulární, tedy λ je vlastní číslo a vektor $\mathbf{v}_\lambda$ je podle definice jemu příslušný vlastní vektor. □

Poznámka 4.2. *Skalár λ je vlastní číslo matice $\mathbf{A}$ právě tehdy, když je λ kořenem charakteristického polynomu matice $\mathbf{A}$.*

Důkaz. Stačí uvážit, že je díky pozorování z loňského semestru matice $\mathbf{A} - \lambda\mathbf{E}$ singulární, právě když je $p(\lambda) = \det(\mathbf{A} - \lambda\mathbf{E}) = 0$. □

Příklad. (1) Hledejme vlastní vektory a vlastní čísla reálné matice $A = \begin{pmatrix} 2 & 2 \\ 1 & 3 \end{pmatrix}$. Nejprve určíme charakteristický polynom $\det(\mathbf{A} - \lambda\mathbf{E}) = \lambda^2 - 5\lambda + 4 = (\lambda - 1)(\lambda - 4)$, tedy vlastní čísla jsou 1 a 4. Dále spočítáme množinu všech řešení homogenních soustav rovnic:

$$\mathbf{A} - \mathbf{E} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \qquad \mathbf{A} - 4 \cdot \mathbf{E} = \begin{pmatrix} -2 & 2 \\ 1 & -1 \end{pmatrix}.$$

Vidíme, že všechny nenulové násobky vektoru $(-2, 1)$ jsou vlastními vektory příslušnými vlastnímu číslu 1 a všechny nenulové násobky vektoru $(1, 1)$ jsou vlastními vektory příslušnými vlastnímu číslu 4.

(2) Reálná matice $\mathbf{B} = \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix}$ nemá žádná reálná vlastní čísla, a tedy ani žádné vlastní vektory, neboť její charakteristický polynom je $\lambda^2 + 1$.

Poznámka 4.3. *Nechť $\mathbf{A}$ a $\mathbf{P}$ jsou čtvercové matice stupně n nad tělesem T, $\mathbf{P}$ je navíc regulární. Potom jsou charakteristické polynomy matic $\mathbf{A}$ a $\mathbf{P}^{-1}\mathbf{A}\mathbf{P}$ stejné, a proto $\sigma(\mathbf{A}) = \sigma(\mathbf{P}^{-1}\mathbf{A}\mathbf{P})$.*

Důkaz. Protože díky distributivitě násobení a sčítání matic je $\mathbf{P}^{-1} \cdot (\mathbf{A} - \lambda\mathbf{E}) \cdot \mathbf{P} = \mathbf{P}^{-1} \cdot \mathbf{A} \cdot \mathbf{P} - \mathbf{P}^{-1} \cdot \lambda\mathbf{E} \cdot \mathbf{P} = \mathbf{P}^{-1} \cdot \mathbf{A} \cdot \mathbf{P} - \lambda\mathbf{E}$, dostáváme

$$\det(\mathbf{P}^{-1} \cdot \mathbf{A} \cdot \mathbf{P} - \lambda\mathbf{E}) = \det(\mathbf{P})^{-1} \cdot \det(\mathbf{A} - \lambda\mathbf{E}) \cdot \det(\mathbf{P}) = \det(\mathbf{A} - \lambda\mathbf{E}).$$

□

Definice. Nechť $\varphi : V \to V$ je endomorfismus vektorového prostoru V nad tělesem T. Řekneme, že $\lambda \in T$ je *vlastní číslo endomorfismu* φ, existuje-li nenulový vektor $\mathbf{v}_\lambda \in V$, pro který $\varphi(\mathbf{v}_\lambda) = \lambda\,\mathbf{v}_\lambda$. Vektor $\mathbf{v}_\lambda$ potom nazveme *vlastním vektorem endomorfismu* φ příslušným vlastnímu číslu λ. Množině $\sigma(\varphi)$ všech vlastních čísel endomorfismu φ budeme říkat *spektrum* endomorfismu φ.

Endomorfismu vektorového prostoru se často říká lineární operátor na prostoru. Je-li φ endomorfismus na prostoru konečné dimenze V a B báze V označujme $[\varphi]_B$ matici φ vzhledem k bázi B.

Věta 4.4. *Mějme V konečně dimenzionální vektorový prostor, φ nějaký endomorfismus na V a B libovolnou bázi V. Potom $\sigma(\varphi) = \sigma([\varphi]_B)$ a $\mathbf{v}$ je vlastní vektor endomorfismu φ právě tehdy když $\{\mathbf{v}\}_B$ je vlastní vektor matice $[\varphi]_B$.*

Důkaz. Podle Poznámky 4.1 je λ vlastní číslo matice $[\varphi]_B$ a $\{\mathbf{v}_\lambda\}_B$ je jemu příslušný vlastní vektor právě tehdy, když $[\varphi]_B\{\mathbf{v}_\lambda\}_B^\mathsf{T} = \lambda\{\mathbf{v}_\lambda\}_B^\mathsf{T}$. To ovšem nastává tehdy a jen tehdy, když $\varphi(\mathbf{v}_\lambda) = \lambda\,\mathbf{v}_\lambda$, protože $\{\varphi(\mathbf{v}_\lambda)\}_B^\mathsf{T} = [\varphi]_B\{\mathbf{v}_\lambda\}_B^\mathsf{T}$. Konečně $\mathbf{v}_\lambda \neq \mathbf{0}$, právě když $\{\mathbf{v}_\lambda\}_B \neq \mathbf{0}$. □

Příklad. Najdeme vlastní čísla a vlastní vektory endomorfismu $\varphi : \mathbb{Z}_5^2 \to \mathbb{Z}_5^2$ daného předpisem $\varphi((x,y)) = (y, x+4y)$. Podle Věty 4.4 nám stačí najít vlastní čísla a vlastní vektory matice $[\varphi]_{K_2} = \begin{pmatrix} 0 & 1 \\ 1 & 4 \end{pmatrix}$ endomorfismu φ vzhledem ke kanonické bázi K_2. Tedy $\begin{vmatrix} 0-\lambda & 1 \\ 1 & 4-\lambda \end{vmatrix} = \lambda^2 - 4\lambda + 4 = (\lambda - 2)^2$. Našli jsme jedno vlastní číslo $\lambda = 2$ matice $[\varphi]_{K_2}$ i endomorfismu φ. Snadno nahlédneme, že vektory $(1,2)$, $(2,4)$, $(3,1)$ a $(4,3)$ jsou právě všechny vlastní vektory matice $[\varphi]_{K_2}$. Podle Věty 4.4 jsou to zároveň souřadnice vlastního vektoru vzhledem ke kanonické bázi. Tudíž vektory $(1,2)$, $(2,4)$, $(3,1)$, $(4,3)$ jsou všechny vlastní vektory endomorfismu φ.

Poznámka 4.5. *Buď φ endomorfismus na prostoru V konečné dimenze a buď B báze V. Matice $[\varphi]_B$ je diagonální právě tehdy, když jsou všechny vektory báze B vlastními vektory endomorfismu φ.*

Důkaz. Označme $B = (\mathbf{b}_1, \dots, \mathbf{b}_n)$ a $(a_{ij}) = [\varphi]_B$. Je-li $[\varphi]_B$ diagonální, pak $\varphi(\mathbf{b}_i) = a_{ii} \cdot \mathbf{b}_i$, tedy a_{ii} jsou vlastní čísla a $\mathbf{b}_i$ jim příslušné vlastní vektory, $i = 1, \dots n$. Naopak, jsou-li vektory $\mathbf{b}_i$ vlastní vektory, pak $\varphi(\mathbf{b}_i) = \lambda_i \cdot \mathbf{b}_i$ pro vlastní čísla λ_i, tedy $\{\varphi(\mathbf{b}_i)\}_B = \lambda_i \mathbf{e}_i$, a proto je matice $[\varphi]_B$ diagonální s vlastními čísly λ_i na diagonále. □

Věta 4.6. *Nechť $\lambda_1, \dots, \lambda_k$ jsou různá vlastní čísla endomorfismu φ na prostoru V a $\mathbf{v}_{\lambda_1}, \dots, \mathbf{v}_{\lambda_k}$ jsou po po řadě jim příslušné vlastní vektory. Potom je posloupnost vektorů $\mathbf{v}_{\lambda_1}, \dots, \mathbf{v}_{\lambda_k}$ lineárně nezávislá.*

Důkaz. Dokazujeme indukcí podle počtu vlastních čísel i.

Vlastní vektor $\mathbf{v}_{\lambda_1}$ je podle definice nenulový, to znamená, že jednočlená posloupnost obsahující pouze $\mathbf{v}_{\lambda_1}$ je lineárně nezávislá.

Předpokládejme, že $\mathbf{v}_{\lambda_1}, \dots, \mathbf{v}_{\lambda_{i-1}}$ je lineárně nezávislá posloupnost, a položme $\sum_{j=1}^i a_j \mathbf{v}_{\lambda_j} = \mathbf{0}$. Potom $\mathbf{0} = \varphi(\sum_{j=1}^i a_j \mathbf{v}_{\lambda_j}) = \sum_{j=1}^i a_j \varphi(\mathbf{v}_{\lambda_j}) = \sum_{j=1}^i a_j \lambda_j \mathbf{v}_{\lambda_j}$. Dále $\mathbf{0} = \lambda_i \sum_{j=1}^i a_j \mathbf{v}_{\lambda_j} = \sum_{j=1}^i a_j \lambda_i \mathbf{v}_{\lambda_j}$, proto

$$\mathbf{0} = (\sum_{j=1}^i a_j \lambda_i \mathbf{v}_{\lambda_j}) - (\sum_{j=1}^i a_j \lambda_j \mathbf{v}_{\lambda_j}) = \sum_{j=1}^i a_j (\lambda_i - \lambda_j) \mathbf{v}_{\lambda_j} = \sum_{j=1}^{i-1} a_j (\lambda_i - \lambda_j) \mathbf{v}_{\lambda_j} .$$

Z indukčního předpokladu plyne, že $a_j(\lambda_i - \lambda_j) = 0$, a dále $\lambda_i \neq \lambda_j$ pro všechna $j = 1, \dots, i-1$. Proto $a_j = 0$ pro všechna $j = 1, \dots, i-1$. Protože $\mathbf{v}_{\lambda_i} \neq \mathbf{0}$ a $a_i \mathbf{v}_{\lambda_i} = \sum_{j=1}^i a_j \mathbf{v}_{\lambda_j} = 0$, dostáváme, že $a_i = 0$. Tudíž posloupnost vektorů $\mathbf{v}_{\lambda_1}, \dots, \mathbf{v}_{\lambda_i}$ je podle definice lineárně nezávislá. □

Definice. Řekneme, že dvě čtvercové matice $\mathbf{A}$ a $\mathbf{B}$ stupně n nad tělesem T jsou *podobné* (značíme $\mathbf{A} \sim \mathbf{B}$), existuje-li regulární matice $\mathbf{P}$ stupně n nad tělesem T, pro kterou $\mathbf{A} = \mathbf{P}^{-1}\mathbf{B}\mathbf{P}$.

Poznámka 4.7. *Jestliže $\mathbf{A} \sim \mathbf{B}$, pak $\sigma(\mathbf{A}) = \sigma(\mathbf{B})$.*

Důkaz. Plyne okamžitě z 4.3. □

Poznámka 4.8. *Relace podobnosti je ekvivalencí na množině všech čtvercových matice stupně n nad tělesem T.*

Důkaz. Relace je reflexivní, tedy $\mathbf{A} \sim \mathbf{A}$, protože $\mathbf{A} = \mathbf{E}^{-1}\mathbf{A}\mathbf{E}$. Jestliže $\mathbf{A} \sim \mathbf{B}$, tj. $\mathbf{A} = \mathbf{P}^{-1}\mathbf{B}\mathbf{P}$, pak $\mathbf{B} = (P^{-1})^{-1}\mathbf{A}\mathbf{P}^{-1}$, kde $\mathbf{P}^{-1}$ je regulární matice, tedy $\mathbf{B} \sim \mathbf{A}$ a relace $\sim$ je symetrická. Konečně předpokládejme, že $\mathbf{A} \sim \mathbf{B}$ a $\mathbf{B} \sim \mathbf{C}$, tj. $\mathbf{A} = \mathbf{P}^{-1}\mathbf{B}\mathbf{P}$ a $\mathbf{B} = \mathbf{Q}^{-1}\mathbf{C}\mathbf{Q}$. Pak stačí položit $\mathbf{S} = \mathbf{Q} \cdot \mathbf{P}$, abychom dostali $\mathbf{A} = \mathbf{S}^{-1}\mathbf{C}\mathbf{S}$, tedy $\mathbf{A} \sim \mathbf{C}$, čímž jsme ověřili tranzitivitu $\sim$. □

Poznámka 4.9. *Nechť φ je endomorfismus na prostoru V konečné dimenze n, $\mathbf{A}$ je čtvercová matice stupně n a B je báze V. Pak matice $[\varphi]_B$ a $\mathbf{A}$ jsou podobné právě tehdy, když existuje báze C prostoru V tak, že $[\varphi]_C = \mathbf{A}$.*

Důkaz. Stačí si uvědomit, že $[\varphi]_B = [\mathrm{Id}]_{BC}^{-1} \cdot [\varphi]_C \cdot [\mathrm{Id}]_{BC}$. □

Definice. Řekneme, že endomorfismu φ na prostoru V konečné dimenze je *diagonalizovatelný*, pokud existuje báze B, vůči níž je matice $[\varphi]_B$ diagonální. Řekneme, že čtvercové matice $\mathbf{A}$ je *diagonalizovatelná*, je-li $\mathbf{A}$ podobná nějaké diagonální matici.

Důsledek 4.10. *Buď V konečně dimenzionální prostor, B nějaká jeho báze a φ endomorfismus na V. Pak φ je diagonalizovatelný právě tehdy, když je matice $[\varphi]_B$ diagonalizovatelná.*

Věta 4.11. *Nechť V je konečně dimenzionální prostor a φ endomorfismus na V. Následující tvrzení jsou ekvivalentní:*

(1) *φ je diagonalizovatelný,*
(2) *existuje báze V složená z vlastních vektorů endomorfismu φ,*
(3) $V = \bigoplus_{\lambda\in\sigma(\varphi)} \mathrm{Ker}(\varphi - \lambda \cdot \mathrm{Id})$.

Důkaz. (1) $\Leftrightarrow$ (2) Ekvivalence je obsahem Poznámky 4.5.

(2) $\Rightarrow$ (3) Označme $V_\lambda = \mathrm{Ker}(\varphi - \lambda \cdot \mathrm{Id})$. Každý vektor báze prostoru V složené z vlastních vektorů přitom leží v podprostoru V_λ pro nějaké vlastní číslo $\lambda \in \sigma(\varphi)$, a proto $V = \sum_{\lambda\in\sigma(\varphi)} V_\lambda$. Nechť $\mathbf{u}_i \in V_{\lambda_i}$, kde $i = 1, \dots, k$ a $\lambda_i \neq \lambda_j$ pro $i \neq j$. Pokud $\mathbf{u}_1 + \cdots + \mathbf{u}_k = \mathbf{0}$, potom $\mathbf{u}_i = \mathbf{0}$ pro všechna $i = 1, \dots, k$ podle 4.6, a proto $V = \bigoplus_{\lambda\in\sigma(\varphi)} V_\lambda$.

(3) $\Rightarrow$ (2) Zvolme bázi B_λ podprostoru $\mathrm{Ker}(\varphi-\lambda\cdot\mathrm{Id})$ pro každé $\lambda \in \sigma(\varphi)$. Zřejmě jsou všechny vektory z bází B_λ nenulové, a proto vlastní. Dále $B = \bigcup_{\lambda\in\sigma(\varphi)} B_\lambda$ je lineárně nezávislou generující množinou, tedy bází prostoru V. □

Vezmeme-li pro libovolnou čtvercovou matici $\mathbf{A}$ endomorfismus φ na T^n s maticí vzhledem ke kanonické bázi $[\varphi]_{K_n} = \mathbf{A}$ dostáváme:

Důsledek 4.12. *Nechť $\mathbf{A}$ je čtvercová matice stupně n nad tělesem T. Následující tvrzení jsou ekvivalentní:*

(1) *$\mathbf{A}$ je diagonalizovatelná,*
(2) *existuje báze T^n složená z vlastních vektorů matice $\mathbf{A}$,*
(3) $T^n = \bigoplus_{\lambda\in\sigma(\mathbf{A})}\{\mathbf{x} \in T^n | \ (\mathbf{A} - \lambda E)\mathbf{x}^{\mathrm{T}} = \mathbf{0}^{\mathrm{T}}\}$.

Poznámka 4.13. *Nechť $\mathbf{A}$ je čtvercová matice stupně n a φ je endomorfismus na prostoru dimenze n.*

(a) *Má-li φ n různých vlastních čísel, je diagonalizovatelný.*
(b) *Má-li $\mathbf{A}$ n různých vlastních čísel, je $\mathbf{A}$ diagonalizovatelná.*

Důkaz. (a) Vezmememe-li pro každé vlastní číslo endomorfismu φ jemu příslušný vlastní vektor, dostaneme podle 4.6 lineárně nezávislou posloupnost n vektorů ve vektorovém prostoru dimenze n, tedy půjde o bázi složenou z vlastních vektorů. Použijeme-li 4.11, vidíme, že je φ diagonalizovatelný endomorfismus.

(b) Podobně jako u 4.12 dostáváme z (a) a Důsledku 4.10. □

Příklad. (1) Reálná matice $\mathbf{A} = \begin{pmatrix} 2 & 2 \\ 1 & 3 \end{pmatrix}$ má dvě různá vlastní čísla, tedy je podle Poznámky 4.13 diagonalizovatelná. Budeme-li matici $\mathbf{A}$ interpretovat jako matici $[\varphi]_{K_2}$ endomorfismu φ například vzhledem ke kanonické bázi K_2, pak $[\varphi]_B = [\mathrm{Id}]_{K_2B}[\varphi]_{K_2}[\mathrm{Id}]_{BK_2} = [\mathrm{Id}]^{-1}_{BK_2}[\varphi]_{K_2}[\mathrm{Id}]_{BK_2}$, kde B je báze sestávající z vlastních vektorů matice $\mathbf{A}$. To znamená, že

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

(2) O endomorfismu φ na $\mathbb{Z}_5^2$ daném předpisem $\varphi((x, y)) = (y, x + 4y)$ jsme zjistili, že má "málo" vlastních vektorů, tedy neexistuje báze $\mathbb{Z}_5^2$ složená z vlastních vektorů endomorfismu φ, a proto φ není podle Věty 4.11 diagonalizovatelný.

(3) Reálná trojúhelníková matice $\mathbf{M} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 2 & 3 & 1 \end{pmatrix}$ má zřejmě charakteristický polynom $(2 - \lambda)^2(1 - \lambda)$, a tudíž $\sigma(\mathbf{M}) = \{1, 2\}$. Hledáme-li množinu všech řešení homogenní soustavy rovnic s maticí $\mathbf{M} - 1\mathbf{E}$, tj. vlastní vektory příslušné vlastnímu číslu 1, vidíme, že existuje jen jeden lineárně nezávislý takový vlastní vektor, protože dimenze podprostoru všech řešení je $3 - h(\mathbf{M} - 1\mathbf{E}) = 3 - 2 = 1$. Podprostor všech řešení homogenní soustavy rovnic s maticí $\mathbf{M} - 2\mathbf{E}$ je ovšem dvoudimenzionální, protože hodnost matice $\mathbf{M} - 2\mathbf{E}$ je $h(\mathbf{M} - 2\mathbf{E}) = 1$. Tedy pro vlastní číslo 2 dostáváme dva lineárně nezávislé vlastní vektory. Podle Věty 4.6 (nebo přímo Poznámky 4.12) máme tříprvkou lineárně nezávislou množinu vlastních vektorů v třídimenzionálním prostoru, tedy jde o bázi a matice $\mathbf{M}$ je diagonalizovatelná.

(4) Reálná trojúhelníková matice $\mathbf{N} = \begin{pmatrix} 2 & 0 & 0 \\ 4 & 2 & 0 \\ 2 & 3 & 1 \end{pmatrix}$ má stejný charakteristický polynom $(2-\lambda)^2(1-\lambda)$ jako matice $\mathbf{M}$, a proto i $\sigma(\mathbf{N}) = \{1, 2\}$. Zřejmě $h(\mathbf{N}-1E) = h(\mathbf{N} - 2E) = 2$, tedy podprostory $\{\mathbf{x} \in \mathbf{R}^3 | \ (\mathbf{N} - \lambda\mathbf{E})\mathbf{x}^{\mathrm{T}} = \mathbf{0}^{\mathrm{T}}\}$ pro $\lambda = 1, 2$ jsou jen jednodimenzionální. Tudíž neexistuje báze prostoru $\mathbf{R}^3$ složená z vlastních vektorů matice $\mathbf{N}$ a matice $\mathbf{N}$ není diagonalizovatelná.

Definice. Řekneme, že reálná nebo komplexní čtvercová matice $\mathbf{U}$ je *unitární*, jestliže $\overline{\mathbf{U}}^{\mathrm{T}}\mathbf{U} = \mathbf{E}$.

Reálná unitární matice se často nazývá ortogonální maticí.

Poznámka 4.14. *Je-li* $\mathbf{U}$ *unitární matice, pak* $\mathbf{U}$ *je regulární,* $\mathbf{U}^{-1} = \overline{\mathbf{U}}^{\mathrm{T}}$ *a* $\overline{\mathbf{U}}^{\mathrm{T}}$ *je také unitární.*

Důkaz. Protože je součin $\overline{\mathbf{U}}^{\mathrm{T}}\mathbf{U}$ regulární matice musí být i $\mathbf{U}$ regulární, navíc z jednoznačnosti existence inverzní matice plyne, že $\mathbf{U}^{-1} = \overline{\mathbf{U}}^{\mathrm{T}}$. Konečně $\mathbf{U}^{-1} = \overline{\mathbf{U}}^{\mathrm{T}}$ je unitární matice, protože $\mathbf{U}\mathbf{U}^{-1} = \mathbf{E}$. □

Důsledek 4.15. *Matice stupně n nad tělesem $T = \mathbf{R}$ nebo $\mathbf{C}$ je unitární právě tehdy, když obsahuje ve sloupcích (v řádcích) ortonormální bázi unitárního prostoru (T^n, ω).*

Poznámka 4.16. *Součin dvou unitárních matic stejného stupně je opět unitární matice.*

Důkaz. Z definice plyne, že $\overline{(\mathbf{UV})}^T \mathbf{UV} = \overline{\mathbf{V}}^T \overline{\mathbf{U}}^T \mathbf{UV} = \overline{\mathbf{V}}^T \mathbf{EV} = \overline{\mathbf{V}}^T \mathbf{V} = \mathbf{E}$. □

Poznámka 4.17. *Buď B ortonormální báze unitárního prostoru (V, g) a C je nějaká báze V. Pak je C ortonormální, právě když je matice přechodu $[\mathrm{Id}]_{CB}$ unitární.*

Důkaz. Buď $n = \dim V$ a $B = (\mathbf{b}_1, \dots, \mathbf{b}_n)$, $C = (\mathbf{c}_1, \dots, \mathbf{c}_n)$. Podle 3.12 existuje unitární izomorfismus $\varphi : V \to T^n$ unitárních prostorů (V, g) a (T^n, ω), pro nějž $\varphi(\mathbf{b}_i) = \mathbf{e}_i$, $i = 1, \dots n$, tedy pro každé j, k platí, že

$$\omega(\{\mathbf{c}_j\}_B \cdot \{\mathbf{c}_k\}_B) = g(\mathbf{c}_j, \mathbf{c}_k)$$

Je-li C ortonormální, pak jsou sloupce matice $[\mathrm{Id}]_{CB}$ ortonormální vzhledem k ω, a proto je $[\mathrm{Id}]_{CB}$ unitární podle 4.15. Naopak, je-li $[\mathrm{Id}]_{CB}$ unitární matice, tedy její sloupce jsou ortonormální, pak $g(\mathbf{c}_j, \mathbf{c}_k) = \delta_{jk}$, tudíž C je ortonormální báze unitárního prostoru (V, g). □

Definice. Nechť je $\mathbf{A}$ čtvercová matice nad tělesem $T = \mathbf{R}$ nebo $\mathbf{C}$ a φ endomorfismus na unitárním prostoru (V, g). Řekneme, že $\mathbf{A}$ je *unitárně diagonalizovatelná*, existuje-li taková unitární matice $\mathbf{U}$ nad T, že $\overline{\mathbf{U}}^{\mathsf{T}}\mathbf{AU}$ je diagonální, a φ je *unitárně diagonalizovatelný*, existuje-li ortonormální báze B prostoru (V, g) složená z vlastních vektorů endomorfismu φ. Matici nazveme $\mathbf{A}$ je *normální*, jestliže $\mathbf{A} \cdot \overline{\mathbf{A}}^{\mathsf{T}} = \overline{\mathbf{A}}^{\mathsf{T}} \cdot \mathbf{A}$.

Příklad. (1) Každá diagonální matice je podle definice normální.

(2) Reálná symetrická matice je přímo z definice normální.

(3) Komplexní matice splňující podmínku $\mathbf{A} = \overline{\mathbf{A}}^{\mathsf{T}}$ je normální, neboť v takovém případě $\mathbf{A}\overline{\mathbf{A}}^{\mathsf{T}} = \mathbf{AA} = \overline{\mathbf{A}}^{\mathsf{T}}\mathbf{A}$.

(4) Unitární matice je díky 4.14 normální.

Věta 4.18. *Buď φ endomorfismus na konečně dimenzionálním unitárním prostoru (V, g) a buď B ortonormální báze (V, g). Pak je ekvivalntní:*

1. *φ je unitárně diagonalizovatelný,*
2. *existuje taková ortonormální báze C prostoru (V, g), že $[\varphi]_C$ je diagonální matice,*
3. *matice $[\varphi]_B$ je unitárně diagonalizovatelná.*

Důkaz. (1)⇔(2) Podle 4.5 je endomorfismus φ unitárně diagonalizovatelný, tj. existuje ortonormální báze C prostoru (V, g) složená z vlastních vektorů endomorfismu φ, právě tehdy existuje-li ortonormální báze C, pro niž je $[\varphi]_C$ diagonální matice.

(2)⇒(3) Buď C ortonormální báze prostoru (V, g), pro níž je $[\varphi]_C$ diagonální matice. Potom je díky 4.17 matice $\mathbf{U} = [\mathrm{Id}]_{CB}$ unitární, a proto podle 4.14 $[\mathrm{Id}]_{BC} = \mathbf{U}^{-1} = \overline{\mathbf{U}}^{\mathsf{T}}$ Protože víme z minulého semestru, že $[\varphi]_C = [\mathrm{Id}]_{BC}[\varphi]_B[\mathrm{Id}]_{CB}$, dostáváme, že $[\varphi]_C = \overline{\mathbf{U}}^{\mathsf{T}}[\varphi]_B\mathbf{U}$ je diagonální, tedy $[\varphi]_B$ je unitárně diagonalizovatelná.

