1 Skalární součin

Definice 1.1 (Standardní skalární součin)

Buďte $\mathbf{u}, \mathbf{v} \in \mathbb{C}^n$. Pak standardní skalární součin $\mathbf{u}$ a $\mathbf{v}$ definujeme jako $\mathbf{u} \cdot \mathbf{v} = \overline{u_1} \cdot v_1 + \ldots + \overline{u_n} \cdot v_n$.

Definice 1.2 (Euklidovská norma)

Nechť $\cdot$ je standardní skalární součin na $\mathbf{V}$. Potom $\forall \mathbf{v} \in \mathbf{V}$ definujeme euklidovskou normu jako $||\mathbf{v}|| = \sqrt{\mathbf{v} \cdot \mathbf{v}}$.

Definice 1.3 (Skalární součin)

Nechť $\mathbf{V}$ je vektorový prostor nad $\mathbb{C}$. Skalární součin je zobrazení $\cdot : \mathbf{V} \times \mathbf{V} \to \mathbb{C}$, které ($\forall \mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbf{V}$ a $\forall t \in \mathbb{C}$) splňuje:

$$\mathbf{u} \cdot \mathbf{v} = \overline{\mathbf{v} \cdot \mathbf{u}}, \text{ (Symetričnost)}$$

$$\mathbf{u} \cdot (t\mathbf{v}) = t(\mathbf{u} \cdot \mathbf{v}), \ \mathbf{u} \cdot (\mathbf{v} + \mathbf{w}) = \mathbf{u} \cdot \mathbf{v} + \mathbf{u} \cdot \mathbf{w}, \text{ (Linearita)}$$

$$\langle \mathbf{u}, \mathbf{u} \rangle \geq 0 \wedge (\langle \mathbf{u}, \mathbf{u} \rangle = 0 \Leftrightarrow \mathbf{u} = \mathbf{o}).$$

Definice 1.4 (Hermitovsky sdružená matice)

Nechť $A = (a_{ij}) \in \mathbb{C}^{m \times n}$, potom hermitovsky sdružená matice je $A^* = (\overline{a_{ji}})$.

Čtvercová matice je Hermitovská, pokud je rovna své hermitovsky sdružené matici.

Definice 1.5

Buď $\mathbb{T} = \mathbb{R}$ nebo $\mathbb{C}$ a buď $A = T^{n \times n}$. Pak A je pozitivně definitní, pokud je hermitovská a platí

$$\mathbf{u} * Au \geq 0 \wedge (\mathbf{u} * Au = 0 \Leftrightarrow \mathbf{u} = \mathbf{o}).$$

Důsledek
$\langle \cdot, \cdot \rangle_A = \cdot^* A \cdot$ je skalární součin, právě když A je pozitivně definitní.

Definice 1.6 (Norma)

Buď $\mathbf{V}$ VP nad $\mathbb{R}$ nebo $\mathbb{C}$ se skalárním součinem $\langle \cdot, \cdot \rangle$. Pak normou vektoru $\mathbf{u} \in \mathbf{V}$ rozumíme $||\mathbf{u}|| = \sqrt{\langle \mathbf{u}, \mathbf{u} \rangle}$.

Tvrzení 1.1 (Vlastnosti normy)

$$||\mathbf{u}|| \geq 0 \wedge (||\mathbf{u}|| = 0 \Leftrightarrow \mathbf{u} = \mathbf{o}).$$

$$\forall t \in \mathbb{T} : ||t\mathbf{u}|| = |t| \cdot ||\mathbf{u}||.$$

$$||\mathbf{u} + \mathbf{v}||^2 + ||\mathbf{u} - \mathbf{v}||^2 = 2||\mathbf{u}||^2 + 2||\mathbf{v}||^2.$$

$$\Re(\langle \mathbf{u}, \mathbf{v} \rangle) = \frac{1}{2}||\mathbf{u} + \mathbf{v}||^2 - ||\mathbf{u}||^2 - ||\mathbf{v}||^2.$$