(3)⇒(2) Předpokládejme, že existuje unítární matice $\mathbf{U}$, pro kterou je $\overline{\mathbf{U}}^{\mathsf{T}}[\varphi]_B\mathbf{U}$ diagonální. Pak existuje jednoznačně určená báze C, pro niž $\mathbf{U} = [\mathrm{Id}]_{CB}$. Tedy podle 4.17 je báze C ortonormální a $[\varphi]_C = [\mathrm{Id}]_{BC}[\varphi]_B[\mathrm{Id}]_{CB} = \overline{\mathbf{U}}^{\mathrm{T}}[\varphi]_B\mathbf{U}$ je diagonální. $\square$

Poznámka 4.19. *Nechť* $\mathbf{A}$ *je čtvercová matice stupně* n *nad tělesem* $T = \mathbf{R}$ *nebo* $\mathbf{C}$*. Pak je* $\mathbf{A}$ *unitárně diagonalizovatelná, právě když existuje ortonormální báze unitárního prostoru* (T^n, ω) *sestávající z vlastních vektorů matice* $\mathbf{A}$*.*

Důkaz. Poznamenejme, že kanonická báze K_n je ortonormální bází unitárním prostoru (T^n, ω). Uvažujeme-li endomorfismus φ na unitárním prostoru (T^n, ω) s maticí $[\varphi]_{K_n} = \mathbf{A}$, tj. $\varphi(\mathbf{v}) = \mathbf{v}\,\mathbf{A}^{\mathrm{T}}$, pak je podle 4.4 $\mathbf{v}$ vlastní vektor endomorfismu φ, právě když je $\mathbf{v} = \{\mathbf{v}\}_{K_n}$ vlastní vektor matice $\mathbf{A}$, a tvrzení je tudíž důsledkem Věty 4.18. $\square$

Následující tvrzení vyslovíme bez důkazu:

Věta (Základní věta algebry)**.** *Každý komplexní polynom stupně alespoň jedna má komplexní kořen.*

Poznámka 4.20. *Každá neprázdná komplexní čtvercová matice a každý endomorfismus na komplexním prostoru nenulové konečné dimenze mají nějaké vlastní číslo.*

Důkaz. Je-li $\mathbf{A} = (a_{ij})$ čtvercová komplexní matice stupně $n \geq 1$, pak $\det(\mathbf{A} - \lambda\mathbf{E}) = q(\lambda) + \prod_{i=1}^{n}(a_{ii} - \lambda)$, kde polynom $q(\lambda)$ je stupně menšího jak n. Proto má charakteristický polynom stupeň $\det(\mathbf{A} - \lambda\mathbf{E})$ právě n a díky Základní větě algebry tedy existuje jeho kořen, tedy podle 4.2 vlastní číslo $\mathbf{A}$. Existence vlastního čísla endomorfismu potom plyne ze Základní věta algebry Věty 4.4. $\square$

Věta 4.21. *Čtvercová komplexní matice* $\mathbf{A}$ *je unitárně diagonalizovatelná, právě když je normální. Navíc, pokud všechna vlastní čísla normální matice* $\mathbf{A}$ *i všechny hodnoty* $\mathbf{A}$ *jsou reálné, potom* $\mathbf{A}$ *je reálná unitárně diagonalizovatelná matice.*

Důkaz. $(\Rightarrow)$ Je-li $\mathbf{A}$ unitárně diagonalizovatelná, existuje unitární matice $\mathbf{U}$ tak, že $\mathbf{D} = \overline{\mathbf{U}}^{\mathrm{T}}\mathbf{A}\mathbf{U}$ je diagonální. Poznamenejme, že $\overline{\mathbf{D}}^{\mathrm{T}}\mathbf{D} = \mathbf{D}\overline{\mathbf{D}}^{\mathrm{T}}$ a $\mathbf{A} = \mathbf{U}\mathbf{D}\overline{\mathbf{U}}^{\mathrm{T}}$. Tudíž

$$\begin{aligned}\mathbf{A}\overline{\mathbf{A}}^{\mathrm{T}} &= \mathbf{U}\mathbf{D}\overline{\mathbf{U}}^{\mathrm{T}}\overline{\mathbf{U}\mathbf{D}\overline{\mathbf{U}}^{\mathrm{T}}}^{\mathrm{T}} = \mathbf{U}\mathbf{D}\overline{\mathbf{U}}^{\mathrm{T}}\mathbf{U}\overline{\mathbf{D}}^{\mathrm{T}}\overline{\mathbf{U}}^{\mathrm{T}} = \mathbf{U}\mathbf{D}\overline{\mathbf{D}}^{\mathrm{T}}\overline{\mathbf{U}}^{\mathrm{T}}\\ &= \mathbf{U}\overline{\mathbf{D}}^{\mathrm{T}}\mathbf{D}\overline{\mathbf{U}}^{\mathrm{T}} = \overline{\mathbf{U}\mathbf{D}\overline{\mathbf{U}}^{\mathrm{T}}}^{\mathrm{T}}\mathbf{U}\mathbf{D}\overline{\mathbf{U}}^{\mathrm{T}} = \overline{\mathbf{A}}^{\mathrm{T}}\mathbf{A}.\end{aligned}$$

Tím jsme ověřili, že $\mathbf{A}$ je normální matice.

$(\Leftarrow)$ Předpokládejme, že je matice $\mathbf{A}$ normální. Nejprve ukážeme, že pokud $\mathbf{A}\,\mathbf{v}^{\mathrm{T}} = \lambda\,\mathbf{v}^{\mathrm{T}}$ pro nějaké vlastní číslo λ a vlastní vektor $\mathbf{v}$ matice $\mathbf{A}$, pak $\overline{\mathbf{A}}^{\mathrm{T}}\mathbf{v}^{\mathrm{T}} = \overline{\lambda}\,\mathbf{v}^{\mathrm{T}}$. K tomu použijeme vlastností standardního skalárního součinu a jednoduché pozorování, že $\mathbf{A}\,\mathbf{v}^{\mathrm{T}} - \lambda\,\mathbf{v}^{\mathrm{T}} = \mathbf{0}^{\mathrm{T}}$ právě tehdy, když $\mathbf{v}\,\mathbf{A}^{\mathrm{T}} - \lambda\,\mathbf{v} = \mathbf{0}$:

$$\begin{aligned}0 &= \omega(\mathbf{v}\,\mathbf{A}^{\mathrm{T}} - \lambda\,\mathbf{v}, \mathbf{v}\,\mathbf{A}^{\mathrm{T}} - \lambda\,\mathbf{v}) = \overline{(\mathbf{v}\,\mathbf{A}^{\mathrm{T}} - \lambda\,\mathbf{v})}(\mathbf{A}\,\mathbf{v}^{\mathrm{T}} - \lambda\,\mathbf{v}^{\mathrm{T}})\\ &= \overline{\mathbf{v}}\overline{\mathbf{A}}^{\mathrm{T}}\mathbf{A}\,\mathbf{v}^{\mathrm{T}} - \lambda\overline{\mathbf{v}}\overline{\mathbf{A}}^{\mathrm{T}}\mathbf{v}^{\mathrm{T}} - \overline{\lambda}\overline{\mathbf{v}}\mathbf{A}\,\mathbf{v}^{\mathrm{T}} + \overline{\lambda}\lambda\overline{\mathbf{v}}\,\mathbf{v}^{\mathrm{T}} =\\ &= \overline{\mathbf{v}}\mathbf{A}\overline{\mathbf{A}}^{\mathrm{T}}\mathbf{v}^{\mathrm{T}} - \lambda\overline{\mathbf{v}}\overline{\mathbf{A}}^{\mathrm{T}}\mathbf{v}^{\mathrm{T}} - \overline{\lambda}\overline{\mathbf{v}}\mathbf{A}\,\mathbf{v}^{\mathrm{T}} + \overline{\lambda}\lambda\overline{\mathbf{v}}\,\mathbf{v}^{\mathrm{T}} = \omega(\mathbf{v}\,\overline{\mathbf{A}} - \overline{\lambda}\,\mathbf{v}, \mathbf{v}\,\overline{\mathbf{A}} - \overline{\lambda}\,\mathbf{v}).\end{aligned}$$

Podle definice skalárního součinu je $\mathbf{v}\,\overline{\mathbf{A}} - \overline{\lambda}\,\mathbf{v} = \mathbf{0}$, a proto je i vektor $\overline{\mathbf{A}}^{\mathrm{T}}\mathbf{v}^{\mathrm{T}} - \overline{\lambda}\,\mathbf{v}^{\mathrm{T}}$ nulový a $\overline{\lambda}$ je vlastní číslo matice $\overline{\mathbf{A}}^{\mathrm{T}}$.

Buď n stupeň matice $\mathbf{A}$. Budeme postupně hledat ortonormální bázi unitárního prostoru $(\mathbf{C}^n, \omega)$ složenou z vlastních vektorů matice $\mathbf{A}$. Podle Poznámky 4.20 existuje nějaké vlastní číslo λ_1 matice $\mathbf{A}$ a jemu příslušný vlastní vektor $\mathbf{v}_1$, můžeme předpokládat, že $\|\,\mathbf{v}_1\,\|_\omega = 1$. Už víme, že $\overline{\mathbf{A}}^{\mathrm{T}}\mathbf{v}_1^{\mathrm{T}} = \overline{\lambda_1}\,\mathbf{v}_1^{\mathrm{T}}$. Položme $U_1 = \langle\mathbf{v}_1\rangle^{\perp}$.

Ukážeme, že $(\mathbf{A}\,\mathbf{u}^{\mathsf{T}})^{\mathsf{T}} = \mathbf{u}\,\mathbf{A}^{\mathsf{T}} \in U_1$ pro každý vektor $\mathbf{u} \in U_1$. Stačí nám ověřit, že $\omega(\mathbf{u}\,\mathbf{A}^{\mathsf{T}}, \mathbf{v}_1) = 0$, k čemuž využijeme první krok důkazu této implikace:

$$\omega(\mathbf{u}\,\mathbf{A}^{\mathsf{T}}, \mathbf{v}_1) = \overline{\mathbf{u}\,\mathbf{A}^{\mathsf{T}}}\,\mathbf{v}_1^{\mathsf{T}} = \overline{\mathbf{u}}\overline{\mathbf{A}}^{\mathsf{T}}\,\mathbf{v}_1^{\mathsf{T}} = \overline{\lambda_1}\overline{\mathbf{u}}\,\mathbf{v}_1^{\mathsf{T}} = \overline{\lambda_1}\omega(\mathbf{u}, \mathbf{v}_1) = 0,$$

Zobrazení $\varphi_1 : U_1 \to U_1$, které každému $\mathbf{u} \in U$ přiřadí vektor $\varphi_1(\mathbf{u}) = \mathbf{u}\,\mathbf{A}^{\mathsf{T}}$ je zřejmě endomorfismem. Pokud U_1 není nulový prostor, pak podle 4.20 existuje vlastní číslo λ_2 endomorfismu φ_1 a příslušný vlastní vektor $\mathbf{v}_2 \in U_1$, který opět můžeme zvolit normovaný. Tedy $\varphi_1(\mathbf{v}_2) = \mathbf{v}_2\,\mathbf{A}^{\mathsf{T}} = \lambda_2\,\mathbf{v}_2$, dále víme, že $\mathbf{v}_2\,\overline{\mathbf{A}} = \overline{\lambda_2}\,\mathbf{v}_2$, protože λ_2 je rovněž vlastní číslo matice $\mathbf{A}$, a vektory $\mathbf{v}_1$ a $\mathbf{v}_2$ jsou ortonormální. Vezmeme nyní podprostor $U_2 = \langle \mathbf{v}_1, \mathbf{v}_2 \rangle^{\perp}$. Stejným způsobem jako v prvním kroku (tentokrát ovšem pro dva vektory) můžeme dokázat, že $\mathbf{u}\,\mathbf{A}^{\mathsf{T}} \in U_2$ pro každé $\mathbf{u} \in U_2$ a pak definujeme endomorfismus $\varphi_2 : U_2 \to U_2$ opět předpisem $\varphi_2(\mathbf{u}) = \mathbf{u}\,\mathbf{A}^{\mathsf{T}}$. Takto budeme pokračovat, dokud U_i nebude nulový podprostor, což nastane právě v okamžiku, kdy $i = n$. Zkonstruujeme tak ortonormální posloupnost vlastních vektorů $\mathbf{v}_1, \dots, \mathbf{v}_n$ matice a, která tvoří bázi $\mathbf{C}^n$, proto je podle 4.19 matice $\mathbf{A}$ unitárně diagonalizovatelná.

Pokud byly reálné všechny hodnoty matice $\mathbf{A}$ i všechna vlastní čísla λ_i, mohli jsme $\mathbf{A}$ chápat jako matici endomorfismus na reálném unitárním prostoru $(\mathbf{R}^n, \omega)$ vzhledem ke kanonické bázi, resp. φ_i jako endomorfismy na reálných vektorových prostorech U_i. Tedy jsme všechny vlastní vektory $\mathbf{v}_i$ mohli brát reálné. Proto opět pomocí Poznámky 4.19 zjišťujeme, že $\mathbf{A}$ je reálnou unitárně diagonalizovatelnou maticí, tj. existuje taková reálná unitární matice $\mathbf{U}$, že $\overline{\mathbf{U}}^{\mathsf{T}}\mathbf{A}\mathbf{U} = \mathbf{U}^{\mathsf{T}}\mathbf{A}\mathbf{U}$ je diagonální reálnou maticí. □

Příklad. (1) Mějme reálnou symetrickou matici $\mathbf{A}$. Uvážíme, že všechna komplexní vlastní $\mathbf{A}$ jsou reálná. Zvolme $\lambda \in \sigma(\mathbf{A})$ a příslušný vlastní vektor $\mathbf{v}$. V důkazu 4.21 jsme ukázali, že $\overline{\mathbf{A}}^{\mathsf{T}}\,\mathbf{v}^{\mathsf{T}} = \overline{\lambda}\,\mathbf{v}^{\mathsf{T}}$. Protože je $\mathbf{A}$ reálná symetrická, tedy $\overline{\mathbf{A}}^{\mathsf{T}} = \mathbf{A}^{\mathsf{T}} = \mathbf{A}$, vidíme, že $\mathbf{A}\,\mathbf{v}^{\mathsf{T}} = \overline{\lambda}\,\mathbf{v}^{\mathsf{T}}$, tedy $\mathbf{v}$ je vlastní vektor příslušný vlastnímu číslu λ i $\overline{\lambda}$. To ovšem podle 4.6 znamená, že $\lambda = \overline{\lambda}$, tedy λ je reálné. Protože $\sigma(\mathbf{A}) \subseteq \mathbf{R}$ a $\mathbf{A}$ je reálná normální matice, jde podle 4.21 o unitárně diagonalizovatelnou matici nad $\mathbf{R}$.

(2) Buď $\mathbf{A} = \begin{pmatrix} 3 & 2 \\ 2 & 6 \end{pmatrix}$ reálná symetrická matice. Spočítáme charkteristický polynom $\det(\mathbf{A} - \lambda\mathbf{E}) = (3-\lambda)(6-\lambda) - 4 = \lambda^2 - 9\lambda + 14 = (\lambda-2)(\lambda-7)$. Vlastní čísla matice $\mathbf{A}$ jsou tedy právě kořeny charakteristického polynomu, tedy reálná čísla 2 a 7. Dále standardním postupem najdeme vlastní vektory, tedy nenulová řešení homogenních soustav rovnic s maticemi, která tvoří právě souřadnicové vektory vlastních vektorů endomorfismu φ:

$$\mathbf{A} - 2 \cdot \mathbf{E} = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}, \quad \mathbf{A} - 7 \cdot \mathbf{E} = \begin{pmatrix} -4 & 2 \\ 2 & -1 \end{pmatrix}.$$

Tedy všechny nenulové násobky vektoru $(-2, 1)$ jsou vlastními vektory matice $\mathbf{A}$ příslušnými vlastnímu číslu 2 a všechny nenulové násobky vektoru $(1, 2)$ jsou vlastními vektory matice $\mathbf{A}$ příslušnými vlastnímu číslu 7. Oba vektory normalizujeme a dostaneme ortonormální bázi $B = (\frac{1}{\sqrt{5}}(-2, 1), \frac{1}{\sqrt{5}}(1, 2))$. Nyní stačí položit $\mathbf{U} = [\mathrm{Id}]_{BK_3} = \frac{1}{\sqrt{5}} \begin{pmatrix} -2 & 1 \\ 1 & 2 \end{pmatrix}$, aby $\mathbf{U}^{\mathsf{T}}\mathbf{A}\mathbf{U} = \begin{pmatrix} 2 & 0 \\ 0 & 7 \end{pmatrix}$.

Poznámka 4.22. *Nechť* $\mathbf{A}$ *je normální komplexní čtvercová matice a* $\mathbf{u}$*,* $\mathbf{v}$ *dva vlastní vektory* $\mathbf{A}$ *příslušné různým vlastním číslům. Potom* $\mathbf{u}$ *a* $\mathbf{v}$ *jsou ortogonální vzhledem ke standardnímu skalárnímu součinu.*

Důkaz. Stejně jako v 4.19 uvažujme endomorfismus φ na unitárním prostoru (T^n, ω) s maticí $[\varphi]_{K_n} = \mathbf{A}$. Podle 4.21 je $[\varphi]_{K_n}$ unitárně diagonalizovatelná matice, tedy díky 4.18 existuje taková ortonormální báze $C = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ prostoru (T^n, ω), složená z vlastních vektorů, tj. $[\varphi]_C = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ . & . & \dots & . \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$ je diagonální s vlastními čísly $\lambda_1, \dots, \lambda_n$ na diagonále. Protože je zobrazení $\mathbf{v} \to \{\mathbf{v}\}_C$ podle 3.12 unitární automorfismus na (T^n, ω), je $\omega(\mathbf{v}, \mathbf{w}) = \omega(\{\mathbf{v}\}_C, \{\mathbf{w}\}_C)$.

Vezměme nyní dva vlastní vektory $\mathbf{v}$ a $\mathbf{w}$ příslušné různým vlastním číslům $\lambda_{\mathbf{v}}$ a $\lambda_{\mathbf{w}}$ a označme $\{\mathbf{v}\}_C = (a_1, \dots, a_n)$ a $\{\mathbf{w}\}_C = (b_1, \dots, b_n)$. Protože $\{\mathbf{v}\}_C [\varphi]_C^{\mathrm{T}} = \lambda_{\mathbf{v}} \{\mathbf{v}\}_C$ a $\{\mathbf{w}\}_C [\varphi]_C^{\mathrm{T}} = \lambda_{\mathbf{w}} \{\mathbf{v}\}_C$ je $a_i = 0$, jestliže $\lambda_i \neq \lambda_{\mathbf{v}}$, a $b_i = 0$, jestliže $\lambda_i \neq \lambda_{\mathbf{w}}$. Proto $\omega(\mathbf{v}, \mathbf{w}) = \omega(\{\mathbf{v}\}_C, \{\mathbf{w}\}_C) = \overline{\{\mathbf{v}\}_C} \{\mathbf{w}\}_C^{\mathrm{T}} = \sum_{i=1}^n a_i b_i = 0$. □

Příklad. O komplexní matici $\mathbf{A} = \begin{pmatrix} 1 & 1-i & -1 \\ 1+i & 2 & -1-i \\ -1 & -1+i & 1 \end{pmatrix}$ už víme, že je normální, neboť $\overline{\mathbf{A}}^{\mathrm{T}} = \mathbf{A}$. Tudíž je podle 4.21 unitárně diagonalizovatelná. Chceme-li najít ortonormální bázi $\mathbf{C}^3$ složenou z vlastních vektorů, stačí nám najít ortonormální báze podprostorů řešení homogení soustavy rovnic s maticí $\mathbf{A} - \lambda \mathbf{E}$ pro jednotlivá vlastní čísla λ, proto podle Poznámky 4.22 musí být jednotlivé podprostory vlastních vektorů vzájemně kolmé.

Charakteristický polynom matice $\mathbf{A}$ je $-\lambda^3 + 4\lambda^2$, proto $\sigma(\mathbf{A}) = \{0, 4\}$. Snadno najdeme ortonormální bázi množiny všech řešení soustavy s maticí

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

Podprostor všech řešení je jednodimenzionální, jeho bázi tvoří například vektor $(1, 1+i, -1)$. Protože $\|(1, 1+i, -1)\|_\omega = 2$, je vektor $\frac{1}{2}(1, 1+i, -1)$ hledaným normalizovaným vektorem. Dále snadno zjistíme, že například vektory $(-1+i, 1, 0)$, $(1, 0, 1)$ tvoří bázi dvoudimenzionálního podprostoru všech řešení soustavy s maticí a. Zbývá tyto vektory ortogonalizovat a normalizovat. To můžeme provést například Gramovou-Schmidtovou ortogonalizací, tak dostaneme ortonormální bázi $\frac{1}{\sqrt{2}}(1, 0, 1)$, $\frac{1}{2\sqrt{2}}(-1+i, 2, 1-i)$. Zjistili jsme, že $\begin{pmatrix} 4 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} =$

$$= \begin{pmatrix} \frac{1}{2} & \frac{1}{2} - \frac{i}{2} & -\frac{1}{2} \\ \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ \frac{-1-i}{2\sqrt{2}} & \frac{1}{\sqrt{2}} & \frac{1-i}{2\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 & 1-i & -1 \\ 1+i & 2 & -1-i \\ -1 & -1+i & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{2} & \frac{1}{\sqrt{2}} & \frac{-1+i}{2\sqrt{2}} \\ \frac{1}{2} + \frac{i}{2} & 0 & \frac{1}{\sqrt{2}} \\ -\frac{1}{2} & \frac{1}{\sqrt{2}} & \frac{1-i}{2\sqrt{2}} \end{pmatrix}.$$

Uvážíme-li, že matice symetrické bilineární formy na reálném unitárním prostoru je vzhledem k libovolné ortonormální bázi symetrická, že symetrická matice je podle

4.21 reálná unitárně diagonalizovatelná a že unitární jsou podle 4.17 právě matice přechodu od ortonormální k ortonormální bázi, dostáváme

Důsledek 4.23. *Je-li f symetrická bilineární forma na reálném unitárním prostoru (V, g) konečné dimenze, pak existuje ortonormální báze (V, g), která je zároveň polární bázi f.*

Příklad. Nechť je f symetrická bilineární forma na reálném unitárním prostoru $(\mathbf{R}^3, \omega)$ s maticí $[f]_{K_3} = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$ vzhledem ke kanonické bázi. Najdeme bázi B, která je ortonormální vzhledem ke skalárnímu součinu ω a polární vzhledem k symetrické bilineární formě f.

Prtože je kanonická báze ortonormální vzhledem k ω, stačí abychom unitárně diagonalizovali matici $\mathbf{A} = [f]_{K_3}$. Nejprve určíme spektrum $\sigma(\mathbf{A}) = \{1, 4\}$ a pro obě vlastní čísla jim příslušné vlastní vektory, tedy pro $\lambda = 1$ vyřešíme homogenní soustavu rovnic s maticí $\mathbf{A} - 1 \cdot \mathbf{E} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ a dostaneme vlastní vektory $\mathbf{v}_1 \in \langle(-1, 1, 0), (-1, 0, 1)\rangle \setminus \{\mathbf{0}\}$, a pro $\lambda = 4$ vyřešíme homogenní soustavu rovnic s maticí $\mathbf{A} - 4 \cdot \mathbf{E} = \begin{pmatrix} -2 & 1 & 1 \\ 1 & -2 & 1 \\ 1 & 1 & -2 \end{pmatrix}$ a dostaneme vlastní vektory $\mathbf{v}_4 \in \langle(1, 1, 1)\rangle \setminus \{\mathbf{0}\}$. Všimněme si, že podle 4.22 musel být vlastní vektor příslušný vlastnímu číslu 4 kolmý na vlastní vektory příslušné vlastnímu číslu 1, tedy $\mathbf{v}_4 \in \langle(-1, 1, 0), (-1, 0, 1)\rangle^{\perp}$.

Nyní najdeme ortonormální báze obou podprostorů vlastních vektorů. Pro vlastní číslo 4 stačí normalizovat, abychom dostali vektor $\frac{1}{\sqrt{3}}(1, 1, 1)$ a pro $\lambda = 1$ najdeme ortonormální bázi $(\frac{1}{\sqrt{2}}(-1, 1, 0), \frac{1}{\sqrt{6}}(-1, -1, 2))$ podprostoru $\langle(-1, 1, 0), (-1, 0, 1)\rangle$ například Gramovou-Schmidtovou ortogonalizací. Položme dále $B = (\frac{1}{\sqrt{3}}(1, 1, 1), \frac{1}{\sqrt{2}}(-1, 1, 0), \frac{1}{\sqrt{6}}(-1, -1, 2))$. Protože jsou B stejně jako K_3 ortonormální báze, je podle 4.17 matice přechodu $\mathbf{U} = [\mathrm{Id}]_{BK_3}$ unitární a

$$\mathbf{U}^{\mathrm{T}}\mathbf{A}\mathbf{U} = \begin{pmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ \frac{-1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{-1}{\sqrt{6}} & \frac{-1}{\sqrt{6}} & \frac{2}{\sqrt{6}} \end{pmatrix} \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{3}} & \frac{-1}{\sqrt{2}} & \frac{-1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & 0 & \frac{2}{\sqrt{6}} \end{pmatrix} = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Podle 2.3 je $[f]_B = [\mathrm{Id}]^{\mathrm{T}}_{BK_3}[f]_{K_3}[\mathrm{Id}]_{BK_3} = \mathbf{U}^{\mathrm{T}}\mathbf{A}\mathbf{U}$ diagonální matice, tedy B je polární báze f.

5. Rozklady matic

Rozkladem matice $\mathbf{A}$ budeme rozumět posloupnost (zpravidla dvou nebo tří) matic $\mathbf{R}_1, \ldots, \mathbf{R}_i$ takových, že platí $\mathbf{A} = \mathbf{R}_1 \ldots \mathbf{R}_i$. Zajímavé (nejen) pro nás budou ty rozklady, které nám usnadní počítání s danou maticí, ať už matici interpretujeme jako matici nějaké soustavy lineárních rovnic, matici homomorfismu vzhledem k nějakým bázím, matici skalárního součinu či jinak.

Tak například víme, že každou matici $\mathbf{A}$ typu (n, m) můžeme elementárními transformacemi na řádky a sloupce převést na matici $\mathbf{D} = (d_{ij})$, která má mimo hlavní diagonálu všechny hodnoty nulové, tedy $d_{ij} = 0$ pro všechna $i \neq j$. V maticovém zápisu to znamená, že $\mathbf{D} = \mathbf{PAQ}$ pro vhodné regulární matice $\mathbf{P}$ stupně n a $\mathbf{Q}$ stupně m. Je-li $\mathbf{A} = [h]_{B_V B_W}$ matice homomorfismu $h : V \to W$ a B_V a B_W báze prostorů V a W, potom existují báze C_V a C_W prostorů V a W, tak, že $\mathbf{P} = [\mathrm{Id}]_{B_W C_W}$, $\mathbf{Q} = [\mathrm{Id}]_{C_V B_V}$ a $\mathbf{D} = [h]_{C_V C_W}$ (připomeňte si, jak báze C_V a C_W najít), tj. $[h]_{C_V C_W} = [\mathrm{Id}]_{B_W C_W}[h]_{B_V B_W}[\mathrm{Id}]_{C_V B_V}$. To znamená, že budeme-li pracovat s homomorfismem h v souřadnicích vzhledem k bázím C_V a C_W, bude počítání (s maticí homomorfismu h) mnohem jednodušší.

LU rozklad

Definice. Řekneme, že matice $\mathbf{A}_U = (a_{ij})$ je *typu U*, jde-li o čtvercovou horní trojúhelníkovou matici (tj. $a_{ij} = 0$ pro všechna $i > j$), matice $\mathbf{A}_L = (a_{ij})$ je *typu L*, jde-li o čtvercovou dolní trojúhelníkovou matici (tj. $a_{ij} = 0$ pro všechna $i < j$) a navíc má na diagonále jedničky (tj. $a_{ii} = 1$ pro všechna i). *LU rozkladem* libovolné čtvercové matice $\mathbf{A}$ rozumíme rozklad $\mathbf{A} = \mathbf{LU}$, kde $\mathbf{L}$ je matice typu L a $\mathbf{U}$ je matice typu U.

Poznámka 5.1. *Nechť $\mathbf{L}_1$ a $\mathbf{L}_2$ jsou dvě matice stejného stupně typu L a $\mathbf{U}_1$ a $\mathbf{U}_2$ jsou dvě matice stejného stupně typu U. Pak součin $\mathbf{L}_1\mathbf{L}_2$ je opět maticí typu L a součin $\mathbf{U}_1\mathbf{U}_2$ je maticí typu U. Navíc $\mathbf{L}_1^{-1}$ vždy existuje a je typu L, a je-li $\mathbf{U}_1$ regulární, potom $\mathbf{U}_1^{-1}$ je typu U.*

Důkaz. Nechť $i > j$ a označme $\mathbf{r} = (r_1, \dots, r_n)$ i-tý řádek matice $\mathbf{U}_1$ a $\mathbf{s} = s_1, \dots, s_n)$ j-tý sloupec matice $\mathbf{U}_2$. Spočítáme hodnotu na pozici (i,j) matice $\mathbf{U}_1\mathbf{U}_2$:

$$\mathbf{rs}^{\mathrm{T}} = \sum_{\nu=1}^{n} r_\nu s_\nu = \sum_{\nu=1}^{j} 0 s_\nu + \sum_{\nu=j+1}^{n} r_\nu 0 = 0,$$

tedy matice $\mathbf{U}_1\mathbf{U}_2$ je typu U. Protože jsou matice $\mathbf{L}_1^{\mathrm{T}}$ a $\mathbf{L}_2^{\mathrm{T}}$ typu U, je $(\mathbf{L}_1\mathbf{L}_2)^{\mathrm{T}} = \mathbf{L}_2^{\mathrm{T}}\mathbf{L}_1^{\mathrm{T}}$ typu U. Vezmeme-li konečně $\mathbf{r} = (r_1, \dots, r_n)$ i-tý řádek matice $\mathbf{L}_1$ a $\mathbf{s} = s_1, \dots, s_n)$ i-tý sloupec matice $\mathbf{L}_2$, pak

$$\mathbf{rs}^{\mathrm{T}} = \sum_{\nu=1}^{n} r_\nu s_\nu = \sum_{\nu=1}^{i-1} 0 s_\nu + 1 \cdot 1 + \sum_{\nu=i+1}^{n} r_\nu 0 = 1,$$

proto je $\mathbf{L}_1\mathbf{L}_2$ typu L.

Konečně, připomeneme-li pro regulární matici $\mathbf{A}$, že $\mathbf{A}^{-1} = \det(\mathbf{A})^{-1}\mathrm{adj}\mathbf{A}$, že adjungovaná matice horní nebo dolní trojúhelníkové matice je opět horní nebo dolní trojúhelníková, a že determinant horní nebo dolní trojúhelníkové matice dostaneme jako součin hodnot na diagonále, vidíme, že matice $\mathbf{L}_1$ je regulární a $\mathbf{L}_1^{-1}$ je typu L a $\mathbf{U}_1^{-1}$ je typu U pro regulární a $\mathbf{U}_1$. □

Poznámka 5.2. *Existuje-li LU rozklad regulární matice, pak je určen jednoznačně.*

Důkaz. Mějme dva LU rozklady $\mathbf{A} = \mathbf{L}_1\mathbf{U}_1 = \mathbf{L}_2\mathbf{U}_2$. Potom $\mathbf{L}_2^{-1}\mathbf{L}_1 = \mathbf{U}_2\mathbf{U}_1^{-1}$ je podle 5.1 zároveň typu L i U, tedy $\mathbf{L}_2^{-1}\mathbf{L}_1 = \mathbf{U}_2\mathbf{U}_1^{-1} = \mathbf{E}$, odkud dostáváme, že $\mathbf{L}_1 = \mathbf{L}_2$ a $\mathbf{U}_1 = \mathbf{U}_2$ □

Příklad. Zjistíme, zda existuje LU rozklad reálné matice $\mathbf{A} = \begin{pmatrix} 1 & 1 & 2 \\ -4 & -1 & 1 \\ 2 & 5 & -1 \end{pmatrix}$.
K tomu účelu zkusíme $\mathbf{A}$ gaussovsky upravovat a příslušné úpravy budeme zaznamenávat do (případné) matice $\mathbf{L}$:

$$\mathbf{A} = \begin{pmatrix} 1 & 1 & 2 \\ -4 & -1 & 1 \\ 2 & 5 & -1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 2 \\ 0 & 3 & 9 \\ 0 & 3 & -5 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 2 \\ 0 & 3 & 9 \\ 0 & 0 & -14 \end{pmatrix} = \mathbf{U}.$$

Při upravování jsme nepotřebovali přehazovat řádky (ani násobit řádek nenulovým skalárem), tedy dostali jsme $\mathbf{L}_k \dots \mathbf{L}_1 \mathbf{A} = \mathbf{U}$, kde $\mathbf{L}_i$ jsou všechno elementární transformační matice odpovídající přičtení výše položeného řádku k řádku níže položenému. Matice $\mathbf{L}_i$ jsou zřejmě typu L a podle 5.1 je součin $\mathbf{L} = \mathbf{L}_1^{-1} \dots \mathbf{L}_k^{-1}$ rovněž typu $\mathbf{L}$, navíc $\mathbf{A} = \mathbf{LU}$. Tudíž jsme našli LU rozklad matice $\mathbf{A}$. Všimněme si, že součin matic $\mathbf{L}_1^{-1} \dots \mathbf{L}_k^{-1}$ obsahuje na příslušných pozicích hodnoty jednotlivých transformačních matic (tj. i-tý řádek a j-tý sloupec, $i > j$, obsahuje hodotu c_{ij}, právě když jsme během Gaussovy eliminace odečítali od i-tého řádku matice $\mathbf{A}$ a c_{ij}-násobek jejího j-tého řádku):

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

Našli jsme tedy (jednoznačně určený) LU rozklad

$$\begin{pmatrix} 1 & 1 & 2 \\ -4 & -1 & 1 \\ 2 & 5 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -4 & 1 & 0 \\ 2 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 2 \\ 0 & 3 & 9 \\ 0 & 0 & -14 \end{pmatrix}.$$

Definice. *Permutační maticí* budeme rozumět čtvercovou matici $\mathbf{P}$, která v každém řádku a každém sloupci obsahuje právě jednu hodnotu 1 a jinak samé 0.

Poznámka 5.3. *Nechť* $\mathbf{P}$ *a* $\mathbf{Q}$ *jsou dvě permutační matice stupně* n.

(a) *Každou permutační matici dostaneme z jednotkové matice vhodným přeházením řádků (sloupců).*
(b) *Součin* $\mathbf{PQ}$ *je permutační matice.*
(c) $\mathbf{P}^{-1} = \mathbf{P}^{\mathsf{T}}$ *je permutační matice.*

Důkaz. (a) Plyne okamžitě z definice.

(b) Součin $\mathbf{PQ}$ pomocí permutace odpovídající matici $\mathbf{P}$ podle (a) přehází řádky matice $\mathbf{Q}$, tedy opět díky (a) je $\mathbf{PQ}$ permutační matice.

(c) Přímým výpočtem zjistíme, že $\mathbf{P}^{\mathsf{T}} \cdot \mathbf{P} = \mathbf{E}$ a $\mathbf{P}^{\mathsf{T}}$ je permutační podle (a). □

Věta 5.4. *Pro každou čtvercovou matici* $\mathbf{A}$ *existuje permutační matice* $\mathbf{P}$ *tak, že matice* $\mathbf{PA}$ *má LU rozklad.*

Důkaz. Tvrzení dokážeme indukcí podle stupně matice pomocí Gaussova algoritmu. Vše je triviální pro matice stupně 1, tedy $(a) = (1) \cdot (a)$ je LU rozklad matice (a).

Předpokládejme, že tvrzení platí pro každou čtvercovou matici stupně $n - 1$ a mějme čtvercovou matici $\mathbf{A}_n = (a_{ij})$ stupně n. Budeme gaussovsky upravovat její první sloupec. Je-li celý nulový, pak položíme $i = 1$, jinak vezmeme nejmenší $i \leq n$, pro které $a_{i1} \neq 0$, přehodíme i-tý řádek s prvním řádkem a vynulujeme ostatní pozice prvního sloupce takto upravené matice $\mathbf{A}_n$. Vyjádříme to pomocí maticového zápisu:

$$\begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{v}^{\mathrm{T}} & \mathbf{E} \end{pmatrix} \mathbf{T}_{1i}\mathbf{A}_n = \begin{pmatrix} a_{i1} & \mathbf{a}_{n-1} \\ \mathbf{0}^{\mathrm{T}} & \mathbf{A}_{n-1} \end{pmatrix},$$

kde $\mathbf{v}^{\mathrm{T}}$ je vhodný sloupcový vektor o $n-1$ souřadnicích, T_{1i} elementární transformační matice (tj. permutační matice), která odpovídá přehození prvního a i-tého řádku, $\mathbf{a}_{n-1} = (a_{i2}, a_{i3}, \dots a_{in})$ a $\mathbf{A}_{n-1}$ je čtvercová matice stupně $n-1$. Nyní využijeme pro matici $\mathbf{A}_{n-1}$ indukční předpoklad, který říká, že existuje permutační matice $\mathbf{P}_{n-1}$, matice $\mathbf{L}_{n-1}$ typu L a matice $\mathbf{U}_{n-1}$ typu U (všechny stupně $n-1$) tak, že $\mathbf{P}_{n-1}\mathbf{A}_{n-1} = \mathbf{L}_{n-1}\mathbf{U}_{n-1}$. To ovšem znamená, že

$$\begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0}^{\mathrm{T}} & \mathbf{P}_{n-1} \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{v}^{\mathrm{T}} & \mathbf{E} \end{pmatrix} \mathbf{T}_{1i}\mathbf{A}_n = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0}^{\mathrm{T}} & \mathbf{P}_{n-1} \end{pmatrix} \begin{pmatrix} a_{i1} & \mathbf{a}_{n-1} \\ \mathbf{0}^{\mathrm{T}} & \mathbf{A}_{n-1} \end{pmatrix} =$$

$$= \begin{pmatrix} a_{i1} & \mathbf{a}_{n-1} \\ \mathbf{0}^{\mathrm{T}} & \mathbf{P}_{n-1}\mathbf{A}_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0}^{\mathrm{T}} & \mathbf{L}_{n-1} \end{pmatrix} \begin{pmatrix} a_{i1} & \mathbf{a}_{n-1} \\ \mathbf{0}^{\mathrm{T}} & \mathbf{U}_{n-1} \end{pmatrix}.$$

Dále si uvědomme, že

$$\begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0}^{\mathrm{T}} & \mathbf{P}_{n-1} \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{v}^{\mathrm{T}} & \mathbf{E} \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{P}_{n-1}\,\mathbf{v}^{\mathrm{T}} & \mathbf{E} \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0}^{\mathrm{T}} & \mathbf{P}_{n-1} \end{pmatrix}.$$

Nyní už stačí jen položit $\mathbf{P}_n = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0}^{\mathrm{T}} & \mathbf{P}_{n-1} \end{pmatrix} \mathbf{T}_{1i}, \quad \mathbf{U}_n = \begin{pmatrix} a_{i1} & \mathbf{a}_{n-1} \\ \mathbf{0}^{\mathrm{T}} & U_{n-1} \end{pmatrix}$ a

$$\mathbf{L}_n = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{P}_{n-1}\,\mathbf{v}^{\mathrm{T}} & \mathbf{E} \end{pmatrix}^{-1} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0}^{\mathrm{T}} & \mathbf{L}_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{0} \\ -\mathbf{P}_{n-1}\,\mathbf{v}^{\mathrm{T}} & \mathbf{L}_{n-1} \end{pmatrix},$$

abychom dostali rovnost $\mathbf{P}_n\mathbf{A}_n = \mathbf{L}_n\mathbf{U}_n$. Konečně díky 5.1 je matice $\mathbf{L}_n$ typu L a podle 5.3(b) je matice $\mathbf{P}_n$ permutační, tedy jsme opravdu našli LU rozklad matice $\mathbf{P}_n\mathbf{A}_n$. □

Příklad. Pro reálnou matici $\mathbf{A} = \begin{pmatrix} 1 & 1 & 2 & 2 \\ -1 & -1 & -2 & 1 \\ 2 & 1 & 0 & 1 \\ 2 & 2 & -1 & 1 \end{pmatrix}$ najdeme permutační matici $\mathbf{P}$ tak, aby matice $\mathbf{PA}$ měla LU rozklad. Stejně jako v důkazu Věty 5.4 budeme matici postupně Gausovsky upravovat, používat budeme pouze přehazování řádků a přičítání násobku výše položeného k níže položenému řádku. Oba typy úprav budeme zaznamenávat (pravý sloupec jen čísluje řádky):

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

Tedy permutační matice, kterou potřebujeme změnit původní matici $\mathbf{A}$, odpovídá permutaci řádků zachycené v pravém sloupci, čili $\mathbf{P} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$. Původním transformacím typu přičtení výše položeného řádku k níže položenému odpovídala matice $\mathbf{L}' = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 \\ 2 & 0 & 0 & 1 \end{pmatrix}$, my ale musíme adekvátně matici $\mathbf{P}$, jako jsme to udělali i v průběhu důkazu Věty 5.4, změnit polohu upravovaných řádků, takže $\mathbf{L} = \mathbf{P}\mathbf{L}'$ a dostáváme LU rozklad matice $\mathbf{PA}$:

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

Příklad. Máme-li LU rozklad matice $\mathbf{A} = \mathbf{LU}$ a uvažujeme-li nehomogenní soustavu rovnic $\mathbf{A}\mathbf{x}^{\mathsf{T}} = \mathbf{y}^{\mathsf{T}}$, potom můžeme úlohu rozdělit na dva jednodušší úkoly, najít nejprve řešení soustavy $\mathbf{L}\mathbf{z}^{\mathsf{T}} = \mathbf{y}^{\mathsf{T}}$ a poté soustavy $\mathbf{U}\mathbf{x}^{\mathsf{T}} = \mathbf{z}^{\mathsf{T}}$. V obou případech počítáme s trojúhelníkovými maticemi, takže při výpočtu už jen dosazujeme, aniž musíme matice jakkoli dále gausovsky upravovat.

Počítejme s LU rozkladem reálné matice

$$\mathbf{A} = \begin{pmatrix} 2 & 1 & -2 \\ -2 & 2 & 3 \\ 2 & 7 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 1 & 2 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 & -2 \\ 0 & 3 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

pro vektor pravých stran $\mathbf{y} = (-3, 2, -1)$. Potom pro $\mathbf{z} = (z_1, z_2, z_3)$ spočítáme $z_1 = y_1 = -3$, dále $-1z_1 + z_2 = 3 + z_2 = y_2 = 2$, tedy $z_2 = -1$ a konečně $z_3 = -1 - 1 \cdot (-3) - 2 \cdot (-1) = 4$. Nyní počítáme soustavu $\mathbf{U}\mathbf{x}^{\mathsf{T}} = \mathbf{z}^{\mathsf{T}}$: $2x_3 = z_3$, tedy $x_3 = 2$, dále $x_2 = \frac{-1-1\cdot 2}{3} = -1$ a $x_1 = \frac{-3-1\cdot(-1)+2\cdot 2}{2} = 1$.

QR rozklad

Definice. Řekneme, že matice $\mathbf{Q}$ je *typu Q*, je-li reálná nebo komplexní a platí, že součin $\overline{\mathbf{Q}}^{\mathsf{T}}\mathbf{Q}$ je jednotková matice. *QR-rozkladem* matice $\mathbf{A}$ nad reálným nebo komplexním tělesem T rozumíme rozklad $\mathbf{A} = \mathbf{QR}$, kde $\mathbf{Q}$ je typu Q a $\mathbf{R}$ je regulární horní trojúhelníková matice s kladnými reálnými hodnotami na diagonále.

Příklad. Každá unitární matice je typu Q.

Poznámka 5.5. *Matice nad tělesem $T = \mathbf{R}$ nebo $\mathbf{C}$ je typu Q, právě když obsahuje ve sloupcích ortonormální posloupnost vektorů vzhledem ke standardnímu skalárnímu součinu ω.*

Důkaz. Okamžitý důsledek definice. □

Poznámka 5.6. *Nechť $\mathbf{A} = \mathbf{QR}$ je QR rozklad matice $\mathbf{A}$ typu (n, m), pak $\mathbf{Q}$ je typu (n, m), $h(\mathbf{A}) = h(\mathbf{Q}) = m$ a QR rozklad je určen jednoznačně. Navíc, označíme-li $\mathbf{A} = (\mathbf{a}_1^{\mathsf{T}}| \dots |\mathbf{a}_m^{\mathsf{T}})$ a $\mathbf{Q} = (\mathbf{q}_1^{\mathsf{T}}| \dots |\mathbf{q}_m^{\mathsf{T}})$, pak $\langle \mathbf{a}_1, \dots, \mathbf{a}_i \rangle = \langle \mathbf{q}_1, \dots, \mathbf{q}_i \rangle$ pro všechna $i = 1, \dots, m$.*

Důkaz. Typ matice $\mathbf{Q}$ je zjevný z definice QR rozkladu.

Uvažujme dva QR rozklady matice $\mathbf{A} = \mathbf{QR} = \mathbf{Q}'\mathbf{R}'$, kde $\mathbf{Q} = (\mathbf{q}_1^{\mathsf{T}}| \dots |\mathbf{q}_m^{\mathsf{T}})$ a $\mathbf{Q}' = (\mathbf{q}_1'^{\mathsf{T}}| \dots |\mathbf{q}_m'^{\mathsf{T}})$. Dále označme $\mathbf{R} = (r_{ij})$ a $\mathbf{R}' = (r'_{ij})$. Indukcí podle i dokážeme, že $\langle \mathbf{a}_1, \dots, \mathbf{a}_i \rangle = \langle \mathbf{q}_1, \dots, \mathbf{q}_i \rangle$, $\mathbf{q}_i = \mathbf{q}'_i$ a $r_{ji} = r'_{ji}$ pro $j = 1, \dots, i$.

Protože $\mathbf{a}_1 = r_{11}\mathbf{q}_1 = r'_{11}\mathbf{q}'_1)$, kde $r_{11} \neq 0$, dostáváme $\langle \mathbf{a}_1 \rangle = \langle \mathbf{q}_1 \rangle = \langle \mathbf{q}'_1 \rangle$. Navíc r_{11}, r'_{11} jsou kladná reálná čísla a $\|\mathbf{q}_1\|_\omega = \|\mathbf{q}'_1\|_\omega$, proto díky 3.3(b) je

$$r_{11} = r_{11}\|\mathbf{q}_1\|_\omega = \|\mathbf{a}_1\|_\omega = r'_{11}\|\mathbf{q}'_1\|_\omega = r'_{11},$$

tudíž $\mathbf{q}_1 = \mathbf{q}'_1$.

Předpokládejme, že $\langle \mathbf{a}_1, \dots, \mathbf{a}_{i-1} \rangle = \langle \mathbf{q}_1, \dots, \mathbf{q}_{i-1} \rangle$ a $\mathbf{q}_j = \mathbf{q}'_j$ pro všechna $j = 1, \dots, i-1$. Všimněme si, že $\mathbf{a}_i = r_{ii}\mathbf{q}_i + \sum_{j=1}^{i-1} r_{ji}\mathbf{q}_j$, kde $r_{ii} \neq 0$, a proto $\mathbf{q}_i = r_{ii}^{-1}[\mathbf{a}_i + \sum_{j=1}^{i-1} r_{ji}\mathbf{q}_j]$. Tedy $\mathbf{a}_i \in \langle \mathbf{q}_1, \dots, \mathbf{q}_i \rangle$ a naopak $\mathbf{q}_i \in \langle \mathbf{q}_1, \dots, \mathbf{q}_{i-1}, \mathbf{a}_i \rangle = \langle \mathbf{a}_1, \dots, \mathbf{a}_{i-1}, \mathbf{a}_i \rangle$ podle indkčního předpokladu. Tím jsme dokázali, že $\langle \mathbf{a}_1, \dots, \mathbf{a}_i \rangle \subseteq \langle \mathbf{q}_1, \dots, \mathbf{q}_i \rangle$ i $\langle \mathbf{q}_1, \dots, \mathbf{q}_i \rangle \subseteq \langle \mathbf{a}_1, \dots, \mathbf{a}_i \rangle$. Díky indukčnímu předpokladu vidíme, že

$$\mathbf{a}_i = r_{ii}\mathbf{q}_i + \sum_{j=1}^{i-1} r_{ji}\mathbf{q}_j = r'_{ii}\mathbf{q}'_i + \sum_{j=1}^{i-1} r'_{ji}\mathbf{q}'_j = r'_{ii}\mathbf{q}'_i + \sum_{j=1}^{i-1} r'_{ji}\mathbf{q}_j,$$

a proto $r_{ji} = \omega(\mathbf{q}_j, \mathbf{a}_i) = r'_{ji}$ pro všechna $j = 1, \dots, i-1$. Tedy dostáváme, že $\mathbf{a}_i = r_{ii}\mathbf{q}_i + \sum_{j=1}^{i-1} r_{ji}\mathbf{q}_j = r'_{ii}\mathbf{q}'_i + \sum_{j=1}^{i-1} r_{ji}\mathbf{q}_j$, a tudíž $r_{ii}\mathbf{q}_i = r'_{ii}\mathbf{q}'_i$. Protože jsou r_{ii}, r'_{ii} kladná reálná čísla a $\|\mathbf{q}_i\|_\omega = \|\mathbf{q}'_i\|_\omega$, opakovaným použitím 3.3(b) zjišťujeme, že

$$r_{ii} = r_{ii}\|\mathbf{q}_i\|_\omega = r'_i\|\mathbf{q}'_i\|_\omega = r'_{ii},$$

a proto $\mathbf{q}_i = \mathbf{q}'_i$.

Konečně, $h(\mathbf{Q}) = m$ podle 3.7 a dokázali jsme, že $h(\mathbf{A}) = \dim\langle \mathbf{a}_1, \dots, \mathbf{a}_m \rangle = \dim\langle \mathbf{q}_1, \dots, \mathbf{q}_m \rangle = h(\mathbf{Q})$. □

Věta 5.7. *Nechť T je reálné nebo komplexní těleso, $\mathbf{a}_1, \dots, \mathbf{a}_m$ je posloupnost lineárně nezávislých vektorů prostoru T^n a $\mathbf{q}_1, \dots, \mathbf{q}_m$ je posloupnost ortonormálních vektorů unitárního prostoru (T^n, ω), kterou z ní vytvoříme Gramovou-Schmidtovou ortogonalizací. Položme $\mathbf{A} = (\mathbf{a}_1^{\mathrm{T}}|\dots|\mathbf{a}_m^{\mathrm{T}})$, $\mathbf{Q} = (\mathbf{q}_1^{\mathrm{T}}|\dots|\mathbf{q}_m^{\mathrm{T}})$ a $\mathbf{R} = (r_{ij})$, kde $r_{ij} = \omega(\mathbf{q}_i, \mathbf{a}_j)$. Potom $\mathbf{A} = \mathbf{QR}$ je QR rozklad matice $\mathbf{A}$.*

Důkaz. Podle 3.9 je $\mathbf{a}_j = \sum_{i=1}^m \omega(\mathbf{q}_i, \mathbf{a}_j)\mathbf{q}_i$, proto platí, že $\mathbf{A} = \mathbf{QR}$. Jelikož díky 5.6 $\langle \mathbf{a}_1, \dots, \mathbf{a}_i \rangle = \langle \mathbf{q}_1, \dots, \mathbf{q}_i \rangle$, je k-tá souřadnice vektoru $\mathbf{a}_j$ vzhledem k bázi $\mathbf{q}_1, \dots, \mathbf{q}_i$ pro všechna $k = j+1, \dots, m$ nulová. Tedy $r_{ij} = 0$, pokud $i > j$. To znamená, že matice $\mathbf{R}$ je horní trojúhelníková. Připomeňme, že během Gramovy-Schmidtovy ortogonalizace dostáváme $\mathbf{q}_i = \frac{\mathbf{q}'_i}{\|\mathbf{q}'_i\|_\omega}$, kde $\mathbf{q}'_i = \mathbf{a}_i - \sum_{j=1}^{i-1} r_{ji}\mathbf{q}_j$ (viz 3.8). Proto $\mathbf{a}_i = \|\mathbf{q}'_i\|_\omega \mathbf{q}_i + \sum_{j=1}^{i-1} r_{ji}\mathbf{q}_j$, a tudíž $r_{ii} = \omega(\mathbf{q}_i, \mathbf{a}_i) = \|\mathbf{q}'_i\|_\omega > 0$. Konečně díky 5.5 je $\mathbf{Q}$ matice typu Q. □

Důsledek 5.8. *Pro reálnou nebo komplexní matici $\mathbf{A}$ existuje QR rozklad, právě když se její hodnost rovná počtu jejích sloupců.*

Příklad. Budeme hledat QR rozklad reálné matice $\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 2 \end{pmatrix}$. Podle 5.7 stačí klasickou Gramovou-Schmidtovou ortogonalizací upravovat lineárně nezávislou posloupnost vektorů $(1,1,1,1)$, $(1,0,1,0)$, $(0,1,0,2)$ unitárního prostoru $(\mathbf{R}^4, \omega)$ a mezivýsledky sepsat do matic Q a R. Všimněme si, že $r_{ii} = \omega(\mathbf{q}_i, \mathbf{a}_i) = \|\mathbf{q}'_i\|_\omega$.

1. $\mathbf{q}_1 = \frac{(1,1,1,1)}{\|(1,1,1,1)\|_\omega} = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})$ a $r_{11} = \|(1,1,1,1)\|_\omega = 2$.

2. $\mathbf{q}_2' = (1,0,1,0) - \omega(\frac{1}{2}(1,1,1,1),(1,0,1,0)) \cdot \frac{1}{2}(1,1,1,1) = \frac{1}{2}(1,-1,1,-1)$. Proto $r_{12} = \omega(\frac{1}{2}(1,1,1,1),(1,0,1,0)) = 1$, $r_{22} = \|\frac{1}{2}(1,-1,1,-1)\|_\omega = 1$ a $\mathbf{q}_2 = (\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2})$.
3. Konečně $r_{13} = \omega(\mathbf{q}_1,(0,1,0,2)) = \frac{3}{2}$, $r_{23} = \omega(\mathbf{q}_2,(0,1,0,2)) = -\frac{3}{2}$, proto $\mathbf{q}_3' = (0,1,0,2) - \frac{3}{2}\cdot(\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2}) + \frac{3}{2}\cdot(\frac{1}{2},-\frac{1}{2},\frac{1}{2},-\frac{1}{2}) = (0,-\frac{1}{2},0,\frac{1}{2})$. Tedy $r_{33} = \|(0,-\frac{1}{2},0,\frac{1}{2})\|_\omega = \frac{1}{\sqrt{2}}$ a $\mathbf{q}_3 = (0,-\frac{1}{\sqrt{2}},0,\frac{1}{\sqrt{2}})$.

Dostáváme QR rozklad $\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 2 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{\sqrt{2}} \\ \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 2 & 1 & \frac{3}{2} \\ 0 & 1 & -\frac{3}{2} \\ 0 & 0 & \frac{1}{\sqrt{2}} \end{pmatrix}$.

URV rozklad

Věta 5.9. *Nechť T je těleso reálných nebo komplexních čísel a $\mathbf{A}$ matice typu (n,m) hodnosti k nad tělesem T. Potom nad T existují unitární matice $\mathbf{U}$ stupně n a $\mathbf{V}$ stupně m a reguární matice $\mathbf{D}$ stupně k, pro něž platí, že*

$$\mathbf{A} = \mathbf{U}\begin{pmatrix} \mathbf{D} & \mathbf{0}_1 \\ \mathbf{0}_2 & \mathbf{0}_3 \end{pmatrix}\overline{\mathbf{V}}^{\mathsf{T}},$$

kde $\mathbf{0}_1$ je nulová matice typu $(k, m-k)$, $\mathbf{0}_2$ je nulová matice typu $(n-k,k)$ a $\mathbf{0}_3$ je nulová matice typu $(n-k, m-k)$.

Důkaz. Označme $\mathcal{R}(\mathbf{A})$ podprostor vektorového prostoru T^m generovaný všemi řádky matice $\mathbf{A}$ a $\mathcal{S}(\mathbf{A})$ budiž podprostor vektorového prostoru T^n generovaný všemi sloupci matice $\mathbf{A}$. Víme, že $k = h(\mathbf{A}) = h(\overline{\mathbf{A}}) = \dim(R(\overline{\mathbf{A}})) = \dim(\mathcal{S}(\mathbf{A}))$. Podle 3.8 existují ortonormální báze $\mathbf{v}_1,\dots,\mathbf{v}_m$ unitárního prostoru (T^m,ω) a ortonormální báze $\mathbf{u}_1,\dots,\mathbf{u}_n$ unitárního prostoru (T^n,ω) tak, že $\mathcal{R}(\overline{\mathbf{A}}) = \langle \mathbf{v}_1,\dots,\mathbf{v}_k\rangle$ a $\mathcal{S}(\mathbf{A}) = \langle \mathbf{u}_1,\dots,\mathbf{u}_k\rangle$. Umístěme sloupcové nektory těchto bází do matic $\mathbf{V}$ a $\mathbf{U}$, tj $\mathbf{U} = (\mathbf{u}_1^{\mathsf{T}} \mid \mathbf{u}_2^{\mathsf{T}} \mid \dots \mid \mathbf{u}_n^{\mathsf{T}})$ a $\mathbf{V} = (\overline{\mathbf{v}_1^{\mathsf{T}}} | \overline{\mathbf{v}_2^{\mathsf{T}}} | \dots | \overline{\mathbf{v}_m^{\mathsf{T}}})$. Poznamenejme, že jde podle 4.15 o unitární matice. Konečně položme $\mathbf{R} = \overline{\mathbf{U}}^{\mathsf{T}}\mathbf{A}\mathbf{V}$. Potom $\mathbf{A} = \mathbf{U}\overline{\mathbf{U}}^{\mathsf{T}}\mathbf{A}\mathbf{V}\overline{\mathbf{V}}^{\mathsf{T}} = \mathbf{U}\mathbf{R}\overline{\mathbf{V}}^{\mathsf{T}}$. Zbývá si uvědomit, že matice $\mathbf{R}$ má požadovaný tvar. Připomeňme, že vektory $\mathbf{u}_i$ pro $i = k+1,\dots,n$ jsou kolmé na $\mathcal{S}(\mathbf{A}) = \langle \mathbf{u}_1,\dots,\mathbf{u}_k\rangle$. To znamená, že $\overline{\mathbf{u}_i}\mathbf{A} = \mathbf{0}$, a tedy i $\mathbf{u}_i\,\mathbf{A}\mathbf{V} = \mathbf{0}\,\mathbf{V} = \mathbf{0}$ pro všechna $i = k+1,\dots,n$. Tedy řádky $k+1,\dots,n$ matice $\mathbf{R}$ jsou nulové. Symetrickou úvahou ověříme, že i sloupce $k+1,\dots,m$ matice $\mathbf{R}$ jsou nulové, čímž jsme dokázali, že matice je $\mathbf{R}$ tvaru $\begin{pmatrix} \mathbf{D} & \mathbf{0}_1 \\ \mathbf{0}_2 & \mathbf{0}_3 \end{pmatrix}$. Konečně obě matice $\overline{\mathbf{U}}^{\mathsf{T}}$i $\mathbf{V}$ jsou regulární, proto $h(\mathbf{A}) = h(\mathbf{R}) = k$. To znamená, že prvních k řádků i sloupců matice $\mathbf{R}$ je lineárně nezávislých, proto je čtvercová matice $\mathbf{D}$ stupně k nutně regulární. $\square$

Definice. Posloupnost matic $\mathbf{U}$, $\begin{pmatrix} \mathbf{D} & \mathbf{0}_1 \\ \mathbf{0}_2 & \mathbf{0}_3 \end{pmatrix}$ a $\overline{\mathbf{V}}^{\mathsf{T}}$ z předchozí věty nazveme *URV rozkladem* reálné nebo komplexní matice $\mathbf{A}$.

Příklad. Hledejme URV rozklad reálné matice $\mathbf{A} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 2 & 0 & 1 & 1 \\ 1 & -1 & 1 & 0 \end{pmatrix}$. Nejdříve musíme najít ortonormální báze podprostorů generovaných řádky a sloupci matice A, které doplníme na ortonormální báze celých prostorů. Snadno nahlédneme, že $(\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, 0, \frac{1}{\sqrt{3}})$, $(\frac{1}{\sqrt{3}}, -\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, 0)$ tvoří ortonormální bázi podprostoru prostoru $\mathbf{R}^4$ tvořeného řádky matice A, kterou můžeme doplnit vektory $(-\frac{1}{\sqrt{6}}, \frac{1}{\sqrt{6}}, \frac{2}{\sqrt{6}}, 0)$, $(\frac{1}{\sqrt{6}}, \frac{1}{\sqrt{6}}, 0, -\frac{2}{\sqrt{6}})$ na ortonormální bázi celého $\mathbf{R}^4$. Podobně najdeme ortonormální bázi $(\frac{1}{\sqrt{6}}, \frac{2}{\sqrt{6}}, \frac{1}{\sqrt{6}})$, $(\frac{1}{\sqrt{2}}, 0, -\frac{1}{\sqrt{2}})$ podprostoru generovaného sloupci, a vektorem $(\frac{1}{\sqrt{3}}, -\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}})$ ji doplníme na ortonormální bázi $\mathbf{R}^3$.

Tedy $\mathbf{U} = \begin{pmatrix} \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{3}} \\ \frac{2}{\sqrt{6}} & 0 & -\frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{3}} \end{pmatrix}$ a $\mathbf{V} = \begin{pmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{3}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} \\ 0 & \frac{1}{\sqrt{3}} & \frac{2}{\sqrt{6}} & 0 \\ \frac{1}{\sqrt{3}} & 0 & 0 & -\frac{2}{\sqrt{6}} \end{pmatrix}$.

V souladu s pozorováním provedeným v důkazu Věty 5.9 dopočítáme matici $\mathbf{R}$:

$$\mathbf{R} = \begin{pmatrix} \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{3}} \\ \frac{2}{\sqrt{6}} & 0 & -\frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{3}} \end{pmatrix}^{\mathrm{T}} \begin{pmatrix} 1 & 1 & 0 & 1 \\ 2 & 0 & 1 & 1 \\ 1 & -1 & 1 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{3}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} \\ 0 & \frac{1}{\sqrt{3}} & \frac{2}{\sqrt{6}} & 0 \\ \frac{1}{\sqrt{3}} & 0 & 0 & -\frac{2}{\sqrt{6}} \end{pmatrix}$$

Tedy $\mathbf{R} = \begin{pmatrix} \frac{3}{\sqrt{2}} & \frac{3}{\sqrt{2}} & 0 & 0 \\ \frac{\sqrt{3}}{\sqrt{2}} & -\frac{\sqrt{3}}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$, našli jsme reálný URV rozklad $\mathbf{A} = \mathbf{URV}^{\mathrm{T}}$.

Poznámka 5.10. *$h(\mathbf{A}) = h(\overline{\mathbf{A}}^{\mathrm{T}}\mathbf{A}) = h(\mathbf{A}\overline{\mathbf{A}}^{\mathrm{T}})$ pro každou komplexní matici $\mathbf{A}$.*

Důkaz. Vezmeme-li URV rozklad $\mathbf{A} = \mathbf{U}\begin{pmatrix} \mathbf{D} & \mathbf{0}_1 \\ \mathbf{0}_2 & \mathbf{0}_3 \end{pmatrix}\overline{\mathbf{V}}^{\mathrm{T}}$ zaručený Větou 5.9, pak

$$\overline{\mathbf{A}}^{\mathrm{T}}\mathbf{A} = \mathbf{U}\begin{pmatrix} \mathbf{D} & \mathbf{0}_1 \\ \mathbf{0}_2 & \mathbf{0}_3 \end{pmatrix}\overline{\mathbf{V}}^{\mathrm{T}}\mathbf{V}\begin{pmatrix} \overline{\mathbf{D}}^{\mathrm{T}} & \mathbf{0}_1 \\ \mathbf{0}_2 & \mathbf{0}_3 \end{pmatrix}\overline{\mathbf{U}}^{\mathrm{T}} = \mathbf{U}\begin{pmatrix} \mathbf{D}\overline{\mathbf{D}}^{\mathrm{T}} & \mathbf{0}_1 \\ \mathbf{0}_2 & \mathbf{0}_3 \end{pmatrix}\overline{\mathbf{U}}^{\mathrm{T}}.$$

Protože je matice $\mathbf{D}$, a proto i matice $\mathbf{D}\overline{\mathbf{D}}^{\mathrm{T}}$ regulární stupně $h(\mathbf{A})$ je $h(\mathbf{A}) = h(\overline{\mathbf{A}}^{\mathrm{T}}) = h(\mathbf{D}\overline{\mathbf{D}}^{\mathrm{T}})$.

Symetrickou úvahou pro součin $\mathbf{A}\overline{\mathbf{A}}^{\mathrm{T}}$ dostaneme rovnost $h(\mathbf{A}) = h(\mathbf{A}\overline{\mathbf{A}}^{\mathrm{T}})$. □

Příklad. (1) O reálné matici $\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$ podle předchozí poznámky bez počítání víme, že $h(\mathbf{A}\mathbf{A}^{\mathrm{T}}) = h(\mathbf{A}) = 1$.

(2) Uvážíme-li matici $\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$ nad tělesem $\mathbf{Z}_5$, pak $\mathbf{A}\mathbf{A}^{\mathrm{T}} = \mathbf{0}$, tedy $h(\mathbf{A}\mathbf{A}^{\mathrm{T}}) = 0 \neq 1 = h(\mathbf{A})$.

Poznámka 5.11. *Nechť $\varphi : W_1 \to W_2$ je homomorfismus, kde (W_1, g_1) a (W_2, g_2) jsou unitární prostory konečné dimenze nad týmž tělesem. Potom existují takové ortonormální báze B_1 prostoru (W_1, g_1) a B_2 prostoru (W_2, g_2), že $[\varphi]_{B_1B_2} = \begin{pmatrix} \mathbf{D} & \mathbf{0}_1 \\ \mathbf{0}_2 & \mathbf{0}_3 \end{pmatrix}$, kde $\mathbf{D}$ je regulární matice a $\mathbf{0}_i$ nulové matice příslušného typu.*

Důkaz. Zvolme nějakou ortonormální bázi M_1 prostoru (W_1, g_1) a ortonormální bázi M_2 prostoru (W_2, g_2), která existuje podle 3.8, a URV rozklad matice $[\varphi]_{M_1M_2} = \mathbf{U}\begin{pmatrix}\mathbf{D} & \mathbf{0}_1\\ \mathbf{0}_2 & \mathbf{0}_3\end{pmatrix}\overline{\mathbf{V}}^{\mathrm{T}}$. Vezmeme-li nyní bázi B_1 prostoru W_1, pro niž $[\mathrm{Id}]_{B_1M_1} = \mathbf{V}$ a bázi B_2 prostoru W_2, pro niž $[\mathrm{Id}]_{B_2M_2} = \mathbf{U}$, pak jde o ortonormální báze podle 4.17, proto $[\mathrm{Id}]_{M_2B_2} = \overline{\mathbf{U}}^{\mathrm{T}}$ a dostáváme

$$[\varphi]_{B_1B_2} = [\mathrm{Id}]_{M_2B_2}[\varphi]_{M_1M_2}[\mathrm{Id}]_{B_1M_1} = \overline{\mathbf{U}}^{\mathrm{T}}\mathbf{U}\begin{pmatrix}\mathbf{D} & \mathbf{0}_1\\ \mathbf{0}_2 & \mathbf{0}_3\end{pmatrix}\overline{\mathbf{V}}^{\mathrm{T}}\mathbf{V} = \begin{pmatrix}\mathbf{D} & \mathbf{0}_1\\ \mathbf{0}_2 & \mathbf{0}_3\end{pmatrix}.$$

□

Příklad. Máme-li homomorfismus $\varphi : \mathbf{R}^4 \to \mathbf{R}^3$, jehož matice vzhledem ke kanonickým bázím je $[\varphi]_{K_4K_3} = \begin{pmatrix}1 & 1 & 0 & 1\\ 2 & 0 & 1 & 1\\ 1 & -1 & 1 & 0\end{pmatrix}$ pak s využitím hodnot z předchozého příkladu zjistíme, že pro matice přechodu

$$[\mathrm{Id}]_{CK_3} = \begin{pmatrix}\frac{1}{\sqrt6} & \frac{1}{\sqrt2} & \frac{1}{\sqrt3}\\ \frac{2}{\sqrt6} & 0 & -\frac{1}{\sqrt3}\\ \frac{1}{\sqrt6} & -\frac{1}{\sqrt2} & \frac{1}{\sqrt3}\end{pmatrix} \quad \text{a} \quad [\mathrm{Id}]_{BK_4} = \begin{pmatrix}\frac{1}{\sqrt3} & \frac{1}{\sqrt3} & -\frac{1}{\sqrt6} & \frac{1}{\sqrt6}\\ \frac{1}{\sqrt3} & -\frac{1}{\sqrt3} & \frac{1}{\sqrt6} & \frac{1}{\sqrt6}\\ 0 & \frac{1}{\sqrt3} & \frac{2}{\sqrt6} & 0\\ \frac{1}{\sqrt3} & 0 & 0 & -\frac{2}{\sqrt6}\end{pmatrix} \quad \text{je}$$

$$[\varphi]_{BC} = [\mathrm{Id}]_{K_3C}[\varphi]_{K_4K_3}[\mathrm{Id}]_{BK_4} = [\mathrm{Id}]^{\mathrm{T}}_{CK_3}[\varphi]_{K_4K_3}[\mathrm{Id}]_{BK_4} = \begin{pmatrix}\frac{3}{\sqrt2} & \frac{3}{\sqrt2} & 0 & 0\\ \frac{\sqrt3}{\sqrt2} & -\frac{\sqrt3}{\sqrt2} & 0 & 0\\ 0 & 0 & 0 & 0\end{pmatrix}.$$

Hledané ortonormální báze najdeme přímo ve sloupečcích matic $[\mathrm{Id}]_{BK_4}$ a $[\mathrm{Id}]_{CK_3}$, tedy $B = ((\frac{1}{\sqrt3}, \frac{1}{\sqrt3}, 0, \frac{1}{\sqrt3}), (\frac{1}{\sqrt3}, -\frac{1}{\sqrt3}, \frac{1}{\sqrt3}, 0), (-\frac{1}{\sqrt6}, \frac{1}{\sqrt6}, \frac{2}{\sqrt6}, 0), (\frac{1}{\sqrt6}, \frac{1}{\sqrt6}, 0, -\frac{2}{\sqrt6}))$. Obdobně $C = ((\frac{1}{\sqrt6}, \frac{2}{\sqrt6}, \frac{1}{\sqrt6}), (\frac{1}{\sqrt2}, 0, -\frac{1}{\sqrt2}), (\frac{1}{\sqrt3}, -\frac{1}{\sqrt3}, \frac{1}{\sqrt3}))$.

Věta 5.12. *Mějme* $\mathbf{A} = \mathbf{U}_1\begin{pmatrix}\mathbf{D}_1 & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{pmatrix}\overline{\mathbf{V}_1}^{\mathrm{T}} = \mathbf{U}_2\begin{pmatrix}\mathbf{D}_2 & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{pmatrix}\overline{\mathbf{V}_2}^{\mathrm{T}}$ *dva URV rozklady matice* $\mathbf{A}$ *nad* $\mathbf{R}$ *nebo* $\mathbf{C}$, *kde* $\mathbf{D}_i$ *jsou regulární matice. Pak* $\mathbf{V}_1\begin{pmatrix}\mathbf{D}_1^{-1} & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{pmatrix}\overline{\mathbf{U}_1}^{\mathrm{T}} = \mathbf{V}_2\begin{pmatrix}\mathbf{D}_2^{-1} & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{pmatrix}\overline{\mathbf{U}_2}^{\mathrm{T}}$.

Důkaz. Otázku podobně jako v 5.11 převedeme na počítání s homomorfismy. Buď $\mathbf{A}$ matice typu (n, m). Nejprve vezměme homomorfismus $\varphi : \mathbf{T}^m \to \mathbf{T}^n$ s maticí $[\varphi]_{K_mK_n} = \mathbf{A}$ vzhledem ke kanonickým bázím a ortonormální báze B a B' prostoru $(\mathbf{T}^m, \omega)$ a ortonormální báze C a C' prostoru $(\mathbf{T}^n, \omega)$, pro něž platí, že $[\mathrm{Id}]_{BK_m} = \mathbf{V}_1$, $[\mathrm{Id}]_{B'K_m} = \mathbf{V}_2$, $[\mathrm{Id}]_{CK_n} = \mathbf{U}_1$ a $[\mathrm{Id}]_{C'K_n} = \mathbf{U}_2$. Pak snadno spočítáme, že

$$[\varphi]_{BC} = \begin{pmatrix}\mathbf{D}_1 & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{pmatrix}, \quad [\varphi]_{B'C'} = \begin{pmatrix}\mathbf{D}_2 & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{pmatrix}$$

Nyní definujme homomorfismy $\psi_1, \psi_2 : \mathbf{T}^n \to \mathbf{T}^m$ maticí

$$[\psi_1]_{CB} = \begin{pmatrix}\mathbf{D}_1^{-1} & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{pmatrix}, \quad [\psi_2]_{C'B'} = \begin{pmatrix}\mathbf{D}_2^{-1} & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{pmatrix}.$$

Opět snadným výpočtem zjistíme, že

$$[\psi_1]_{K_nK_m} = \mathbf{V}_1 \begin{pmatrix} \mathbf{D}_1^{-1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \overline{\mathbf{U}_1}^{\mathsf{T}} \quad [\psi_2]_{K_nK_m} = \mathbf{V}_2 \begin{pmatrix} \mathbf{D}_2^{-1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \overline{\mathbf{U}_2}^{\mathsf{T}},$$

proto stačí dokázat, že $\psi_1 = \psi_2$.

Označme si $B = (\mathbf{b}_1, \dots, \mathbf{b}_m)$ $B' = (\mathbf{b}'_1, \dots, \mathbf{b}'_m)$, $C = (\mathbf{c}_1, \dots, \mathbf{c}_m)$ $C' = (\mathbf{c}'_1, \dots, \mathbf{c}'_m)$. Konečne položme $s = h(\mathbf{A})$ a všimněme, si, že z matic $[\varphi]_{BC}$, $[\varphi]_{B'C'}$, $[\psi]_{CB}$ a $[\psi]_{C'B'}$ podle definice matice homomorfismu zjistíme, že

$$\operatorname{Ker}\varphi = \langle \mathbf{b}_{s+1}, \dots, \mathbf{b}_m \rangle = \langle \mathbf{b}'_{s+1}, \dots, \mathbf{b}'_m \rangle,$$

a dále $\operatorname{Im}\psi_1 = \langle \mathbf{b}_1, \dots, \mathbf{b}_s \rangle$ a $\operatorname{Im}\psi_2 = \langle \mathbf{b}'_1, \dots, \mathbf{b}'_s \rangle$. To znamená, že máme $\operatorname{Im}(\psi_1) = \langle \mathbf{b}_1, \dots, \mathbf{b}_s \rangle = \langle \mathbf{b}_{s+1}, \dots, \mathbf{b}_m \rangle^{\perp} = \langle \mathbf{c}_{s+1}, \dots, \mathbf{c}_m \rangle^{\perp} = \langle \mathbf{c}_1, \dots, \mathbf{c}_s \rangle = \operatorname{Im}(\psi_2)$. Podobně z matic homomorfismů nahlédneme, že $\operatorname{Im}\varphi = \langle \mathbf{c}_1, \dots, \mathbf{c}_s \rangle = \langle \mathbf{c}'_1, \dots, \mathbf{c}'_s \rangle$ a že $\operatorname{Ker}\psi_1 = \langle \mathbf{c}_{s+1}, \dots, \mathbf{c}_n \rangle$ a $\operatorname{Ker}\psi_2 = \langle \mathbf{c}'_{s+1}, \dots, \mathbf{c}'_n \rangle$, proto i $\operatorname{Ker}(\psi_1) = \operatorname{Im}\varphi^{\perp} = \operatorname{Ker}(\psi_2)$.

Protože $[\phi\psi_1]_{CC} = \begin{pmatrix} \mathbf{E} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}$ a $[\phi\psi_2]_{C'C'} = \begin{pmatrix} \mathbf{E} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}$ máme $\phi\psi_1 = \mathrm{Id} = \phi\psi_2$ na $\operatorname{Im}\varphi$ a $\phi\psi_1 = 0 = \phi\psi_2$ na $\operatorname{Im}\varphi^{\perp}$. Tudíž $\phi(\psi_1 - \psi_2) = 0$ a $\operatorname{Im}(\psi_1 - \psi_2) \subseteq \operatorname{Ker}\phi$. Konečně protože $\operatorname{Im}(\psi_1 - \psi_2) \subseteq \mathbf{b}_1, \dots, \mathbf{b}_s \rangle$ a $\operatorname{Ker}\varphi = \langle \mathbf{b}_{s+1}, \dots, \mathbf{b}_m \rangle$, dostáváme, že $\operatorname{Im}(\psi_1 - \psi_2) = \{\mathbf{0}\}$, tedy $\psi_1 = \psi_2$. □

Definice. Buď $\mathbf{A} = \mathbf{U} \begin{pmatrix} \mathbf{D} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \overline{\mathbf{V}}^{\mathsf{T}}$ URV rozklad reálné nebo komplexní matice $\mathbf{A}$ typu (n, m), kde $\mathbf{D}$ je regulární. Jednoznačně určenou matici $\mathbf{A}^{\dagger} = \mathbf{V} \begin{pmatrix} \mathbf{D}^{-1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \overline{\mathbf{U}}^{\mathsf{T}}$ typu (m, n) nazveme *(Moore-Penroseovou) pseudoinverzní maticí* k matici $\mathbf{A}$.

Poznámka 5.13. *Nechť* $\mathbf{A}$ *je reálná nebo komplexní matice. Pak platí:*

(a) *je-li* $\mathbf{A}$ *regulární, pak* $\mathbf{A}^{\dagger} = \mathbf{A}^{-1}$.
(b) $\mathbf{A}\mathbf{A}^{\dagger}\mathbf{A} = \mathbf{A}$ *a* $\mathbf{A}^{\dagger}\mathbf{A}\mathbf{A}^{\dagger} = \mathbf{A}^{\dagger}$,
(c) $\mathbf{A}\mathbf{A}^{\dagger} = (\overline{\mathbf{A}\mathbf{A}^{\dagger}})^{\mathsf{T}}$ *a* $\mathbf{A}^{\dagger}\mathbf{A} = (\overline{\mathbf{A}^{\dagger}\mathbf{A}})^{\mathsf{T}}$,
(d) $\overline{\mathbf{A}}^{\mathsf{T}} = \overline{\mathbf{A}}^{\mathsf{T}}\mathbf{A}\mathbf{A}^{\dagger} = \mathbf{A}^{\dagger}\mathbf{A}\overline{\mathbf{A}}^{\mathsf{T}}$,
(e) $\overline{\mathbf{A}^{\dagger}}^{\mathsf{T}} = (\overline{\mathbf{A}}^{\mathsf{T}})^{\dagger}$,

Důkaz. Uvažujme URV rozklad $\mathbf{A} = \mathbf{U} \begin{pmatrix} \mathbf{D} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \overline{\mathbf{V}}^{\mathsf{T}}$. Přímočarým výpočtem zjistíme, že

$$\mathbf{A}\mathbf{A}^{\dagger} = \mathbf{U} \begin{pmatrix} \mathbf{D} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \overline{\mathbf{V}}^{\mathsf{T}} \mathbf{V} \begin{pmatrix} \mathbf{D}^{-1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \overline{\mathbf{U}}^{\mathsf{T}} = \mathbf{U} \begin{pmatrix} \mathbf{E} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \overline{\mathbf{U}}^{\mathsf{T}},$$

$$\mathbf{A}^{\dagger}\mathbf{A} = \mathbf{V} \begin{pmatrix} \mathbf{D}^{-1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \overline{\mathbf{U}}^{\mathsf{T}} \mathbf{U} \begin{pmatrix} \mathbf{D} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \overline{\mathbf{V}}^{\mathsf{T}} = \mathbf{V} \begin{pmatrix} \mathbf{E} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \overline{\mathbf{V}}^{\mathsf{T}}$$

proto

(a) $\mathbf{A}\mathbf{A}^{\dagger} = \mathbf{E}$ pro regulární $\mathbf{A}$,
(b) $\mathbf{A}\mathbf{A}^{\dagger}\mathbf{A} = \mathbf{U} \begin{pmatrix} \mathbf{E} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \overline{\mathbf{U}}^{\mathsf{T}} \mathbf{U} \begin{pmatrix} \mathbf{D} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \overline{\mathbf{V}}^{\mathsf{T}} = \mathbf{A}$ a obdobně $\mathbf{A}^{\dagger}\mathbf{A}\mathbf{A}^{\dagger} = \mathbf{A}^{\dagger}$,

(c) $(\overline{\mathbf{A}\mathbf{A}^\dagger})^{\mathrm{T}} = \overline{\mathbf{U}\begin{pmatrix}\mathbf{E} & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{pmatrix}\overline{\mathbf{U}}^{\mathrm{T}}}^{\mathrm{T}} = \mathbf{U}\begin{pmatrix}\mathbf{E} & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{pmatrix}\overline{\mathbf{U}}^{\mathrm{T}} = \mathbf{A}\mathbf{A}^\dagger$ a podobně $(\overline{\mathbf{A}^\dagger\mathbf{A}})^{\mathrm{T}} = \overline{\mathbf{V}\begin{pmatrix}\mathbf{E} & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{pmatrix}\overline{\mathbf{V}}^{\mathrm{T}}}^{\mathrm{T}} = \mathbf{V}\begin{pmatrix}\mathbf{E} & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{pmatrix}\overline{\mathbf{V}}^{\mathrm{T}} = \mathbf{A}^\dagger\mathbf{A}$,

(d) $\overline{\mathbf{A}}^{\mathrm{T}}\mathbf{A}\mathbf{A}^\dagger = \mathbf{V}\begin{pmatrix}\overline{\mathbf{D}}^{\mathrm{T}} & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{pmatrix}\overline{\mathbf{U}}^{\mathrm{T}}\mathbf{U}\begin{pmatrix}\mathbf{E} & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{pmatrix}\overline{\mathbf{U}}^{\mathrm{T}} = \mathbf{V}\begin{pmatrix}\overline{\mathbf{D}}^{\mathrm{T}} & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{pmatrix}\overline{\mathbf{U}}^{\mathrm{T}} = \overline{\mathbf{A}}^{\mathrm{T}}$ a symetricky $\mathbf{A}^\dagger\mathbf{A}\overline{\mathbf{A}}^{\mathrm{T}} = \mathbf{V}\begin{pmatrix}\mathbf{E} & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{pmatrix}\overline{\mathbf{V}}^{\mathrm{T}}\mathbf{V}\begin{pmatrix}\overline{\mathbf{D}}^{\mathrm{T}} & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{pmatrix}\overline{\mathbf{U}}^{\mathrm{T}} = \mathbf{V}\begin{pmatrix}\overline{\mathbf{D}}^{\mathrm{T}} & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{pmatrix}\overline{\mathbf{U}}^{\mathrm{T}} = \overline{\mathbf{A}}^{\mathrm{T}}$.

(e) Konečně $\overline{\mathbf{A}^\dagger}^{\mathrm{T}} = \overline{\mathbf{V}\begin{pmatrix}\mathbf{D}^{-1} & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{pmatrix}\overline{\mathbf{U}}^{\mathrm{T}}}^{\mathrm{T}} = \mathbf{V}\begin{pmatrix}\overline{\mathbf{D}}^{\mathrm{T}\,-1} & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{pmatrix}\overline{\mathbf{U}}^{\mathrm{T}} = (\overline{\mathbf{A}}^{\mathrm{T}})^\dagger$

□

Příklad. Spočítejme pseudoinverzní matici k matici $\mathbf{A} = \begin{pmatrix}1 & 1 & 1\\ 1 & -1 & 1\end{pmatrix}$. Uvědomme si, že nám Poznámky 5.10 a 5.13(d) v tomto případě poskytují jinou metodu nalezení pseudoinverzní matice, než je URV rozklad. Protože matice $\mathbf{A}$ má hodnost dva, a tudíž má podle 5.10 i čtvercová matice $\mathbf{A}\overline{\mathbf{A}}^{\mathrm{T}}$ stupně dva hodnost dva, je $\mathbf{A}\overline{\mathbf{A}}^{\mathrm{T}}$ regulární matice. Jednoduchou úpravou druhé části 5.13(d) dostáváme, že $\mathbf{A}^\dagger = \overline{\mathbf{A}}^{\mathrm{T}}(\mathbf{A}\overline{\mathbf{A}}^{\mathrm{T}})^{-1}$. Snadno zjistíme, že $(\mathbf{A}\overline{\mathbf{A}}^{\mathrm{T}})^{-1} = \begin{pmatrix}3 & 1\\ 1 & 3\end{pmatrix}^{-1} = \begin{pmatrix}\frac{3}{8} & -\frac{1}{8}\\ -\frac{1}{8} & \frac{3}{8}\end{pmatrix}$, a proto

$$\mathbf{A}^\dagger = \begin{pmatrix}1 & 1\\ 1 & -1\\ 1 & 1\end{pmatrix}\begin{pmatrix}\frac{3}{8} & -\frac{1}{8}\\ -\frac{1}{8} & \frac{3}{8}\end{pmatrix} = \begin{pmatrix}\frac{1}{4} & \frac{1}{4}\\ \frac{1}{2} & -\frac{1}{2}\\ \frac{1}{4} & \frac{1}{4}\end{pmatrix}.$$

Příklad. Nechť $\mathbf{A}\mathbf{x}^{\mathrm{T}} = \mathbf{y}^{\mathrm{T}}$ je obecně nehomogenní soustava rovnic. Podle 5.13(d) je $\overline{\mathbf{A}}^{\mathrm{T}}\mathbf{A}\mathbf{A}^\dagger\mathbf{y}^{\mathrm{T}} = \overline{\mathbf{A}}^{\mathrm{T}}\mathbf{y}^{\mathrm{T}}$. Pokud položíme $\mathbf{x}_0^{\mathrm{T}} = \mathbf{A}^\dagger\mathbf{y}^{\mathrm{T}}$, vidíme, že $\overline{\mathbf{A}}^{\mathrm{T}}\mathbf{A}\mathbf{x}_0^{\mathrm{T}} = \overline{\mathbf{A}}^{\mathrm{T}}\mathbf{y}^{\mathrm{T}}$, tedy $\mathbf{A}^\dagger\mathbf{y}^{\mathrm{T}}$ je přibližným řešením soustavy $\mathbf{A}\mathbf{x}^{\mathrm{T}} = \mathbf{y}^{\mathrm{T}}$ metodou nejmenších čtverců (pokud je soustava řešitelná, tak je to, jak víme, exaktní řešení dané soustavy).

Vezmeme-li například soustavu rovnic $\mathbf{A}\begin{pmatrix}x_1\\ x_2\end{pmatrix} = \begin{pmatrix}3\\ 2\\ 1\end{pmatrix}$, kde $\mathbf{A} = \begin{pmatrix}1 & 1\\ 1 & -1\\ 1 & 1\end{pmatrix}$, pak určíme $\mathbf{A}^\dagger = \begin{pmatrix}\frac{1}{4} & \frac{1}{2} & \frac{1}{4}\\ \frac{1}{4} & -\frac{1}{2} & \frac{1}{4}\end{pmatrix}$ pomocí předchozího příkladu a Poznámky 5.16. Přibližné řešení soustavy metodou nejmenších čtverců je $\mathbf{x}_0^{\mathrm{T}} = \mathbf{A}^\dagger\begin{pmatrix}3\\ 2\\ 1\end{pmatrix} = \begin{pmatrix}2\\ 0\end{pmatrix}$.

SVD rozklad

Poznámka 5.14. *Nechť $\mathbf{A}$ je komplexní čtvercová matice. Pak $\overline{\mathbf{A}}^{\mathrm{T}}\mathbf{A}$ je normální matice a všechna vlastní čísla $\overline{\mathbf{A}}^{\mathrm{T}}\mathbf{A}$ jsou reálná a nezáporná.*

Důkaz. Označme $\mathbf{C} = \overline{\mathbf{A}}^{\mathrm{T}}\mathbf{A}$, pak $\overline{\mathbf{C}}^{\mathrm{T}} = \mathbf{C}$, proto $\overline{\mathbf{C}}^{\mathrm{T}} \cdot \mathbf{C} = \cdot\mathbf{C}\mathbf{C} = \mathbf{C} \cdot \overline{\mathbf{C}}^{\mathrm{T}}$, tedy $\mathbf{C}$ je normální. Díky 4.21 existuje unitární matice $\mathbf{U}$, pro kterou $\overline{\mathbf{U}}^{\mathrm{T}}\mathbf{C}\mathbf{U}$ je diagonální matice na jejíž diagonále jsou postupně všechna vlastní čísla λ_i matice $\mathbf{C}$. Označíme-li $\mathbf{u}_1, \dots, \mathbf{u}_n$ sloupce matice $\mathbf{U}$, pak $\lambda_i = \overline{\mathbf{u}_i \, \mathbf{A}^{\mathsf{T}} \mathbf{A} \, \mathbf{u}_i^{\mathsf{T}}} = \omega(\mathbf{u}_i \, \mathbf{A}^{\mathsf{T}}, \mathbf{u}_i \, \mathbf{A}^{\mathsf{T}})$, tedy λ_i jsou nezáporná reálná čísla. □

Věta 5.15. *Nechť T je reálné nebo komplexní těleso a $\mathbf{A}$ je matice typu (n, m) hodnosti k nad T. Potom nad tělesem T existují unitární matice $\mathbf{U}$ stupně n a $\mathbf{V}$ stupně m a diagonální matice $\mathbf{D}$ s kladnými reálnými hodnotami na diagonále stupně k tak, že*

$$\mathbf{A} = \mathbf{U} \begin{pmatrix} \mathbf{D} & \mathbf{0}_1 \\ \mathbf{0}_2 & \mathbf{0}_3 \end{pmatrix} \overline{\mathbf{V}}^{\mathsf{T}},$$

kde $\mathbf{0}_1$ je nulová matice typu $(k, m-k)$, $\mathbf{0}_2$ je nulová matice typu $(n-k, k)$ a $\mathbf{0}_3$ je nulová matice typu $(n-k, m-k)$.

Důkaz. Podle 5.14 je matice $\overline{\mathbf{A}}^{\mathsf{T}}\mathbf{A}$ normální a všechna vlastní čísla $\overline{\mathbf{A}}^{\mathsf{T}}\mathbf{A}$ jsou nezáporná reálná. Věta 4.21 říká, že $\overline{\mathbf{A}}^{\mathsf{T}}\mathbf{A}$ je unitárně diagonalizovatelná, navíc, je-li $\mathbf{A}$ reálná, jde o reálnou unitárně diagonalizovatelnou matici. Tedy existuje taková unitární matice $\mathbf{V} = (\mathbf{v}_1^{\mathsf{T}} \,|\, \dots \,|\, \mathbf{v}_m^{\mathsf{T}})$ stupně m nad tělesem T, že $\overline{\mathbf{V}}^{\mathsf{T}}(\overline{\mathbf{A}}^{\mathsf{T}}\mathbf{A})\mathbf{V}$ je diagonální matice, která má na diagonále po řádě právě vlastní čísla $\lambda_1, \dots, \lambda_m$, všechna nezáporná. Podle 5.10 je $h(\mathbf{A}) = h(\overline{\mathbf{A}}^{\mathsf{T}}\mathbf{A}) = h(\overline{\mathbf{V}}^{\mathsf{T}}(\overline{\mathbf{A}}^{\mathsf{T}}\mathbf{A})\mathbf{V})$, proto právě k čísel λ_i je kladných, můžeme předpokládat, že jsou to právě vlastní čísla $\lambda_1, \dots, \lambda_k$ a $\lambda_{k+1} = \dots = \lambda_m = 0$. Všimněme si, že pro všechna $i = k+1, \dots, m$:

$$\omega(\mathbf{v}_i \, \mathbf{A}^{\mathsf{T}}, \mathbf{v}_i \, \mathbf{A}^{\mathsf{T}}) = \overline{\mathbf{v}_i}\overline{\mathbf{A}}^{\mathsf{T}}\mathbf{A} \, \mathbf{v}_i^{\mathsf{T}} = 0 \cdot \overline{\mathbf{v}_i} \, \mathbf{v}_i^{\mathsf{T}} = 0,$$

tedy $\mathbf{A} \, \mathbf{v}_i^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}}$ v důsledku definice skalárního součinu. Dále položíme $\sigma_i = \sqrt{\lambda_i}$ a $\mathbf{u}_i^{\mathsf{T}} = \frac{A \, \mathbf{v}_i^{\mathsf{T}}}{\sigma_i}$ pro všechna $i = 1, \dots, k$. Potom

$$\omega(\mathbf{u}_i, \mathbf{u}_i) = \frac{\overline{\mathbf{v}_i}\overline{\mathbf{A}}^{\mathsf{T}}}{\sigma_i} \frac{\mathbf{A} \, \mathbf{v}_i^{\mathsf{T}}}{\sigma_i} = \frac{\overline{\mathbf{v}_i}(\overline{\mathbf{A}}^{\mathsf{T}}\mathbf{A}) \, \mathbf{v}_i^{\mathsf{T}}}{\lambda_i} = \frac{\lambda_i \overline{\mathbf{v}_i} \, \mathbf{v}_i^{\mathsf{T}}}{\lambda_i} = 1,$$

$$\omega(\mathbf{u}_i, \mathbf{u}_j) = \frac{\overline{\mathbf{v}_i}\overline{\mathbf{A}}^{\mathsf{T}}}{\sigma_i} \frac{\mathbf{A} \, \mathbf{v}_j^{\mathsf{T}}}{\sigma_j} = \frac{\overline{\mathbf{v}_i}(\overline{\mathbf{A}}^{\mathsf{T}}\mathbf{A}) \, \mathbf{v}_j^{\mathsf{T}}}{\sigma_i\sigma_j} = \frac{\lambda_j \overline{\mathbf{v}_i} \, \mathbf{v}_j^{\mathsf{T}}}{\sigma_i\sigma_j} = 0,$$

pro každé $i, j = 1, \dots, k$, $i \neq j$. Tedy posloupnost vektorů $\mathbf{u}_1 \dots, \mathbf{u}_k$ je ortonormální v unitárním prostoru (T^n, ω) a můžeme ji podle Věty 3.8 doplnit na ortonormální bázi $\mathbf{u}_1 \dots, \mathbf{u}_k, \mathbf{u}_{k+1} \dots, \mathbf{u}_n$ prostoru (T^n, ω). Definujme nyní matici $\mathbf{U} = (\mathbf{u}_1^{\mathsf{T}} \,|\, \dots \,|\, \mathbf{u}_n^{\mathsf{T}})$ a spočítejme hodnotu r_{ij} na i-tém řádku a j-tém sloupci matice $\mathbf{R} = \overline{\mathbf{U}}^{\mathsf{T}}\mathbf{A}\mathbf{V}$:

$$r_{ij} = \overline{\mathbf{u}_i}\mathbf{A} \, \mathbf{v}_j^{\mathsf{T}} = \overline{\mathbf{u}_i}\sigma_j \, \mathbf{u}_j = \sigma_j \omega(\mathbf{u}_i, \mathbf{u}_j) = \begin{cases} 0 & \text{pro } i \neq j, \\ \sigma_j & \text{pro } i = j, \end{cases}$$

pro každé $i = 1, \dots, n$ a každé $j = 1, \dots, k$. Konečně pro $i = 1, \dots, n$ a $j = k+1, \dots, m$

$$r_{ij} = \overline{\mathbf{u}_i}\mathbf{A} \, \mathbf{v}_j^{\mathsf{T}} = \overline{\mathbf{u}_i} \, \mathbf{0}^{\mathsf{T}} = 0.$$

Matice $\mathbf{U}$ a $\mathbf{V}$ jsou unitární, proto $\mathbf{A} = \mathbf{U}\overline{\mathbf{U}}^{\mathsf{T}}\mathbf{A}\mathbf{V}\overline{\mathbf{V}}^{\mathsf{T}} = \mathbf{U}\mathbf{R}\overline{\mathbf{V}}^{\mathsf{T}}$, kde $\mathbf{R}$ zjevně splňuje požadavky věty. □

Definice. Posloupnost matic $\mathbf{U}$, $\begin{pmatrix} \mathbf{D} & \mathbf{0}_1 \\ \mathbf{0}_2 & \mathbf{0}_3 \end{pmatrix}$ a $\overline{\mathbf{V}}^{\mathsf{T}}$ z předchozí věty nazveme *SVD rozkladem* (anglicky single value decomposition) reálné nebo komplexní matice $\mathbf{A}$.

Kladným reálným číslům na diagonále matice $\mathbf{D}$ budeme říkat *singulární hodnoty* matice $\mathbf{A}$.

Důsledek 5.16. *Singulární hodnoty komplexní (reálné) matice* $\mathbf{A}$ *jsou určeny jednoznačně jako* $\sqrt{\lambda}$ *pro všechna kladná vlastní čísla* λ *matice* $\overline{\mathbf{A}}^{\mathsf{T}}\mathbf{A}$ *nebo* $\mathbf{A}\overline{\mathbf{A}}^{\mathsf{T}}$.

Důsledek 5.17. *Nechť* $\varphi : V \to W$ *je homomorfismus, kde* (V,ω) *a* (W,ω) *jsou unitární prostory nad týmž tělesem. Potom existují ortonormální báze* B_V *prostoru* (V,ω) *a* B_W *prostoru* (W,ω) *tak, že* $[\varphi]_{B_V B_W} = \begin{pmatrix} \mathbf{D} & \mathbf{0}_1 \\ \mathbf{0}_2 & \mathbf{0}_3 \end{pmatrix}$, *kde* $\mathbf{D}$ *je diagonální matice s kladnou diagonálou a* $\mathbf{0}_i$ *nulové matice příslušného typu.*

Příklad. Najděme SVD rozklad reálné matice $\mathbf{A} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 2 & 0 & 1 & 1 \\ 1 & -1 & 1 & 0 \end{pmatrix}$. Nejprve spočítáme $\overline{\mathbf{A}}^{\mathsf{T}}\mathbf{A} = \begin{pmatrix} 6 & 0 & 3 & 3 \\ 0 & 2 & -1 & 1 \\ 3 & -1 & 2 & 1 \\ 3 & 1 & 1 & 2 \end{pmatrix}$ a určíme tak spektrum $\sigma(\overline{\mathbf{A}}^{\mathsf{T}}\mathbf{A}) = \{0,3,9\}$. Singulární hodnoty matice $\mathbf{A}$ jsou $\sqrt{3}$, 3. Snadno najdeme normalizované vlastní vektory příslušné vlastním číslům 3 a 9: $\mathbf{v}_3 = (0, \frac{2}{\sqrt{6}}, -\frac{1}{\sqrt{6}}, \frac{1}{\sqrt{6}})$ a $\mathbf{v}_9 = (\frac{2}{\sqrt{6}}, 0, \frac{1}{\sqrt{6}}, \frac{1}{\sqrt{6}})$. Už jsme spočítali, že tuto dvojici můžeme doplnit dvojicí vektorů $(-\frac{1}{\sqrt{6}}, \frac{1}{\sqrt{6}}, \frac{2}{\sqrt{6}}, 0)$, $(\frac{1}{\sqrt{6}}, \frac{1}{\sqrt{6}}, 0, -\frac{2}{\sqrt{6}})$ vlastních vzhledem k vlastnímu číslu 0 na ortonormální bázi celého $(\mathbf{R}^4, \omega)$.

Nyní spočítáme $\mathbf{u}_3 = \frac{1}{\sqrt{3}}\,\mathbf{v}_3\,A^{\mathsf{T}} = (\frac{1}{\sqrt{2}}, 0, -\frac{1}{\sqrt{2}})$ a $\mathbf{u}_9 = \frac{1}{3}\,\mathbf{v}_9\,A^{\mathsf{T}} = (\frac{1}{\sqrt{6}}, \frac{2}{\sqrt{6}}, \frac{1}{\sqrt{6}})$. Vektor $(\frac{1}{\sqrt{3}}, -\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}})$ doplňuje dvojici $\mathbf{u}_3, \mathbf{u}_9$ na ortonormální bázi $\mathbf{R}^3$. Nyní už můžeme napsat SVD rozklad matice $\mathbf{A} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 2 & 0 & 1 & 1 \\ 1 & -1 & 1 & 0 \end{pmatrix} =$

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

Příklad. Vyhledávač.

Mějme systém n výrazů a m dokumentů, v nichž budeme chtít vyhledávat výrazy. Na i-té souřadnici vektoru $\mathbf{c}_j$ budeme mít zaznamenán počet výskytů i-tého slova v j-tém dokumentu. Předpokládejme, že každý dokument obsahuje alespoň jeden výraz, tedy $\mathbf{c}_j \neq \mathbf{0}$. Normalizujeme-li tento vektor $\mathbf{d}_j = \frac{\mathbf{c}_j}{\|\mathbf{c}_j\|_\omega}$, budeme mít na i-té souřadnici vektoru $\mathbf{d}_j$ podíl i-tého slova v j-tém dokumentu vztažený k tomuto dokumentu. Položme $\mathbf{A} = (\mathbf{d}_1^{\mathsf{T}}|\ldots|\mathbf{d}_m^{\mathsf{T}})$.

Zadáme-li otázku sestávající z jisté množiny vyšetřovaných výrazů, budeme se ptát na relevanci jednotlivých dokumentů vzhledem k této otázce. K tomu účelu vytvoříme vektor $\mathbf{q}$, který má na i-té souřadnici hodnotu 1, pokud otázka obsahuje i-tý výraz a všude jinde budou nuly. Uvědomme si, jaký význam má vektor $(x_1,\ldots,x_m) = \frac{\mathbf{qA}}{\|\mathbf{q}\|_\omega}$. Podle 3.4(a) $\mathbf{qd}_i^{\mathsf{T}} = \omega(\mathbf{q},\mathbf{d}_i) \le \|\mathbf{q}\|_\omega\|\mathbf{d}_i\|_\omega = \|\mathbf{q}\|_\omega$, proto $x_i \le 1$. Zřejmě $x_i = \mathbf{qd}_i^{\mathsf{T}} = 0$ právě tehdy, když se žádný z dotazovaných výrazů nevyskytuje v i-tém dokumentu.

Pomocí SVD faktorizace můžeme odstranit "šumy" metody a zároveň zjednodušit výpočet. Nechť $\mathbf{U} = (\mathbf{u}_1^{\mathsf T} | \dots | \mathbf{u}_n^{\mathsf T})$ a $\mathbf{V} = (\mathbf{v}_1^{\mathsf T} | \dots | \mathbf{v}_m^{\mathsf T})$ a $\mathbf{A} = \mathbf{URV}^{\mathsf T}$ je SVD rozklad se singulárními hodnotami $\sigma_1 \geq \dots \geq \sigma_r$, kde $r = h(\mathbf{A})$. Snadno spočítáme, že $\mathbf{A} = \sum_{i=1}^r \sigma_i \, \mathbf{u}_i^{\mathsf T} \, \mathbf{v}_i$ (kde $\mathbf{u}_i^{\mathsf T} \, \mathbf{v}_i$ je matice typu (n, m)). Předpokládejme, že singulární hodnoty $\sigma_{k+1}, \dots, \sigma_r$ jsou výrazně menší než singulární hodnoty $\sigma_1, \dots, \sigma_k$. Vezměme místo matice $\mathbf{A} = \sum_{i=1}^r \sigma_i \, \mathbf{u}_i^{\mathsf T} \, \mathbf{v}_i$ matici $A_k = \sum_{i=1}^k \sigma_i \, \mathbf{u}_i^{\mathsf T} \, \mathbf{v}_i$. Dále vezměme $\mathbf{U}_k = (\mathbf{u}_1^{\mathsf T} | \dots | \mathbf{u}_k^{\mathsf T})$, $\mathbf{V}_k = (\mathbf{v}_1^{\mathsf T} | \dots | \mathbf{v}_k^{\mathsf T})$ a $\mathbf{D}_k$ buď diagonální čtvercová matice stupně k, která má na diagonále po řadě hodnoty $\sigma_1, \dots, \sigma_k$. Tedy platí: $\mathbf{A}_k = \mathbf{U}_k \mathbf{D}_k \mathbf{V}_k^{\mathsf T}$. Nahraďme původní hodnoty x_i hodnotami

$$\xi_i = \frac{\mathbf{q} \mathbf{A}_k \mathbf{e}_i^{\mathsf T}}{\|\mathbf{q}\|_\omega \|\mathbf{e}_i \mathbf{A}_k^{\mathsf T}\|_\omega}.$$

Konečně položme $\mathbf{S}_k = \mathbf{D}_k \mathbf{V}_k^{\mathsf T} = (\mathbf{s}_1 | \dots | \mathbf{s}_k)$. Potom $\mathbf{A}_k \mathbf{e}_i^{\mathsf T} = \mathbf{U}_k \mathbf{s}_i^{\mathsf T}$. Uvědomíme-li si, že zobrazení $\mathbf{s} \to \mathbf{s} U^{\mathsf T}$ je unitární pro libovolnou matici $\mathbf{U}$ typu Q, pak $\|\mathbf{s}\|_\omega = \|\mathbf{s}\mathbf{U}^{\mathsf T}\|_\omega$, a proto

$$\|\mathbf{e}_i \mathbf{A}_k^{\mathsf T}\|_\omega = \|\mathbf{s}_i \mathbf{U}_k^{\mathsf T}\|_\omega = \|\mathbf{s}_i\|_\omega.$$

Tedy k určení relevance i-tého dokumentu stačí spočítat

$$\xi_i = \frac{\mathbf{q} \mathbf{U}_k \mathbf{s}_i^{\mathsf T}}{\|\mathbf{q}\|_\omega \|\mathbf{s}_i\|_\omega}$$

a k tomu nám stačí předem znát (a pro daný systém dokumentů jednou spočítat) matice $\mathbf{S}_k$ a $\mathbf{U}_k$. Jeli k výrazně menší než r (v mnoha konkrétních situacích to opravdu nastává) je výpočet hodnot ξ_i výrazně jednodušší než výpočet x_i.

Choleskyho rozklad symetrické matice

Definice. Řekneme, že symetrická reálná čtvercová matice $\mathbf{A}$ stupně n je *pozitivně definitní*, jestliže $\mathbf{v} \, \mathbf{A} \, \mathbf{v}^{\mathsf T} > 0$ pro každý nenulový vektor $\mathbf{v} \in \mathbf{R}^n$.

Poznámka 5.18. *Buď* $\mathbf{A}$ *symetrická reálná čtvercová matice stupně* n. *Pak je následující ekvivalentní:*

(1) $\mathbf{A}$ *je pozitivně definitní,*
(2) *Zobrazení* $f : \mathbf{R}^n \times \mathbf{R}^n \to \mathbf{R}$ *dané předpisem* $f(\mathbf{u}, \mathbf{v}) = \mathbf{u} \, \mathbf{A} \, \mathbf{v}^{\mathsf T}$ *je pozitivně definitní symetrická bilineární forma,*
(3) *existuje regulární matice* $\mathbf{P}$ *tak, že* $\mathbf{A} = \mathbf{P}^{\mathsf T}\mathbf{P}$.

Důkaz. (1)$\Rightarrow$(2) Protože je $\mathbf{A}$ symetrická čtvercová matice, zobrazení f je podle 2.6 symetrická bilineární forma s maticí vzhledem ke kanonické bázi $\mathbf{A}$, navíc, je-li $\mathbf{A}$ pozitivně definitní, pak je díky 3.2 f pozitivně definitní.

(2)$\Rightarrow$(3) Protože je $\mathbf{A}$ matice f vzhledem ke kanonické bázi a díky 2.23 existuje báze B vůči níž má f jednotkovou matici, stačí položit $\mathbf{P} = [\mathrm{Id}]_{K_n B}$ a využít Větu 2.3, podle které $\mathbf{A} = [f]_{K_n} = [\mathrm{Id}]_{K_n B}^{\mathsf T} [f]_{K_n} [\mathrm{Id}]_{K_n B} = \mathbf{P}^{\mathsf T}\mathbf{E}\mathbf{P} = \mathbf{P}^{\mathsf T}\mathbf{P}$.

(3)$\Rightarrow$(1) Vezmeme-li nenulový vektor $\mathbf{v} \in \mathbf{R}^n$, pak $\mathbf{v} \, P^{\mathsf T}$ je pro regulární matici $\mathbf{P}$ opět nenulový, a proto $\mathbf{v} \, \mathbf{A} \, \mathbf{v}^{\mathsf T} = \mathbf{v} \, P^{\mathsf T}\mathbf{P} \, \mathbf{v}^{\mathsf T} = \omega(\mathbf{v} \, P^{\mathsf T}, \mathbf{v} \, P^{\mathsf T}) > 0$ $\square$

Příklad. Zjistíme, zda je reálná matice $\mathbf{A} = \begin{pmatrix} 1 & -1 & 1 \\ -1 & 5 & 1 \\ 1 & 1 & 3 \end{pmatrix}$ pozitivně definitní.

Budeme-li ji chápat jako matici reálné bilineární f formy vzhledem ke kanonické bázi, stačí podle Poznámky 5.18 ověřit, zda je tato forma pozitivně definitní. Tedy potřebujeme zjistit, zda matice formy f vzhledem k polární bázi obsahuje na diagonále samá kladná čísla. Budeme tedy symetricky upravovat matici $\mathbf{A}$:

$$\begin{pmatrix} 1 & -1 & 1 \\ -1 & 5 & 1 \\ 1 & 1 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 2 \\ 0 & 2 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Vidíme, že matice má na diagonále pouze kladná čísla, tudíž je pozitivně definitní.

Věta 5.19. *Je-li $\mathbf{A}$ pozitivně definitní symetrická reálná čtvercová matice stupně n, pak existuje právě jedna taková reálná horní trojúhelníková matice $\mathbf{R}$ stupně n s kladnými hodnotami na diagonále, že $\mathbf{A} = \mathbf{R}^{\mathsf{T}}\mathbf{R}$.*

Důkaz. Vezměme regulární matici $\mathbf{P}$, pro níž $\mathbf{A} = \mathbf{P}^{\mathsf{T}}\mathbf{P}$, kterou zaručuje Poznámka 5.18. Podle 5.7 existuje QR rozklad matice $\mathbf{P} = \mathbf{QR}$, proto $\mathbf{A} = \mathbf{P}^{\mathsf{T}}\mathbf{P} = \mathbf{R}^{\mathsf{T}}\mathbf{Q}^{\mathsf{T}}\mathbf{QR} = \mathbf{R}^{\mathsf{T}}\mathbf{R}$. Matice $\mathbf{R}$ je podle definice QR rozkladu horní trojúhelníková s kladnými čísly na diagonále.

Zbývá nám ověřit jednoznačnost. Nechť tedy $\mathbf{A} = \mathbf{R}^{\mathsf{T}}\mathbf{R} = \mathbf{S}^{\mathsf{T}}\mathbf{S}$ pro dvě horní trojúhelníkové matice $\mathbf{R} = (r_{ij})$ a $\mathbf{S} = (s_{ij})$ takové, že $r_{ii} > 0$ a $s_{ii} > 0$. Nejprve si všimněme, že diagonála matice $\mathbf{SR}^{-1}$ je opět kladná. Zřejmě $(\mathbf{RS}^{-1})^{\mathsf{T}} = (\mathbf{S}^{\mathsf{T}})^{-1}\mathbf{R}^{\mathsf{T}} = \mathbf{SR}^{-1}$. Matice $\mathbf{R}$ a $\mathbf{S}$ jsou obě typu U, proto i součin $\mathbf{RS}^{-1}$ a $\mathbf{SR}^{-1}$ jsou podle 5.1 typu U. To ovšem znamená, že jsou matice $\mathbf{RS}^{-1}$ a $\mathbf{SR}^{-1}$ horní a zároveň dolní trojúhelníkové, tedy diagonální. Dále $(\mathbf{SR}^{-1})^{-1} = \mathbf{RS}^{-1} = (\mathbf{RS}^{-1})^{\mathsf{T}} = \mathbf{SR}^{-1}$, tudíž $\mathbf{SR}^{-1}$ je diagonální matice s kladnou diagonálou inverzní sama k sobě, tj. $\mathbf{SR}^{-1} = \mathbf{E}$, a proto $\mathbf{S} = \mathbf{R}$. □

Definice. Nechť $\mathbf{A}$ je pozitivně definitní symetrická reálná čtvercová matice. Potom jednoznačně určenému rozkladu $A = \mathbf{R}^{\mathsf{T}}\mathbf{R}$, kde $\mathbf{R}$ je reálná horní trojúhelníková matice s kladnými čísly na diagonále, budeme říkat *Choleskyho rozklad.*

Příklad. Spočítejme Choleskyho rozklad matice $\mathbf{A} = \begin{pmatrix} 1 & -1 & 1 \\ -1 & 5 & 1 \\ 1 & 1 & 3 \end{pmatrix}$. Budeme-li počítat v souladu s důkazem 5.19, měli bychom nejprve najít regulární matici P tak, aby $\mathbf{P}^{\mathsf{T}}\mathbf{P} = \mathbf{A}$, a potom bychom hledali QR rozklad matice $\mathbf{P}$. Jednodušší ovšem bude, když se nám podaří rovnou určit matici $\mathbf{P}$ jako horní trojúhelníkovou s kladnými čísly na digonále. Upravujme opět matici $\mathbf{A}$ symetrickými elementárními úpravami na řádky a na sloupce tak, abychom dostali jednotkovou matici (tj. kromě odčítání řádků budeme řádky a zároveň odpovídající sloupce násobit také skalárem) a úpravy inverzní k provedeným úpravám na řádky si zapamatujeme

$$\begin{pmatrix} 1 & -1 & 1 \\ -1 & 5 & 1 \\ 1 & 1 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 2 \\ 0 & 2 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Inverzní úpravy k provedeným jsou:

$$R^{\mathsf{T}} = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 2 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

Zřejmě $(\mathbf{R}^{\mathrm{T}})^{-1}\mathbf{A}\mathbf{R}^{-1} = \mathbf{E}$, tedy $\mathbf{R}^{\mathrm{T}}\mathbf{R} = \mathbf{A}$ a matice $\mathbf{R}$ splňuje podmínky Cholesкyho rozkladu. Tedy $\mathbf{A} = \begin{pmatrix} 1 & -1 & 1 \\ -1 & 5 & 1 \\ 1 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 2 & 0 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.

6. Jordanův kanonický tvar matice

Je-li f endomorfismus na prostoru V, bude $f^n = f \dots f$ značit složení n endomorfismů f pro každé $n \geq 1$ a $f^0 = \mathrm{Id}$. Je-li B nějaká množina, pak zápisem $f[B]$ budeme rozumět množinu $\{f(b) \mid b \in B\}$.

Poznámka 6.1. *Nechť f je endomorfismus na komplexním vektorovém prostoru V konečné dimenze n. Potom $\operatorname{Im} f^k \supseteq \operatorname{Im} f^{k+1}$ a $\operatorname{Ker} f^k \subseteq \operatorname{Ker} f^{k+1}$ pro každé $k \geq 1$ a dále*

(a) $\operatorname{Im} f^m = \operatorname{Im} f^n$ *pro všechna $m \geq n$,*
(b) $\operatorname{Ker} f^m = \operatorname{Ker} f^n$ *pro všechna $m \geq n$,*
(c) $V = \operatorname{Im} f^n \oplus \operatorname{Ker} f^n$.

Důkaz. Nejprve si všimněme, že $f^{k+1}(V) = f^k(f(V)) \subseteq f^k(V)$, a jestliže $f^k(\mathbf{v}) = \mathbf{0}$, pak $f^{k+1}(\mathbf{v}) = f(f^k(\mathbf{v})) = f(\mathbf{0}) = \mathbf{0}$, proto $\operatorname{Im} f^k \supseteq \operatorname{Im} f^{k+1}$ a $\operatorname{Ker} f^k \subseteq \operatorname{Ker} f^{k+1}$.

(a) Protože $\dim(\operatorname{Im} f^k) < \dim(\operatorname{Im} f^{k+1})$, jakmile $\operatorname{Im} f^k \neq \operatorname{Im} f^{k+1}$, existuje k, pro které $\operatorname{Im} f^k = \operatorname{Im} f^{k+1}$. Kdyby $k > n$ měli bychom $n = \dim(V) > \dim(\operatorname{Im} f) > \dim(\operatorname{Im} f^2) > \cdots > \dim(\operatorname{Im} f^{n+1}) > \dim(\operatorname{Im} f^{n+1}) \geq 0$, což není možné, proto $\operatorname{Im} f^n = \operatorname{Im} f^{n+1} = \operatorname{Im} f^{n+2} = \dots$.

(b) Dostáváme z (a), inkluze $\operatorname{Ker} f^k \subseteq \operatorname{Ker} f^{k+1}$ a z dokázaného faktu, že $\dim(\operatorname{Ker} f^k) = n - \dim(\operatorname{Im} f^k)$.

(c) Zvolme $\mathbf{v} \in V$. Protože $\operatorname{Im} f^{2n} = \operatorname{Im} f^n$, existuje vektor $\mathbf{w} \in V$, pro který $f^{2n}(\mathbf{w}) = f^n(\mathbf{v})$. Nyní $f^n(\mathbf{v} - f^n(\mathbf{w})) = f^n(\mathbf{v}) - f^{2n}(\mathbf{w}) = \mathbf{0}$, proto $\mathbf{v} - f^n(\mathbf{w}) \in \operatorname{Ker} f^n$ a $\mathbf{v} = f^n(\mathbf{w}) + (\mathbf{v} - f^n(\mathbf{w})) \in \operatorname{Im} f^n \vee \operatorname{Ker} f^n$. Tedy $V = \operatorname{Im} f^n \vee \operatorname{Ker} f^n$. Konečně protože $n = \dim(V) = \dim(\operatorname{Im} f^n) + \dim(\operatorname{Ker} f^n)$. □

Definice. Buď φ endomorfismus na vektorovém prostoru V, řekneme, že podprostor U prostoru V je *invariantním podprostorem endomorfismu* φ, pokud $\varphi(U) \subseteq U$.

Příklad. (1) Triviální podprostory $\{\mathbf{0}\}$ a V prostoru V jsou invariantními podprostory libovolného endomorfismu na V.

(2) Mějme podprostor $U = \langle \mathbf{v}_1, \dots, \mathbf{v}_k \rangle$ prostoru V generovaný vlastními vektory endomorfimsu φ na V. Pak U je invariantním podprostorem endomorfismu φ.

Je-li φ endomorfimus na vektorovém prostoru V a U je jeho invariantním podprostor, pak restrikcí endomorfismu φ na invariantním podprostor U budeme rozumět endomorfismus φ_U na U daný předpisem $\varphi_U(\mathbf{u}) = \varphi(\mathbf{u})$ pro každé $\mathbf{u} \in U$.

Věta 6.2. *Nechť φ je endomorfismus na komplexním vektorovém prostoru konečné dimenze n, $\lambda \in \sigma(\varphi)$ a $f = \varphi - \lambda\,\mathrm{Id}$. Pak $\operatorname{Im} f^k$ a $\operatorname{Ker} f^k$ jsou invariantní podprostory endomorfismu φ pro každé $k \geq 1$.*

Důkaz. Je-li $\mathbf{u} \in \operatorname{Im} f^k$, pak $\varphi(\mathbf{u}) = f(\mathbf{u}) + \lambda\,\mathbf{u}$. Protože $\lambda\,\mathbf{u}$ i $f(\mathbf{u})$ leží v $\operatorname{Im} f^k$, leží také $\varphi(\mathbf{u})$ v $\operatorname{Im} f^k$ a prostor je invariantní.

Nechť $\mathbf{u} \in \operatorname{Ker} f^k$. Ptáme se, zda $\varphi(\mathbf{u}) \in \operatorname{Ker} f^k$. Platí $f^k(\varphi(\mathbf{u})) = f(f^k(\mathbf{u})) + \lambda f^k(\mathbf{u}) = 0$ a prostor $\operatorname{Ker} f^k$ je tedy invariantní. □

Poznámka 6.3. *Buď f endomorfismus na vektorovém prostoru konečné dimenze. Je-li $r > 1$ a B lineárně nezávislá podmnožina nějakého doplňku* $\operatorname{Ker} f^{r-1}$ *v* $\operatorname{Ker} f^r$, *pak je $f[B]$ lineárně nezávislá podmnožina nějakého doplňku* $\operatorname{Ker} f^{r-2}$ *v* $\operatorname{Ker} f^{r-1}$.

Důkaz. Nechť $B = \{\mathbf{u}_1, \dots, \mathbf{u}_k\}$. Máme-li lineární kombinaci $\sum_{j=1}^k \alpha_j f(\mathbf{u}_j) = \mathbf{0}$, pak také $f\left(\sum_{j=1}^k \alpha_j \mathbf{u}_j\right) = \mathbf{0}$. Protože $\langle B\rangle$ má nulový průnik s $\operatorname{Ker} f^{r-1}$, a tedy také s $\operatorname{Ker} f$, platí $\sum_{j=1}^k \alpha_j \mathbf{u}_j = 0$. Všechny koeficienty jsou tedy nulové, neboť B je lineárně nezávislá množina. Vztah $f[B] \subset \operatorname{Ker} f^{r-1}$ plyne z toho, že pro každé $\mathbf{u} \in B$ platí $0 = f^r(\mathbf{u}) = f^{r-1}(f(\mathbf{u}))$. Konečně, pokud $f^{r-2}\left(\sum_{j=1}^k \alpha_j f(\mathbf{u}_j)\right) = \mathbf{0}$, pak $f^{r-1}\left(\sum_{j=1}^k \alpha_j \mathbf{u}_j\right) = \mathbf{0}$, a tedy jsou jako výše všechny koeficienty nulové, díky $\langle B\rangle \bigcap \operatorname{Ker} f^{r-1} = \{\mathbf{0}\}$. □

Věta 6.4. *Buď φ endomorfismus na komplexním vektorovém prostoru V konečné dimenze n, $\lambda \in \sigma(\varphi)$ a nechť platí, že* $\operatorname{Ker}(\varphi - \lambda \operatorname{Id})^k = V$ *pro nějaké $k > 0$. Potom $\sigma(\varphi) = \{\lambda\}$ a existuje báze B prostoru V a taková čísla $\epsilon_1, \dots, \epsilon_{n-1} \in \{0, 1\}$, že*

$$[\varphi]_B = \begin{pmatrix} \lambda & \epsilon_1 & 0 & \dots & 0 \\ 0 & \lambda & \epsilon_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda & \epsilon_{n-1} \\ 0 & 0 & \dots & 0 & \lambda \end{pmatrix}$$

Důkaz. Položme $f = \varphi - \lambda \operatorname{Id}$. Nechť $s \geq 0$ je takové číslo, pro které $\operatorname{Ker} f^s = V$ a $\operatorname{Ker} f^{s-1} \neq V$. Budeme postupně konstruovat bázi s požadovanými vlastnostmi.

Nejprve zvolme bázi B_s nějakého doplňku podprostoru $\operatorname{Ker} f^{s-1}$ v prostoru $\operatorname{Ker} f^s = V$ a označíme ji B_s. Dále postupně definujeme množiny B_r, $r = 1, \dots, s-1$, tak, aby B_r byla báze nějakého doplňku podprostoru $\operatorname{Ker} f^{r-1}$ v prostoru $\operatorname{Ker} f^r$ a současně $f[B_{r+1}] \subseteq B_r$. To je možné díky Větě 6.2. Dostaneme tak bázi $B = \bigcup_{i=1}^s B_i$ celého prostoru V. Vektory báze lze seřadit tak, aby pro libovolné po sobě následující vektory $\mathbf{v}_{i-1}, \mathbf{v}_i$ platilo

$$f(\mathbf{v}_i) = \begin{cases} \mathbf{0} \text{ nebo} \\ \mathbf{v}_{i-1}, \end{cases} \qquad \text{a tedy} \qquad \varphi(\mathbf{v}_i) = \begin{cases} \lambda\,\mathbf{v}_i \text{ nebo} \\ \lambda\,\mathbf{v}_i + \mathbf{v}_{i-1}\,. \end{cases}$$

To ovšem znamená, že má matice endomorfismu φ vzhledem k bázi B právě požadovaný tvar. □

Definice. Mějme čtvercové komplexní matice

$$\mathbf{J}_i = \begin{pmatrix} \lambda_i & 1 & 0 & \dots & 0 \\ 0 & \lambda_i & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_i & 1 \\ 0 & 0 & \dots & 0 & \lambda_i \end{pmatrix}, \quad \mathbf{J} = \begin{pmatrix} \mathbf{J}_1 & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{J}_2 & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{J}_k \end{pmatrix}.$$

Potom matici $\mathbf{J}_i$, která má na diagonále komplexní číslo λ_i, nad diagonálou, tj. na pozicích $(i, i+1)$, jedničku a všude jinde nuly, nazveme *Jordanovou buňkou* a matici $\mathbf{J}$ obsahující v blocích na diagonále Jordanovy buňky $\mathbf{J}_i$ nazveme *Jordanovou maticí.*

Poznámka 6.5. *Nechť* $\mathbf{J}$ *je Jordanova matice podobná matici* $\mathbf{A}$*, buď* $\lambda \in \sigma(\mathbf{A})$*. Označíme-li* $\mathbf{F} = \mathbf{A} - \lambda\mathbf{E}$*, pak* $h(\mathbf{F}^{s-1}) + h(\mathbf{F}^{s+1}) - 2h(\mathbf{F}^s)$ *udává právě počet Jordanových buněk matice stupně* s *s hodnotou* λ *na diagonále v matici* $\mathbf{J}$*.*

Důkaz. Protože jsou matice $\mathbf{A}$ a $\mathbf{J}$ podobné, existuje regulární matice $\mathbf{P}$, pro níž $\mathbf{J} = \mathbf{P}^{-1}\mathbf{A}\mathbf{P}$. Snadno nahlédneme, že $\mathbf{J} - \lambda\mathbf{E} = \mathbf{P}^{-1}(\mathbf{A} - \lambda\mathbf{E})\mathbf{P}$ a $(\mathbf{J} - \lambda\mathbf{E})^s = \mathbf{P}^{-1}(\mathbf{A} - \lambda\mathbf{E})^s\mathbf{P}$ pro každé s, proto $h((\mathbf{J} - \lambda\mathbf{E})^s) = h((\mathbf{A} - \lambda\mathbf{E})^s)$ a můžeme tedy bez újmy na obecnosti počítat s maticí $\mathbf{F} = \mathbf{J} - \lambda\mathbf{E}$.

Je-li $\mathbf{J}_i$ Jordanova buňka stupně s matice $\mathbf{J}$ a $\sigma(\mathbf{J}_i) = \{\lambda\}$, potom a $h((\mathbf{J}_i - \lambda\mathbf{E})^{s-k}) = k$ pro všechna přirozená $k < s$ a $(\mathbf{J}_i - \lambda\mathbf{E})^s = \mathbf{0}$. Jestliže $\lambda \notin \sigma(\mathbf{J}_i)$, pak $h((\mathbf{J}_i - \lambda\mathbf{E})^k) = s$ pro všechna k. Odtud vidíme, že $h((\mathbf{J}_i - \lambda\mathbf{E})^{s-1}) - h((\mathbf{J}_i - \lambda\mathbf{E})^{s-1})$ je to rovno jedné, právě když $\sigma(\mathbf{J}_i) = \{\lambda\}$ a stupeň $\mathbf{J}_i$ je aspoň s, a je to rovno nule jindy. Nyní stačí poznamenat, že rozdíl hodností $h(\mathbf{F}^{s-1}) - h(\mathbf{F}^s)$ udává právě počet Jordanových buněk stupně aspoň s v matice $\mathbf{J}$, proto $h(\mathbf{F}^{s-1}) - h(\mathbf{F}^s) - (h(\mathbf{F}^s) - h(\mathbf{F}^{s+1})) = h(\mathbf{F}^{s-1}) + h(\mathbf{F}^{s+1}) - 2h(\mathbf{F}^s)$ je počet Jordanových buněk matice stupně právě s s vlastním číslam λ. □

Díky 6.4 a předchozímu pozorování dostáváme

Důsledek 6.6. *Nechť* φ *je endomorfismus na komplexním vektorovém prostoru* V *konečné dimenze,* $\lambda \in \sigma(\varphi)$ *a nechť platí, že* $\operatorname{Ker}(\varphi - \lambda \operatorname{Id})^k = V$ *pro nějaké* $k > 0$*. Potom existuje báze* B *prostoru* V *taková, že je* $[\varphi]_B$ *Jordanova matice. Tato matice je určena jednoznačně až na pořadí Jordanových buněk*

Věta 6.7 (Jordanova věta)**.** *Buď* φ *endomorfismus na konečně dimenzionálním komplexním vektorovém prostoru* V*. Pak existuje báze* B *prostoru* V*, pro níž je* $[\varphi]_B$ *Jordanovou maticí. Tato matice je určena jednoznačně až na pořadí Jordanových buněk.*

Důkaz. Položme $n = \dim(V)$ a předpokládejme, že $n > 0$, v opačném případě je tvrzení triviální. Nejprve rozložíme vektorový prostor V na direktní součet invariantních podprostorů, na nichž bude restrikce endomorfismu φ splňovat předpoklady Věty 6.4.

Podle 4.20 existuje vlastní číslo λ_1 endomorfismu φ. Definujme $f_1 = \varphi - \lambda_1 \operatorname{Id}$. Potom 6.2 zaručuje, že $\operatorname{Im} f_1^n$ a $\operatorname{Ker} f_1^n$ jsou invariantní podprostory endomorfismu φ a podle 6.1(c) máme $V = \operatorname{Im} f_1^n \oplus \operatorname{Ker} f_1^n$. Označme nyní ψ_1 restrikci endomorfismu φ na invariantní podprostor $\operatorname{Im} f_1^n$. Pokud $\operatorname{Im} f_1^n \neq \{\mathbf{0}\}$ použijeme opět Poznámku 4.20, podle níž existuje vlastní číslo λ_2 endomorfismu ψ_1 (a tedy i endomorfismu φ). Označme nyní $f_2 = \psi_1 - \lambda_2 \operatorname{Id}$. Díky 6.1(c) a 6.2 dostáváme rozklad $\operatorname{Im} f_1^n = \operatorname{Im} f_2^n \oplus \operatorname{Ker} f_2^n$ podprostoru $\operatorname{Im} f_1$ na dva invariantní podprostory. Dále definujme restrikci ψ_2 endomorfismu ψ_1 (a zároveň φ) na invariantní podprostor $\operatorname{Im} f_2^n$a je-li tento prostor nenulový dostáváme vlastní číslo λ_3 endomorfismu ψ_2 a φ. Opět definujeme $f_3 = \psi_2 - \lambda_3 \operatorname{Id}$ a dostáváme invariantní (vzhledem k φ i ψ_2) rozklad $\operatorname{Im} f_2^n = \operatorname{Im} f_3^n \oplus \operatorname{Ker} f_3^n$ atd.

Všimněme si, že v každém kroku je $\dim(\operatorname{Ker} f_i^n) \geq 1$, protože podprostor $\operatorname{Ker} f_i^n$ obsahuje vlastní vektory příslušné vlastnímu číslu λ_i. Proto po konečně mnoha krocích nastane $\operatorname{Im} f_k^n = \{\mathbf{0}\}$ a získáme tak rozklad

$$V = \operatorname{Ker} f_1^n \oplus \operatorname{Ker} f_2^n \oplus \cdots \oplus \operatorname{Ker} f_k^n.$$

Definujeme-li nyní endomorfismus φ_i jako restrikci endomorfismu φ na invariantní podprostor $\operatorname{Ker} f_i^n$, pak φ_i splňuje předpoklady 6.6. Tudíž existují báze B_i

podprostorů $\operatorname{Ker} f_i^n$ tak, že $[\varphi_i]_{B_i}$ je Jordanova matice. Konečně položme $B = \bigcup_{i=1}^k B_i$. Zřejmě je B báze celého V a navíc

$$[\varphi]_B = \begin{pmatrix} [\varphi_1]_{B_1} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & [\varphi_2]_{B_2} & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & [\varphi_k]_{B_k} \end{pmatrix},$$

tedy $[\varphi]_B$ je opět Jordanova matice.

Zbývá ověřit jednoznačnost nalezené Jordanovy matice. Nechť tedy B a C jsou dvě báze takové, že $[\varphi]_B$ a $[\varphi]_C$ jsou Jordanovy matice. Potom jsou matice $[\varphi]_B$ a $[\varphi]_C$ podobné a závěr plyne z 6.5. □

Příklad. Mějme endomorfismus φ na $\mathbf{C}^3$ s maticí $[\varphi]_{K_3} = \begin{pmatrix} 2 & -2 & -1 \\ 1 & 3 & 1 \\ 1 & 2 & 4 \end{pmatrix}$ vzhledem ke kanonické bázi K_3. Najdeme bázi, vůči níž bude mít φ Jordanovu matici. Nejprve musíme určit spektrum $\sigma(\varphi) = \{3\}$. Definujme $f = \varphi - 3\,\mathrm{Id}$. Určíme jádra $\operatorname{Ker} f$ a $\operatorname{Ker} f^2$ ($\operatorname{Ker} f^3$ už nutně musí být celý prostor $\mathbf{C}^3$). Nejprve spočítáme matice

$$[f]_{K_3} = [\varphi]_{K_3} - 3E = \begin{pmatrix} -1 & -2 & -1 \\ 1 & 0 & 1 \\ 1 & 2 & 1 \end{pmatrix}, \quad [f^2]_{K_3} = [f]_{K_3}^2 = \begin{pmatrix} -2 & 0 & -2 \\ 0 & 0 & 0 \\ 2 & 0 & 2 \end{pmatrix}.$$

Dále najdeme řešení homogenních soustav rovnic s danými maticemi, což budou právě jádra endomorfismů f a f^2. Tedy $\operatorname{Ker} f^3 = \mathbf{C}^3$, $\operatorname{Ker} f^2 = \langle (0,1,0), (1,0,-1) \rangle$ a $\operatorname{Ker} f = \langle (1,0,-1) \rangle$. Zvolíme vektor doplňku $\operatorname{Ker} f^2$ v prostoru $\operatorname{Ker} f^3$, například $(1,0,0)$. Konečně spočítáme vektory $f(1,0,0) = (-1,1,1)$ a $f^2(1,0,0) = (-2,0,2)$ a položíme $B = ((-2,0,2), (-1,1,1), (1,0,0))$. Potom $[\varphi]_B = \begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 3 \end{pmatrix}$.

Uvážíme-li, že čtvercovou komplexní matici můžeme chápat jako matici endomorfismu vzhledem ke kanonické bázi prostoru $\mathbf{C}^n$, dostáváme

Definice. Jordanovu matici podobnou komplexní čtvercové matici $\mathbf{A}$ nazveme *Jordanovým kanonickým tvarem matice* $\mathbf{A}$.

Důsledek 6.8. (1) *Každá kompexní čtvercová matice má Jordanův kanonickým tvar, který je určen jednozmačně až na pořadí buněk.*

(2) *Dvě kompexní čtvercové matice jsou podobné, právě když mají až na pořadí Jordanových buněk stejný Jordanův kanonický tvar.*

Všimněme si, že na diagonále Jordanova kanonického tvaru matice se vyskytují všechna vlastní čísla, každé tolikrát, jaká je jeho násobnost v charakteristickém polynomu.

Příklad. Spočítáme Jordanův kanonický tvar komplexní matice $\mathbf{A} = \begin{pmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 3 & 4 & 2 \end{pmatrix}$

Okamžitě vidíme, že $\sigma(\mathbf{A}) = \{2\}$. Snadno také zjistíme, že matice $\mathbf{A} - 2\mathbf{E}$ má hodnost 2, proto existuje až na násobek jen jeden vlastní vektor matice $\mathbf{A}$. Je-li $\mathbf{A}$ podobná Jordanově matici $\mathbf{J}$, pak $\mathbf{P}^{-1}\mathbf{A}\mathbf{P} = \mathbf{J}$, proto i $\mathbf{P}^{-1}(\mathbf{A} - 2\mathbf{E})\mathbf{P} = \mathbf{J} - 2\mathbf{E}$

pro nějakou regulární matici $\mathbf{P}$. Tedy hodnosti matic $\mathbf{A}-2\mathbf{E}$ a $\mathbf{J}-2\mathbf{E}$ jsou stejné. To ovšem znamená, že ze tří možných Jordanových matic

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \quad \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \quad \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

je matici $\mathbf{A}$ podobná právě poslední z nich.

Příklad. Komplexní matice $\begin{pmatrix} 5 & 3 \\ -3 & -1 \end{pmatrix}$ a $\begin{pmatrix} 2 & 0 \\ 9 & 2 \end{pmatrix}$ mají obě stejný Jordanův kanonický tvar $\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$, a proto jsou podobné.

Připomeňme přirozenou definici k-té mocniny čtvercové matice $\mathbf{A}^k = \overbrace{\mathbf{A}\mathbf{A}\dots\mathbf{A}}^{\text{k-krát}}$.

Příklad. Jordanova věta nám může pomoct při počítání mocnin matic. Nejdříve si uvědomme, že mocninou libovolné Jordanovy matice $\mathbf{J}$ skládající se z Jordanových buněk $\mathbf{J}_1, \dots, \mathbf{J}_s$ je

$$\mathbf{J}^k = \begin{pmatrix} \mathbf{J}_1 & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{J}_2 & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{J}_s \end{pmatrix}^k = \begin{pmatrix} \mathbf{J}_1^k & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{J}_2^k & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{J}_s^k \end{pmatrix}$$

a mocninu Jordanovy buňky dostaneme jako

$$\mathbf{J}_i^k = \begin{pmatrix} \lambda_i & 1 & 0 & \dots & 0 \\ 0 & \lambda_i & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_i & 1 \\ 0 & 0 & \dots & 0 & \lambda_i \end{pmatrix}^k = \begin{pmatrix} \lambda_i^k & \binom{k}{1}\lambda_i^{k-1} & \binom{k}{2}\lambda_i^{k-2} & \dots & \binom{k}{n-1}\lambda_i^{k-n+1} \\ 0 & \lambda_i^k & \binom{k}{1}\lambda_i^{k-1} & \dots & \binom{k}{n-2}\lambda_i^{k-n+2} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_i^k & \binom{k}{1}\lambda_i^{k-1} \\ 0 & 0 & \dots & 0 & \lambda_i^k \end{pmatrix},$$

kde definitoricky položíme $\binom{k}{r}\lambda_i^{k-r} = 0$ pro $r > k$. Dále z 6.8 víme, že pro každou čtvercovou komplexní matici $\mathbf{A}$ existují regulární matice $\mathbf{P}$ a Jordanova matice $\mathbf{J}$ tak, že $\mathbf{A} = \mathbf{P}\mathbf{J}\mathbf{P}^{-1}$, proto $\mathbf{A}^k = \mathbf{P}\mathbf{J}\mathbf{P}^{-1}\mathbf{P}\mathbf{J}\mathbf{P}^{-1}\dots\mathbf{P}\mathbf{J}\mathbf{P}^{-1} = \mathbf{P}\mathbf{J}^k\mathbf{P}^{-1}$.

Popsaným postupem najdeme mocnimu $\mathbf{A}^{45}$ pro matici $\mathbf{A} = \frac{1}{3}\begin{pmatrix} 2 & -2 & -1 \\ 1 & 3 & 1 \\ 1 & 2 & 4 \end{pmatrix}$.

Už jsme spočítali (viz příklad po 6.7), že

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

Proto

$$\mathbf{A}^{45} = \frac{1}{3^{45}} \begin{pmatrix} -2 & -1 & 1 \\ 0 & 1 & 0 \\ 2 & 1 & 0 \end{pmatrix} \begin{pmatrix} 3^{45} & 45 \cdot 3^{44} & 990 \cdot 3^{43} \\ 0 & 3^{45} & 45 \cdot 3^{44} \\ 0 & 0 & 3^{45} \end{pmatrix} \begin{pmatrix} -2 & -1 & 1 \\ 0 & 1 & 0 \\ 2 & 1 & 0 \end{pmatrix}^{-1} =$$

$$= \begin{pmatrix} -2 & -1 & 1 \\ 0 & 1 & 0 \\ 2 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 15 & 110 \\ 0 & 1 & 15 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -\frac{1}{2} & \frac{1}{2} \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} -234 & -30 & -235 \\ 15 & 1 & 15 \\ 235 & 30 & 236 \end{pmatrix}.$$

Definice. *Spektrálním poloměrem* komplexní čtvercové matice $\mathbf{A}$ nazveme reálné číslo $\rho(\mathbf{A}) = max\{|\lambda| \in \mathbf{R} \mid \lambda \in \sigma(\mathbf{A})\}$.

Poznámka 6.9. *Je-li $\mathbf{A}$ komplexní čtvercová matice a k přirozené číslo, pak*

(a) $\sigma(\mathbf{A}^k) = \{\lambda_1^k, \dots, \lambda_s^k\}$, *jestliže* $\sigma(\mathbf{A}) = \{\lambda_1, \dots, \lambda_s\}$,
(b) $\rho(\mathbf{A}^k) = \rho(\mathbf{A})^k$,
(c) $\rho(\mathbf{A}) = 0$, *právě když existuje* $k > 0$ *tak, že* $\mathbf{A}^k = \mathbf{0}$,
(d) $\rho(a \cdot \mathbf{A}) = |a|\rho(\mathbf{A})$ *pro každé* $a \in \mathbf{C}$.

Důkaz. Označme $\mathbf{J}$ Jordanův kanonický tvar matice $\mathbf{A}$.

(a) Stačí spočítat $\mathbf{J}^k$ a uvážit, že $\sigma(\mathbf{A}^k) = \sigma(\mathbf{J}^k)$.

(b) Plyne okamžitě z (a).

(c) Protože $\rho(\mathbf{A}) = 0$, právě když $\sigma(\mathbf{A}) = \{0\}$, tedy Jordanův kanonický tvar $\mathbf{J}$ matice $\mathbf{A}$ má na diagonále samé 0. Proto existuje $k > 0$ tak, že $\mathbf{J}^k = \mathbf{0}$, a tedy $\mathbf{A}^k = \mathbf{0}$.

(d) Je-li $\sigma(\mathbf{A}) = \{\lambda_1, \dots, \lambda_s\}$, stačí si všimnout, že $\sigma(a\mathbf{A}) = \{a\lambda_1, \dots, a\lambda_s\}$. □

Příklad. Snado spočítáme, že pro komplexní matici $M = \begin{pmatrix} -2 & 3 & 2 \\ -1 & 1 & 1 \\ -1 & 2 & 1 \end{pmatrix}$ je spektrum $\sigma(M) = \{0\}$, proto $\rho(M) = 0$ a $M^k = \mathbf{0}$ pro vhodné přirozené číslo k (zřejmě už $M^3 = \mathbf{0}$).

Budeme psát $A = \lim_{n\to\infty} A_n$, kde $A = (a_{ij})$ a $A_n = (a_{nij})$ jsou reálné nebo komplexní matice stejného typu, pokud $a_{ij} = \lim_{n\to\infty} a_{nij}$ pro všechna i, j. Pokud všechny posloupnosti $\{a_{nij}\}_n$ konvergují, říkáme, že posloupnost matic $\{A_n\}_n$ konverguje.

Poznámka 6.10. *Nechť je $\mathbf{A}$ komplexní čtvercová matice a* $\rho(\mathbf{A}) < 1$.

(a) $\lim_{n\to\infty} \mathbf{A}^n = \mathbf{0}$,
(b) $\lim_{n\to\infty} (\mathbf{E} + \mathbf{A} + \mathbf{A}^2 + \dots + \mathbf{A}^n) = (\mathbf{E} - \mathbf{A})^{-1}$.

Důkaz. Buď $\mathbf{J} = \begin{pmatrix} \mathbf{J}_1 & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{J}_2 & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{J}_s \end{pmatrix}$ Jordanův kanonický tvar matice $\mathbf{A}$, tedy existuje regulární matice $\mathbf{P}$, pro níž $\mathbf{A} = \mathbf{PJ}P^{-1}$.

(a) Protože

$$\mathbf{A}^n = \mathbf{PJ}^n P^{-1} = \mathbf{P} \begin{pmatrix} \mathbf{J}_1^n & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{J}_2^n & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{J}_s^n \end{pmatrix} \mathbf{P}^{-1}$$

stačí dokázat, že $\lim_{n\to\infty} \mathbf{J}^n = \mathbf{0}$. Připomeňme, že

$$\mathbf{J}_i^n = \begin{pmatrix} \lambda_i & 1 & 0 & \dots & 0 \\ 0 & \lambda_i & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_i & 1 \\ 0 & 0 & \dots & 0 & \lambda_i \end{pmatrix}^n = \begin{pmatrix} \lambda_i^n & \binom{n}{1}\lambda_i^{n-1} & \binom{n}{2}\lambda_i^{n-2} & \dots & \binom{n}{s-1}\lambda_i^{n-s+1} \\ 0 & \lambda_i^n & \binom{n}{1}\lambda_i^{n-1} & \dots & \binom{n}{s-2}\lambda_i^{n-s+2} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_i^n & \binom{n}{1}\lambda_i^{n-1} \\ 0 & 0 & \dots & 0 & \lambda_i^n \end{pmatrix},$$

kde s je stupeň matice $\mathbf{J}_i$. Protože je $|\lambda_i| < 0$, dostáváme, že $\lim_{n\to\infty} \lambda_i^n = 0$ a $\lim_{n\to\infty} \binom{n}{k}\lambda_i^{n-k} = 0$ pro $k < s$, tedy $\lim_{n\to\infty} \mathbf{J}^n = \mathbf{0}$.

(b) Podobně jako v (a) nahlédneme, že existuje limita $\lim_{n\to\infty}(\sum_{i=0}^n \mathbf{J}^i)$, a proto existuje $\lim_{n\to\infty}(\sum_{i=0}^n \mathbf{A}^i)$. Poté stačí dokázat, že

$$\lim_{n\to\infty}((\mathbf{E}-\mathbf{A})\sum_{i=0}^n \mathbf{A}^i) = \lim_{n\to\infty}(\mathbf{E}-\mathbf{A}^{n+1}) = \mathbf{0},$$

což platí díky (a). □

7. Nezáporné matice

Jsou-li $\mathbf{A} = (a_{ij})$ a $\mathbf{B} = (b_{ij})$ dvě reálné matice stejného typu, potom budeme psát $\mathbf{A} > \mathbf{B}$ resp. $\mathbf{A} \geq \mathbf{B}$, pokud $a_{ij} > b_{ij}$ resp. $a_{ij} \geq b_{ij}$ pro všechny indexy i, j. Podobně pro reálné (řádkové nebo sloupcové) vektory $\mathbf{u} = (u_1, \ldots, u_n)$ a $\mathbf{v} = (v_1, \ldots, v_n)$ budeme psát $\mathbf{u} > \mathbf{v}$ resp. $\mathbf{u} \geq \mathbf{v}$ pokud $u_i > v_i$ resp. $u_i \geq v_i$ pro všechna $i = 1, \ldots, n$.

Definice. Nechť $\mathbf{A}$ je matice. Řekneme, že $\mathbf{A}$ je *kladná* resp. *nezáporná*, pokud je reálná a $\mathbf{A} > \mathbf{0}$ resp $\mathbf{A} \geq \mathbf{0}$. Podobně nazveme vektor $\mathbf{v}$ *kladným* resp. *nezáporným*, pokud se jedná o reálný vektor a $\mathbf{v} > \mathbf{0}$, resp. $\mathbf{v} \geq \mathbf{0}$.

Poznámka 7.1. *Nechť $\mathbf{N}_1$ a $\mathbf{N}_3$ jsou nezáporné matice typu (n, m) a $\mathbf{N}_2$ a $\mathbf{N}_4$ jsou nezáporné matice typu (m, k). Pokud $\mathbf{N}_1 \geq \mathbf{N}_3$ a $\mathbf{N}_2 \geq \mathbf{N}_4$, pak $\mathbf{N}_1\mathbf{N}_2 \geq \mathbf{N}_3\mathbf{N}_4$. Jestlie $\mathbf{N}_1 > \mathbf{N}_3$ a $\mathbf{N}_2 > \mathbf{N}_4$, pak $\mathbf{N}_1\mathbf{N}_2 > \mathbf{N}_3\mathbf{N}_4$.*

Důkaz. Stačí uvážit, že $\mathbf{N}_1\mathbf{N}_2 \geq \mathbf{N}_1\mathbf{N}_4 \geq \mathbf{N}_3\mathbf{N}_4$ v prvním případě, a $\mathbf{N}_1\mathbf{N}_2 > \mathbf{N}_1\mathbf{N}_4 > \mathbf{N}_3\mathbf{N}_4$. □

Pro reálnou nebo komplexní matici $\mathbf{A} = (a_{ij})$ budeme značit $|\mathbf{A}| = (|a_i j|)$ a podobně pro vektor $\mathbf{v} = (v_1, \ldots, v_n)$ budeme značit $|\,\mathbf{v}\,| = (|v_1|, \ldots, |v_n|)$. Zřejmě $|\mathbf{A}| = \mathbf{A}$ pro každou nezápornou matici.

Poznámka 7.2. *Nechť $\mathbf{P}$ je kladná a $\mathbf{N}$ nezáporná čtvercová matice. Potom*

(a) *$\mathbf{P}^k$ je kladná a $\mathbf{N}^k$ je nezáporná matice pro každé $k > 0$,*
(b) *$\mathbf{N}\,\mathbf{u}^{\mathrm{T}} \geq \mathbf{N}\,\mathbf{v}^{\mathrm{T}}$, jestliže $\mathbf{u} \geq \mathbf{v} \geq \mathbf{0}$ a mají-li součiny smysl,*
(c) *$\mathbf{P}\,\mathbf{u}^{\mathrm{T}} > \mathbf{P}\,\mathbf{v}^{\mathrm{T}}$, jestliže $\mathbf{u} \geq \mathbf{v} \geq 0$, $\mathbf{v} \neq \mathbf{u}$ a mají-li součiny smysl,*
(d) *$\mathbf{N}|\,\mathbf{u}\,|^{\mathrm{T}} \geq |\mathbf{N}\,\mathbf{u}^{\mathrm{T}}\,|$ pro každý vektor $\mathbf{u}$, mají-li součiny smysl,*
(e) *$\rho(\mathbf{P}) > 0$.*

Důkaz. (a) Indukční rozšíření 7.1.
(b) a (c) Okamžitý důsledek 7.1.
(d) Snadno dostaneme $\mathbf{N}|\,\mathbf{u}\,|^{\mathrm{T}} = |\mathbf{N}||\,\mathbf{u}\,|^{\mathrm{T}} \geq |\mathbf{N}\,\mathbf{u}^{\mathrm{T}}\,|$.
(e) Protože $\mathbf{P}^k \neq \mathbf{0}$ podle (a), není $\rho(\mathbf{P})$ rovno nule díky 6.9(c). □

Věta 7.3. *Nechť $\mathbf{A}$ je kladná čtvercová matice. Potom $\rho(\mathbf{A})$ je vlastní číslo matice $\mathbf{A}$, a pokud je $\mathbf{v}$ vlastním vektorem příslušným vlastnímu číslu $\rho(\mathbf{A})$, pak $|\,\mathbf{v}\,|$ je kladným vlastním vektorem příslušným $\rho(\mathbf{A})$.*

Důkaz. Vezměme vlastní číslo λ, pro něž $|\lambda| = \rho(\mathbf{A})$ a buď $\mathbf{v}$ příslušný vlastní vektor. Podle 6.9 a 7.2(e) můžeme bez újmy na obecnosti předpokládat, že $\rho(\mathbf{A}) = 1$, tj. $\rho(\mathbf{A}) > 0$ a místo matice $\mathbf{A}$ vezmeme matici $\frac{\mathbf{A}}{\rho(\mathbf{A})}$. Potom podle 7.2(d) platí, že

$$\mathbf{A}|\,\mathbf{v}\,|^{\mathrm{T}} = |\mathbf{A}||\,\mathbf{v}\,|^{\mathrm{T}} \geq |\mathbf{A}\,\mathbf{v}^{\mathrm{T}}\,| = |\lambda\,\mathbf{v}^{\mathrm{T}}\,| = |\lambda||\,\mathbf{v}\,|^{\mathrm{T}} = \rho(\mathbf{A})|\,\mathbf{v}\,|^{\mathrm{T}} = |\,\mathbf{v}\,|^{\mathrm{T}},$$

neboť $\mathbf{A}$ je kladná. Dokažme nyní, že $|\,\mathbf{v}\,|^{\mathsf{T}} \geq \mathbf{A}|\,\mathbf{v}\,|^{\mathsf{T}}$.

Položme $\mathbf{u}^{\mathsf{T}} = \mathbf{A}|\,\mathbf{v}\,|^{\mathsf{T}}$ a ke sporu předpokládejme, že $\mathbf{u} \neq |\,\mathbf{v}\,|$. Už jsme dokázali, že $\mathbf{u}^{\mathsf{T}} = \mathbf{A}|\,\mathbf{v}\,|^{\mathsf{T}} \geq |\,\mathbf{v}\,|^{\mathsf{T}}$, proto $\mathbf{w} = \mathbf{u} - |\,\mathbf{v}\,| \geq \mathbf{0}$ a $\mathbf{w} \neq \mathbf{0}$. Podle 7.2(c) $\mathbf{u}^{\mathsf{T}} > \mathbf{0}^{\mathsf{T}}$ a $\mathbf{A}\,\mathbf{w}^{\mathsf{T}} > \mathbf{0}^{\mathsf{T}}$, tedy existuje (dostatečně malé) $\epsilon > 0$ takové, že $\mathbf{A}\,\mathbf{w}^{\mathsf{T}} > \epsilon\,\mathbf{u}^{\mathsf{T}}$. Proto

$$\mathbf{A}\,\mathbf{u}^{\mathsf{T}} - \mathbf{u}^{\mathsf{T}} = \mathbf{A}\,\mathbf{w}^{\mathsf{T}} > \epsilon\,\mathbf{u}^{\mathsf{T}}, \quad \text{tudíž} \quad \frac{\mathbf{A}\,\mathbf{u}^{\mathsf{T}}}{1+\epsilon} > \mathbf{u}^{\mathsf{T}}.$$

Položíme $\mathbf{B} = \frac{\mathbf{A}}{1+\epsilon}$. Z 7.2(c) plyne, že $\mathbf{B}\,\mathbf{u}^{\mathsf{T}} > \mathbf{u}^{\mathsf{T}}$, $\mathbf{B}^2\,\mathbf{u}^{\mathsf{T}} > \mathbf{B}\,\mathbf{u}^{\mathsf{T}} > \mathbf{u}^{\mathsf{T}}$ atd. Tedy $\mathbf{B}^k\,\mathbf{u}^{\mathsf{T}} > \mathbf{u}^{\mathsf{T}}$ pro každé $k > 0$. Podle 6.9 je $\rho(\mathbf{B}) = \frac{\rho(\mathbf{A})}{1+\epsilon} < 1$, proto nám 6.10(a) zaručuje, že $\lim_{n\to\infty} \mathbf{B}^n = \mathbf{0}$. Dostali jsme spor s tím, že $\mathbf{u}$ je kladný vektor, neboť $\mathbf{B}^k\,\mathbf{u}^{\mathsf{T}} > \mathbf{u}^{\mathsf{T}}$, a proto $\mathbf{0}^{\mathsf{T}} = \lim_{n\to\infty} \mathbf{B}^n\,\mathbf{u}^{\mathsf{T}} \geq \mathbf{u}^{\mathsf{T}} > \mathbf{0}^{\mathsf{T}}$. Tudíž $|\,\mathbf{v}\,|^{\mathsf{T}} = \mathbf{A}|\,\mathbf{v}\,|^{\mathsf{T}}$. □

Věta 7.4 (Perronova věta). *Nechť* $\mathbf{A}$ *je kladná čtvercová matice. Potom* $\rho(\mathbf{A})$ *je vlastní číslo matice* $\mathbf{A}$ *a existuje právě jeden jeho kladný vlastní vektor* $\mathbf{p} = (p_1, \dots, p_n)$ *tak, že* $p_1 + \dots + p_n = 1$. *Navíc každý vlastní vektor příslušný vlastnímu číslu* $\rho(\mathbf{A})$ *je násobkem vektoru* $\mathbf{p}$.

Důkaz. Ve Větě 7.3 jsme dokázali, že $\rho(\mathbf{A})$ je vlastním číslem matice $\mathbf{A}$, a že pro něj existuje kladný vlastní vektor $|\,\mathbf{v}\,| = \mathbf{v} = (v_1, \dots, v_n)$. Položíme-li $\mathbf{p} = \frac{\mathbf{v}}{v_1 + \dots + v_n}$, pak $\mathbf{p}$ zřejmě splňuje požadavek věty. Konečně předpokládejme, že $\mathbf{u}$ je vlastním vektorem příslušným vlastnímu číslu $\rho(A)$, pro nějž $\mathbf{u} = (u_1, \dots, u_n) \notin \langle \mathbf{v} \rangle = \langle \mathbf{p} \rangle$. Vektor $\mathbf{u}$ je nenulový, tedy existuje i tak, že $u_i \neq 0$. Zřejmě je $\mathbf{w} = \mathbf{v} - \frac{v_i}{u_i}\,\mathbf{u}$ opět (nenulovým) vlastním vektorem, jehož i-tá souřadnice je ovšem nulová, tedy $|\,\mathbf{w}\,|$ není kladný vektor. Podle 7.3 ovšem vektor $|\,\mathbf{w}\,|$ kladným vlastním vektorem je, čímž jsme odvodili spor. □

Poznámka 7.5. *Jsou-li* $\mathbf{A}$ *a* $\mathbf{B}$ *dvě nezáporné čtvercové matice stejného stupně a* $\mathbf{A} \geq \mathbf{B}$, *pak* $\rho(\mathbf{A}) \geq \rho(\mathbf{B})$.

Důkaz. Předpokládejme, že $\rho(\mathbf{A}) < \rho(\mathbf{B})$, a $\mathbf{A}_1 = \frac{1}{\rho(\mathbf{B})}\mathbf{A}$ a $\mathbf{B}_1 = \frac{1}{\rho(\mathbf{B})}\mathbf{B}$ Potom $\rho(\mathbf{A}_1) < 1$, a proto $\mathbf{A}_1^n \to \mathbf{0}$ podle 6.10(a), tedy i $\mathbf{B}_1^n \to \mathbf{0}$. Konečně, protože $\rho(\mathbf{B}_1) = 1$, existuje komplexní vlastní číslo λ a vlastní vektor $\mathbf{v}$, pro které $|\lambda| = 1$ a $\mathbf{B}_1^n\,\mathbf{v}^{\mathsf{T}} = \lambda^n\,\mathbf{v}^{\mathsf{T}}$. Ovšem $\lambda^n \not\to 0$, zatímco $\mathbf{B}_1^n\,\mathbf{v}^{\mathsf{T}} \to \mathbf{0}$, spor. □

Poznámka 7.6. *Je-li* $\mathbf{A}$ *nezáporná čtvercová matice, pak je* $\rho(A)$ *vlastní číslo matice* $\mathbf{A}$ *a existuje nezáporný vlastní vektor matice* A *příslušný vlastnímu číslu* $\rho(\mathbf{A})$.

Důkaz. Pro každé přirozené číslo $k > 1$ definujme kladnou matici $\mathbf{A}_k$ takto: $(\mathbf{A}_k)_{i,j} = \frac{1}{k}$, pokud $(\mathbf{A})_{i,j} = 0$ a jinak $(\mathbf{A}_k)_{i,j} = (A)_{i,j}$. Matice $\mathbf{A}$ je zřejmě limitou posloupnosti $(\mathbf{A}_k)_1^\infty$. Podle Perronovy věty má každá matice $\mathbf{A}_k$ kladný vlastní vektor $\mathbf{v}_k$, jehož součet souřadnic je jedna. Z posloupnosti $(\mathbf{v}_k)_1^\infty$ tedy můžeme vybrat konvergentní podposloupnost konvergující k nějakému vektoru $\mathbf{v}$. Díky 7.5 $\rho(\mathbf{A}_k) \geq \rho(\mathbf{A}_{k+1}) \geq \rho(\mathbf{A})$, proto $\rho(\mathbf{A}_k)$ konverguje k reálnému $\lambda \geq \rho(\mathbf{A})$. Poznamenejme, že součet jeho souřadnic je 1, proto je $\mathbf{v}$ nenulový. Konečně

$$\mathbf{A}\,\mathbf{v}^{\mathsf{T}} = \lim_{k\to\infty} \mathbf{A}_k \cdot \lim_{k\to\infty} \mathbf{v}_k^{\mathsf{T}} = \lim_{k\to\infty} \mathbf{A}_k\,\mathbf{v}_k^{\mathsf{T}} = \lim_{k\to\infty} \rho(\mathbf{A}_k)\,\mathbf{v}_k^{\mathsf{T}} = \lambda\,\mathbf{v}^{\mathsf{T}},$$

Tedy $\mathbf{v}$ je vlastní vektor matice $\mathbf{A}$ a $\lambda \geq \rho(\mathbf{A})$. □

Příklad. Je-li $\mathbf{A} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, pak $\rho(\mathbf{A}) = 0$ a nezáporný vlastní vektor matice $\mathbf{A}$ je tvaru $(r, 0)$ pro r kladné, tedy kladný vlastní vektor ani kladné vlastní číslo matice $\mathbf{A}$ neexistuje.

Definice. Řekneme, že matice $\mathbf{A}$ je *primitivní*, pokud je nezáporná čtvercová a existuje $k > 0$ takové, že $\mathbf{A}^k > \mathbf{0}$.

Věta 7.7 (Perronova-Frobeniova věta)**.** *Nechť $\mathbf{A}$ je primitivní matice. Potom $\rho(\mathbf{A})$ je kladné vlastní číslo matice $\mathbf{A}$ a existuje právě jeden kladný vlastní vektor $\mathbf{p} = (p_1, \dots, p_n)$ tak, že $p_1 + \dots + p_n = 1$. Navíc každý vlastní vektor příslušný vlastnímu číslu $\rho(\mathbf{A})$ je násobkem vektoru $\mathbf{p}$.*

Důkaz. Podle 7.6 je $\rho(\mathbf{A})$ vlastní číslo $\mathbf{A}$ a díky 7.4 s 6.9(b) je $\rho(\mathbf{A}^k) = \rho(\mathbf{A})^k$ vlastní číslo $\mathbf{A}^k$ a $\rho(\mathbf{A})^k > 0$, je-li $k > 0$ takové, že $\mathbf{A}^k > \mathbf{0}$. Navíc máme-li $\mathbf{A}\,\mathbf{v}^{\mathrm{T}} = \rho(\mathbf{A})\,\mathbf{v}^{\mathrm{T}}$, pak $\mathbf{A}^k\,\mathbf{v}^{\mathrm{T}} = \rho(\mathbf{A})^k\,\mathbf{v}^{\mathrm{T}}$. Z unicity vlastního vektoru matice $\mathbf{A}^k$ příslušného vlastnímu číslu $\rho(\mathbf{A}^k)$ plyne závěr. □

Jednoznačně určenému vektoru $\mathbf{p}$ z 7.4 a 7.7 budeme říkat *Perronův vektor* matice $\mathbf{A}$.

Příklad. Mějme orientovaný (případně kladnými reálnými hodnotami ohodnocený orientovaný) graf $\mathcal{G}$ s množinou vrcholů $\{v_1, \dots, v_n\}$ a buď $\mathbf{A}$ matice incidence grafu $\mathcal{G}$, tj.

$$a_{ij} = \begin{cases} 1 & \text{pokud existuje hrana } v_i \to v_j \\ 0 & \text{jindy} \end{cases}$$

(v případě ohodnoceného grafu je a_{ij} rovno hodnotě hrany $v_i \to v_j$). Poznamenejme, že $\mathbf{A}$ je nezáporná čtvercová matice. Předpokládejme, že jsou každé dva různé vrcholy grafu $\mathcal{G}$ spojeny orientovanou cestou (tj. pro každé i a j existuje posloupnost hran $v_i \to v_{i_1} \to \dots v_{i_s} \to v_j$, řekneme, že $\mathcal{G}$ je *silně souvislý*), ukážeme, že $(\mathbf{A} + \mathbf{E})^n > \mathbf{0}$, tedy že $\mathbf{A} + \mathbf{E}$ je primitivní matice. Uvědomme si, že nejkratší orientovaná cesta z vrcholu i do vrcholu j má nejvýše $n - 1$ hran, vezměme si takovou orientovanou cestu $v_i \to v_{i_1} \to \dots v_{i_{k-1}} \to v_j$, která zřejmě obsahuje právě $k < n$ hran. Dále si všimněme, že číslo na pozici (i, j) matice $\mathbf{A}^{k+1}$ je součtem nezáporných hodnot, z nichž sčítanec $a_{ii_1} a_{i_1 i_2} \dots a_{i_{k-2} i_{k-1}} a_{i_{k-1} j}$ je zřejmě kladný. Protože však je hodnota na j-té pozici diagonály matice $(\mathbf{A} + \mathbf{E})^{n-k-1}$ také kladná, máme na místě (i, j) matice $(\mathbf{A} + \mathbf{E})^n = (\mathbf{A} + \mathbf{E})^{k+1} (\mathbf{A} + \mathbf{E})^{n-k-1}$ kladné číslo. Tím jsme dokázali, že $(\mathbf{A} + \mathbf{E})^n$ je kladná matice, tedy matice $\mathbf{A} + \mathbf{E}$ je primitivní. Navíc si všimněme, že $\mathbf{A}^n \neq \mathbf{0}$, proto $\rho(\mathbf{A}) > 0$ podle 6.9(d).

Příklad (Google)**.** Mějme systém webových stránek označených čísly $1, 2, \dots, n$, který budeme reprezentovat jako vrcholy grafu $\mathcal{G}$, přitom z vrcholu (stránky) i povede j do hrana právě tehdy, když bude na stránku i odkazovat stránka j. Nechť $\mathbf{A} = (a_{ij})$ je matice incidence tohoto grafu. Vyslovme požadavek, že důležitost i-té webové stránky je lineárně závislá na součtu důležitostí stránek, které na ni odkazují. To můžeme pomocí matice A vyjádřit tak, že $x_i = c \sum_{j=1}^{n} a_{ij} x_j$, kde x_i je "hodnota důležitosti" i-té stránky a c je kladná konstanta vyjadřující naší přímou úměrnost. Označíme-li $\mathbf{x} = (x_1, \dots, x_n)$ *vektor důležitosti*, pak $\mathbf{A}\mathbf{x}^{\mathrm{T}} = \frac{1}{c}\mathbf{x}^{\mathrm{T}}$. Pochopitelně chceme, aby byl vektor důležitost nezáporný.

Budeme předpokládat, že orientovaný graf webu $\mathcal{G}$ je silně souvislý (tj. vyšetřujeme zvlášť každou komponentu silné souvislosti grafu webu, hrany v takovém případě mohou vést pouze z "důležitější" komponenty do komponenty "méně důležité", žádná opačně). Zjistili jsme (viz předchozí příklad), že $\rho(\mathbf{A}) > 0$, dále podle 7.6 je $\rho(\mathbf{A})$ vlastní číslo matice $\mathbf{A}$, a podle 7.7 je $\rho(\mathbf{A}) + 1 > 1$ vlastní číslo matice $\mathbf{A}+\mathbf{E}$. Tudíž $r = \rho(\mathbf{A}+\mathbf{E}) \geq \rho(\mathbf{A})+1 > 1$. Navíc víme, že $\mathbf{A}+\mathbf{E}$ je primitivní matice, tedy podle 7.7 existuje kladný Perronův vektor $\mathbf{x}$, pro nějž $(\mathbf{A}+\mathbf{E})\mathbf{x}^{\mathrm{T}} = r\mathbf{x}^{\mathrm{T}}$, a proto $\mathbf{A}\mathbf{x}^{\mathrm{T}} = (r-1)\mathbf{x}^{\mathrm{T}}$. Položíme-li $c = \frac{1}{r-1} > 0$, našli jsme vektor důležitosti (dané komponenty souvislosti) našeho systém webových stránek.

Definice. *Stochastickou maticí* budeme rozumět nezápornou čtvercovou matici, jejíž každý řádek ma součet hodnot roven jedné.

Poznámka 7.8. *Součin stochastických matic stejného stupně je stochastickou maticí.*

Důkaz. Mějme stochastické matice $\mathbf{S} = (s_{ij})$, $\mathbf{P} = (p_{ij})$, pak součet hodnot v i-tém řádku matice $\mathbf{SP}$ je $\sum_j \sum_k s_{ik}p_{kj} = \sum_k s_{ik} \sum_j p_{kj} = \sum_k s_{ik} = 1$. □

Příklad. Buď $S_1, S_2, \ldots, S_n$ stavy (nějakého děje či přístroje) a označme p_{ij} pravděpodobnost toho, že po uplynutí jedné časové jednotky nastane po stavu S_i stav S_j. Protože po každém stavu nastane některý ze stavů S_j, platí, že $\sum_{j=1}^{n} p_{ij} = 1$. Tedy $\mathbf{P} = (p_{ij})$ je stochastická matice. Pozice (i,j) (podle 7.9 rovněž stochastické) matice $\mathbf{P}^k$ přitom obsahuje právě pravděpodobnost toho, že se po uplynutí k časových jednotek stav S_i změní na stav S_j.

Poznámka 7.9. *Nechť* $\mathbf{A}$ *je stochastická matice stupně* n *a* $\mathbf{e} = (1,1,\ldots,1) \in \mathbf{R}^n$. *Pak* $\mathbf{A}\mathbf{e}^{\mathrm{T}} = \mathbf{e}^{\mathrm{T}}$ *a* $\rho(\mathbf{A}) = 1$.

Důkaz. Podmínka $\mathbf{A}\mathbf{e}^{\mathrm{T}} = \mathbf{e}^{\mathrm{T}}$ plyne přímo z definice stochastické matice. Díky 7.6 je $\rho(\mathbf{A})$ vlastní číslo a existuje jeho nezáporný vlastní vektor $\mathbf{v} = (v_1, \ldots, v_n)$, pro který platí $v_i \leq 1$ pro všechna i a existuje takové j, že $v_i \neq 0$. Potom $\mathbf{A}^s \mathbf{v}^{\mathrm{T}} = \rho(\mathbf{A})^s \mathbf{v}^{\mathrm{T}}$ pro všechna $s \in \mathbf{N}$. Označíme-li $(x_1, \ldots, x_n) = \mathbf{A}^s \mathbf{v}^{\mathrm{T}}$, pak $x_i = \sum_j \mathbf{A}^s_{ij} v_j \leq \sum_j \mathbf{A}^s_{ij} = 1$, protože $\mathbf{A}^s$ je stochastická matice podle 7.8. To ovšem znamená, že $\rho(\mathbf{A})^s v_j \leq 1$ pro všechna s, tedy $\rho(\mathbf{A}) = 1$. □

Poznámka 7.10. *Nechť* $\mathbf{S}$ *je stochastická matice a* $\mathbf{A}$ *nezáporná matice, pro níž* $\mathbf{A} \neq \mathbf{S}$, $S \geq \mathbf{A}$ *a existuje kladný vlastní vektor matice* $\mathbf{A}^{\mathrm{T}}$ *příslušný vlastnímu číslu* $\rho(\mathbf{A}) = \rho(\mathbf{A}^{\mathrm{T}})$. *Pak* $\rho(\mathbf{A}) < 1$.

Důkaz. Podle 7.5 a 7.9 je $\rho(\mathbf{A}) \leq 1$ vlastní číslo $\mathbf{A}$. Bu $\lambda = \rho(\mathbf{A})$ a $\mathbf{v}$ kladný vlastní vektor matice $\mathbf{A}^{\mathrm{T}}$ příslušný λ. Potom $\mathbf{e} = \mathbf{e}\mathbf{S}^{\mathrm{T}} \geq \mathbf{e}\mathbf{A}^{\mathrm{T}}$ a existuje souřadnice, kde se součiny liší, proto $\mathbf{e}\,\mathbf{v}^{\mathrm{T}} = \mathbf{e}\mathbf{S}^{\mathrm{T}}\,\mathbf{v}^{\mathrm{T}} > \mathbf{e}\mathbf{A}^{\mathrm{T}}\,\mathbf{v}^{\mathrm{T}} = \lambda\mathbf{e}\,\mathbf{v}^{\mathrm{T}}$, tudíž $\lambda < 1$. □

Příklad (Leontievův ekonomický model)**.** Uvažujeme uzavřenou soustavu průmyslových podniků označených $P_1, \ldots, P_n$, z nichž každý vyrábí právě jeden výrobek. *P-jednotkou* nazveme počet (resp. podíl) výrobků podniku P s cenou rovnou jedné finanční jednotce (např 1 US dolar). Označme

s_i počet P_i-jednotek produkovaných podnikem P_i za rok a

a_{ij} počet P_i-jednotek potřebných pro produkci jedné P_j-jednotky, potom je

$a_{ij}s_j$ počet P_i-jednotek spotřebovaných podnikem P_j za rok,

$\sum_{j=1}^{n} a_{ij}s_j$ počet P_i-jednotek spotřebovaných všemi podniky za rok a

$c_j = \sum_{i=1}^n a_{ij}$ je množství finančních jednotek nutných k výrobě P_j-jednotky.

Konečně

$d_i = s_i - \sum_{j=1}^n a_{ij} s_j$ je počet P_i-jednotek určených k (vnější) spotřebě.

Položme $\mathbf{A} = (a_{ij}) \geq \mathbf{0}$ a nazvěme $\mathbf{d} = (d_1, \dots, d_n) \geq \mathbf{0}$ *vektorem poptávky* a $\mathbf{s} = (s_1, \dots, s_n)$ *vektorem nabídky*. Rádi bychom určili vektor $\mathbf{s}$ pro předem daný vektor poptávky $\mathbf{d}$, samozřejmě rozumným řešením úlohy budou jen nezáporné hodnoty s_i, tj požadujeme, aby $\mathbf{s} \geq \mathbf{0}$.

Převedeme-li úlohu do maticového tvaru máme najít $\mathbf{s}$ tak, aby $\mathbf{d}^{\mathsf{T}} = (\mathbf{E} - \mathbf{A})\mathbf{s}^{\mathsf{T}}$, tedy pro regulární matici dostáváme, že $\mathbf{s}^{\mathsf{T}} = (\mathbf{E} - \mathbf{A})^{-1}\mathbf{d}^{\mathsf{T}}$. Nemáme ovšem ničím zaručeno, že matice $(\mathbf{E} - \mathbf{A})^{-1}$ a vektor $\mathbf{s}$ budou nezáporné (koneckonců nevíme ani to, zda je matice $(\mathbf{E} - \mathbf{A})$ regulární), proto musíme uvážit další podmínky kladené na systém. Předně můžeme oprávněně předpokládat, že každý výrobek alespoň zprostředkovaně ke své produkci potřebuje všechny ostatní výrobky, tj. orientovaný ohodnocený graf s maticí $\mathbf{A}$ je silně souvislý. Navíc by ve zdravé ekonomice mělo pro všechna j platit, že $c_j \leq 1$ (tj. náklady na výrobek by neměly převyšovat cenu výrobku) a alespoň jeden podnik P_k by měl vydělávat, tj. $c_k < 1$. Potom $S \geq \mathbf{A}^{\mathsf{T}}$ pro nějakou stochastickou matici $\mathbf{S} \neq \mathbf{A}^{\mathsf{T}}$, stejnou úvahou jako v předchozím příkladu najdeme kladný vlastní vektor matice A příslušný $\rho(A)$, proto podle Poznámky 7.10 je $\rho(\mathbf{A}) = \rho(\mathbf{A}^{\mathsf{T}}) < 1$. Tudíž z 6.10(b) dostáváme, že $(\mathbf{E} - \mathbf{A})^{-1} = \lim\limits_{n\to\infty} (\mathbf{E} + \mathbf{A} + \mathbf{A}^2 + \dots + \mathbf{A}^n) \geq \mathbf{0}$ (mohli bychom dokonce dokázat, že $(\mathbf{E} - \mathbf{A})^{-1}$ je kladná matice, což plyne z pozorování, které jsme učinili v předchozích dvou příkladech, totiž že $(\mathbf{E} + \mathbf{A})^k > \mathbf{0}$). Ukázali jsme, že za vyslovených předpokladů je matice $(\mathbf{E} - \mathbf{A})$ regulární a vektor nabídky je jednoznačně určený nezáporný vektor $\mathbf{s}^{\mathsf{T}} = (\mathbf{E} - \mathbf{A})^{-1}\mathbf{d}^{\mathsf{T}} \geq \mathbf{0}^{\mathsf{T}}$.

8. Afinní a euklidovské prostory

Definice. *Afinním prostorem* nazveme dvojici (A, V), kde A je neprázdná množina (bodů) a V je vektorový prostor konečné dimenze, spolu se zobrazením $+ : A \times V \to A$ splňujícím podmínky

(1) $a + \mathbf{0} = a$ a $a + (\mathbf{u} + \mathbf{v}) = (a + \mathbf{u}) + \mathbf{v}$ pro všechna $a \in A$ a $\mathbf{u}, \mathbf{v} \in V$,
(2) pro každé $a, b \in A$ existuje právě jeden vektor $\mathbf{v} \in V$ tak, že $a + \mathbf{v} = b$.

Jednoznačně určený vektor $\mathbf{v}$ pro nějž $a + \mathbf{v} = b$ budeme značit $b - a$.

Euklidovským prostorem budeme rozumět trojici (A, V, g), kde (A, V) je afinní a (V, g) reálný unitární prostor.

Všimněme si, že symbolem $+$ značíme dvě různá zobrazení, jednak binární operaci na vektorovém prostoru a potom zobrazení „posunutí bodu o vektor". Podobně i symbol $-$ používáme ve dvou různých (vzájemně nezaměnitelných) významech.

Příklad. 1) Nechť V je libovolný vektorový prostor konečné dimenze, potom dvojice (V, V) s afinním zobrazením $V \times V \to V$ daným vektorovým sčítáním je afinním prostorem.

2) Nechť (V, g) je libovolný reálný unitární prostor konečné dimenze, potom dvojice (V, V, g) se zobrazením $V \times V \to V$ daným vektorovým sčítáním je euklidovským prostorem.

3) Obvyklý „geometrický” třídimenzionální prostor bodů a vektorů v $\mathbf{R}^3$ se standardním pojmem vzdálenosti, je euklidovským prostorem $(\mathbf{R}^3, \mathbf{R}^3, \omega)$ z předchozí konstrukce.

Poznámka 8.1. *Buď (A, V) afinním prostoru, $a, b, c \in A$ a $\mathbf{u}, \mathbf{v} \in V$. Pak*

a) $a + (b - a) = b$ *($\in A$),*
b) $(a - b) + (b - c) = a - c$ *($\in V$),*
c) $(a + \mathbf{u}) - (b + \mathbf{v}) = (a - b) + \mathbf{u} - \mathbf{v}$ *($\in V$),*
d) $(a + \mathbf{u}) - (b + \mathbf{u}) = (a - b)$,
e) $(a + \mathbf{u}) - (a + \mathbf{v}) = \mathbf{u} - \mathbf{v}$.

Definice. *Podprostorem afinního prostoru* (A, V) nazveme takovou dvojici (B, W), že $B \subseteq A$, W je podprostorem V a (B, W) je afinním prostorem s operací posunutí bodu o vektor $+ : A \times V \to A$ omezenou na podmnožinu $B \times W$. *Podprostorem euklidovského prostoru* (A, V, g) nazveme podprostor (B, W) afinního podprostoru (A, V).

Každý euklidovský prostor je zároveň afinním prostorem (zapomeneme-li na skalární součin), proto následující tvrzení o afinních prostorech popisují i vlastnosti euklidovských prostorů.

Poznámka 8.2. *Nechť (A, V) je afinní prostor, $\emptyset \neq B \subseteq A$ a W je podprostor V. Pak (B, W) je podprostorem (A, V) právě tehdy, když pro každé $a, b \in B$ a $\mathbf{v} \in W$ je $b - a \in W$ a $a + \mathbf{v} \in B$.*

Poznámka 8.3. *Nechť (A, V) je afinní prostor.*

a) *Je-li W podprostor V, $a \in A$ a $B = \{a + \mathbf{w} \mid \mathbf{w} \in W\}$, pak (B, W) je podprostor (A, V).*
b) *Je-li (B, W) podprostor (A, V) a $a \in B$, pak $B = \{a + \mathbf{w} \mid \mathbf{w} \in W\}$.*

Předchozí poznámka umožňuje zápis libovolnéhp podprostoru (B, W) afinního podprostoru (A, V) ve tvaru $B = b + W$, tj. jako součtu vybraného bodu $b \in B$ a podprostoru W. Všimněme si, že $A = a + V$ pro všechny body $a \in A$.

Příklad. Mějme afinní prostor $(\mathbf{R}^3, \mathbf{R}^3)$ (nebo euklidovský prostor $(\mathbf{R}^3, \mathbf{R}^3, \omega)$). Pak každou reálnou přímku můžeme vyjádřit ve tvaru $\{a + t\,\mathbf{v} \mid t \in \mathbf{R}\} = a + \langle \mathbf{v} \rangle$ a každou rovinu můžeme vyjádřit ve tvaru $\{a + (s\,\mathbf{u} + t\,\mathbf{v}) \mid s, t \in \mathbf{R}\} = a + \langle \mathbf{u}, \mathbf{v} \rangle$, kde $\mathbf{u}$ a $\mathbf{v}$ jsou lineárně nezávislé vektory. V Poznámce 8.2 a) jsme ukázali, že přímky a roviny jsou podprostory afinního prostoru $(\mathbf{R}^3, \mathbf{R}^3)$. Přidáme-li k nim ještě podprostory tvaru $a + \{\mathbf{0}\}$ a $\mathbf{R}^3 = a + \mathbf{R}^3$, pak nám Poznámka 8.2 b) říká, že už žádné další podprostory afinního prostoru $(\mathbf{R}^3, \mathbf{R}^3)$ neexistují.

Definice. *Souřadnou soustavou* afinního prostoru (A, V) budeme rozumět takovou posloupnost $S = \{a, \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$, že $a \in A$ a $B = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ je báze V. *Souřadnicemi* bodu $b \in A$ vzhledem k souřadné soustavě S nazveme souřadnice vektoru $b - a$ vzhledem k bázi B, píšeme $\{b\}_S = \{b - a\}_B$.

Kartézskou souřadnou soustavou euklidovského prostoru (A, V, g) nazveme souřadnou soustavu $S = \{a, \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$ afinního prostoru (A, V), v níž $(\mathbf{v}_1, \dots, \mathbf{v}_n)$ tvoří ortonormální bázi unitárního prostoru (V, g).

Poznámka 8.4 (Transformace souřadnic)**.** *Nechť $S = \{a, \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$ a $S' = \{a', \mathbf{v}'_1, \mathbf{v}'_2, \dots, \mathbf{v}'_n\}$ jsou dvě souřadné soustavy v afinním prostoru (A, V). Pak pro každý bod $b \in A$ platí*

$$\{b\}_S = \{a'\}_S + \{b\}_{S'} [\mathrm{Id}]^{\mathrm{T}}_{(\mathbf{v}'_i)(\mathbf{v}_i)},$$

kde $[\mathrm{Id}]_{(\mathbf{v}'_i)(\mathbf{v}_i)}$ *je matice přechodu od báze* $(\mathbf{v}_1,\dots,\mathbf{v}_n)$ *k bázi* $(\mathbf{v}'_1,\dots,\mathbf{v}'_n)$.

Příklad. Uvažujme afinní prostor $(\mathbf{R}^2,\mathbf{R}^2)$ se sčítáním bodu a vektoru po složkách (tj. daným sčítáním v reálném vektorovém prostoru $\mathbf{R}^2$). Pro přehlednost budeme body i jejich souřadnice označovat $[r,s]\in\mathbf{R}^2$ narozdíl od vektorů značených $(r,s)\in\mathbf{R}^2$. Mějme souřadné soustavy $S=\{[0,0],(1,0),(0,1)\}$ a $S'=\{[1,1],(1,1),(1,-1)\}$ a označme $B=((1,0),(0,1))$ a $B'=((1,1),(1,-1))$. Známe-li souřadnice bodu $\{b\}_{S'}=[1,2]$. Určíme podle Poznámky 8.3 jeho souřadnice vzhledem ke (kanonické) bázi S:

$$\{b\}_S=\{[1,1]\}_S+[1,2][\mathrm{Id}]^{\mathtt{T}}_{B'B}=\{[1,1]-[0,0]\}_B+[1,2]\begin{pmatrix}1&1\\1&-1\end{pmatrix}=$$

$$=[1,1]+[3,-1]=[4,0].$$

Věta 8.5 (Popis podprostorů rovnicemi)**.** *Buď* V *vektorový prostor nad tělesem* T *dimenze* n*,* W *jeho podprostor dimenze* $n-k$*,* $S=\{a,\mathbf{v}_1,\mathbf{v}_2,\dots,\mathbf{v}_n\}$ *souřadná soustava v afinním prostoru* (A,V) *a nechť* (B,W) *je podprostor* (A,V)*, kde* $B=b+W$*. Pak existuje matice* M *typu* (k,n) *a vektor* $\mathbf{y}\in T^k$ *tak, že bod* $c\in A$ *leží v* B *právě tehdy, když* $M\{c\}^{\mathtt{T}}_S=\mathbf{y}^{\mathtt{T}}$.

Důkaz. Označme $D=(\mathbf{v}_1,\mathbf{v}_2,\dots,\mathbf{v}_n)$ a $W_D=\{\{\mathbf{w}\}_D\in\mathbf{T}^n|\ \mathbf{w}\in W\}\subseteq\mathbf{T}^n$. Pak je W_D podprostor dimenze $n-k$ prostoru $\mathbf{T}^n$. Zvolme nějakou bázi $(\mathbf{w}_1,\dots,\mathbf{w}_{n-k})$ podprostoru W_D a seřaďme vektory $\mathbf{w}_i$ do matice $B=\begin{pmatrix}\mathbf{w}_1\\\vdots\\\mathbf{w}_{n-k}\end{pmatrix}$. Matice B má zřejmě hodnost $n-k$ a existuje nějaká báze $(\mathbf{v}_1,\dots,\mathbf{v}_k)\subseteq T^n$ podprostoru všech řešení homogenní soustavy s maticí B. Položme $M=\begin{pmatrix}\mathbf{v}_1\\\vdots\\\mathbf{v}_k\end{pmatrix}$. Snadno nahlédneme, že M je matice hodnosti k, jejíž množinu všech řešení tvoří právě W_D. Podle Poznámky 8.3 je $c\in B$, právě když $c-b\in W$, tj. $\{c-b\}_D\in W_D$. To nastává v důsledku Poznámky 8.1 b) právě tehdy, když $\mathbf{0}=M\{c-b\}^{\mathtt{T}}_D=M\{c-a\}^{\mathtt{T}}_D-M\{b-a\}^{\mathtt{T}}_D=M\{c\}^{\mathtt{T}}_S-M\{b\}^{\mathtt{T}}_S$, což je konečně ekvivalentní tomu, že $M\{c\}_S=\mathbf{y}^{\mathtt{T}}$, kde $\mathbf{y}=M\{b\}_S$. □

Příklad. Buď $S=\{[0,0,0,0],(1,0,0,0),(0,1,0,0),(0,0,1,0),(0,0,0,1)\}$ souřadná soustava v afinním prostoru $(\mathbf{R}^4,\mathbf{R}^4)$ a buď (B,W) podprostor $(\mathbf{R}^4,\mathbf{R}^4)$, kde $W=\langle(2,1,-2,-1),(1,1,3,1)\rangle$ a $B=[0,2,1,0]+W$. Najdeme podle Věty 8.5 rovnice, které nám vzhledem k souřadné soustavě S určují podprostor B.

Snadno zjistíme, že například vektory $(5,-8,1,0)$ a $(2,-3,0,1)$ tvoří bázi řešení homogenní soustavy rovnic s maticí $\begin{pmatrix}2&1&-2&-1\\1&1&3&1\end{pmatrix}$. Dále $\{[0,2,1,0]\}_S=[0,2,1,0]$, proto v podprostoru B leží právě ty body $x\in A$ pro něž

$$\begin{pmatrix}5&-8&1&0\\2&-3&0&1\end{pmatrix}x^{\mathtt{T}}=\begin{pmatrix}5&-8&1&0\\2&-3&0&1\end{pmatrix}[0,2,1,0]^{\mathtt{T}}=[-15,-6]^{\mathtt{T}}.$$

Tedy $\{[x_1,x_2,x_3,x_4]\}_S=[x_1,x_2,x_3,x_4]\in B$ právě tehdy, když

$$\begin{aligned}5x_1-8x_2+x_3&=-15,\\2x_1-3x_2+x_4&=-6.\end{aligned}$$

Definice. Buď (B_1, W_1) a (B_2, W_2) dva podprostory afinního prostoru (A, V). Pak řekneme, že podprostory (B_1, W_1) a (B_2, W_2) jsou

– *rovnoběžné*, pokud $W_1 \subseteq W_2$ nebo $W_2 \subseteq W_1$,
– *různoběžné*, pokud nejsou rovnoběžné a $B_1 \cap B_2 \neq \emptyset$,
– *mimoběžné*, pokud nejsou rovnoběžné ani různoběžné.

Poznámka 8.6. *Nechť* (B_1, W_1) *a* (B_2, W_2) *jsou dva podprostory afinního prostoru* (A, V)*. Pak jsou následující podmínky ekvivalentní.*

(1) $B_1 \cap B_2 \neq \emptyset$.
(2) *Pro každé* $b_1 \in B_1$ *a* $b_2 \in B_2$ *je* $b_1 - b_2 \in W_1 + W_2$.
(3) *Existují* $b_1 \in B_1$ *a* $b_2 \in B_2$ *takové, že* $b_1 - b_2 \in W_1 + W_2$.

Příklad. Podprostory $[1,1,2,0] + \langle (1,0,1,0), (1,1,0,0) \rangle$ a $[0,0,1,0] + \langle (0,0,0,1) \rangle$ afinního prostoru $(\mathbf{R}^4, \mathbf{R}^4)$ podle definice zřejmě nejsou rovnoběžné, neboť platí, že $\langle (1,0,1,0), (1,1,0,0) \rangle \cap \langle (0,0,0,1) \rangle = \{\mathbf{0}\}$. Navíc $(1,1,1,0) = [1,1,2,0] - [0,0,1,0] \notin \langle (1,0,1,0), (1,1,0,0), (0,0,0,1) \rangle$, proto jsou podprostory podle Poznámky 8.6 mimoběžné.

Příklad (Vzdálenost mimoběžných podprostorů)**.** Buď (B_1, W_1) a (B_2, W_2) dvojice mimoběžných podprostorů euklidovského prostoru (A, V, g). *Vzdáleností* dvou bodů $a, b \in A$ budeme rozumět hodnotu $\|a - b\|_g$ a vzdáleností podprostorů B_1 a B_2 budeme nazývat hodnotu $d(B_1, B_2) = min\{\|b_1 - b_2\|_g | \ b_1 \in B_1, \ b_2 \in B_2\}$. Pokud $B_1 = a_1 + W_1$ a $B_2 = a_2 + W_2$, hledáme minimální hodnotu $\|(a_1 - a_2) - \mathbf{w}\,\|_g$, kde $\mathbf{w} \in W_1 + W_2$. Z Poznámky 3.17 víme, že hodnota $\|(a_1 - a_2) - \mathbf{w}\,\|_g$ je minimální, pokud $\mathbf{w} = P_{W_1 + W_2}(a_1 - a_2)$, tj. vektor je $(a_1 - a_2) - \mathbf{w}$ kolmý na W. Můžeme tedy úkol řešit pomocí metody nejmenších čtverců.

Mějme $B_1 = [1,0,5] + \langle (1,1,2) \rangle$ a $B_2 = [0,0,1] + \langle (1,0,1) \rangle$ dva mimoběžné podprostory euklidovského prostoru $(\mathbf{R}^3, \mathbf{R}^3, \omega)$. Pomocí metody nejmenších čtverců zjistíme, že $([1,0,5] - [0,0,1]) - 1 \cdot (1,1,2) - 1 \cdot (1,0,1) = (-1,-1,1)$ je kolmou částí rozkladu vektoru $[1,0,5] - [0,0,1]$ na část vektoru z W a $W^{\perp}$. Z předchozí úvahy plyne, že vzdálenost podprostorů B_1 a B_2 je $\|(-1,-1,1)\|_\omega = \sqrt{3}$.