Věta 1.2 (Cauchy-Schwarzova nerovnost)

Buď $\mathbb{T} = \mathbb{R}$ *nebo* $\mathbb{C}$*,* $\mathbf{V}$ *VP nad* $\mathbb{T}$ *se skalárním součinem* $\langle \cdot, \cdot \rangle$*. Pak platí* $\forall \mathbf{u}, \mathbf{v} \in \mathbf{V}$: $| \langle \mathbf{u}, \mathbf{v} \rangle | \leq ||\mathbf{u}|| \cdot ||\mathbf{v}||$. *Rovnost platí právě tehdy, pokud* $(\mathbf{u}, \mathbf{v})$ *je lineárně závislá.*

Důkaz
Případ 1): $(\mathbf{u}, \mathbf{v})$ je LZ: Buď $\mathbf{u} = t\mathbf{v}$: $| \langle \mathbf{u}, \mathbf{v} \rangle | = | \langle \mathbf{u}, t \cdot \mathbf{u} \rangle | = |t| \cdot | \langle \mathbf{u}, \mathbf{u} \rangle | = |t| \cdot ||\mathbf{u}|| \cdot ||\mathbf{u}|| = ||\mathbf{u}|| \cdot ||\mathbf{v}||$.

Případ 2): $(\mathbf{u}, \mathbf{v})$ je LN: Víme, že $||\mathbf{u} - t\mathbf{v}||^2 > 0$. Zvolme t tak, aby $\langle \mathbf{v}, \mathbf{u} - t\mathbf{v} \rangle = 0$. (To lze, protože $\langle \mathbf{v}, \mathbf{u} - t\mathbf{v} \rangle = \langle \mathbf{v}, \mathbf{u} \rangle - t \langle \mathbf{v}, \mathbf{v} \rangle = \langle \mathbf{v}, \mathbf{u} \rangle - t||\mathbf{v}||^2 \implies t = \frac{\langle \mathbf{v}, \mathbf{u} \rangle}{||\mathbf{v}||^2}$.) $0 < ||\mathbf{u} - t\mathbf{v}||^2 = \langle \mathbf{u} - t\mathbf{v}, \mathbf{u} - t\mathbf{v} \rangle = \langle \mathbf{u}, \mathbf{u} - t\mathbf{v} \rangle - \overline{t} \cdot \langle \mathbf{v}, \mathbf{u} - t\mathbf{v} \rangle = \langle \mathbf{u}, \mathbf{u} - t\mathbf{v} \rangle = \langle \mathbf{u}, \mathbf{u} \rangle - t \langle \mathbf{u}, \mathbf{v} \rangle = ||\mathbf{u}||^2 - \frac{\langle \mathbf{v}, \mathbf{u} \rangle \cdot \langle \mathbf{u}, \mathbf{v} \rangle}{||\mathbf{v}||^2} = ||\mathbf{u}||^2 - \frac{\overline{\langle \mathbf{u}, \mathbf{v} \rangle} \cdot \langle \mathbf{u}, \mathbf{v} \rangle}{||\mathbf{v}||^2} = ||\mathbf{u}||^2 - \frac{|\langle \mathbf{u}, \mathbf{v} \rangle|^2}{||\mathbf{v}||^2}$.

Tj. $0 < ||\mathbf{u}||^2 \cdot ||\mathbf{v}||^2 - | \langle \mathbf{u}, \mathbf{v} \rangle |^2$, tedy $| \langle \mathbf{u}, \mathbf{v} \rangle | \leq ||\mathbf{u}|| \cdot ||\mathbf{v}||$. □

Důsledek (Trojúhelníková nerovnost)
Buď $\mathbb{T} = \mathbb{R}$ nebo $\mathbb{C}$, $\mathbf{V}$ VP nad $\mathbb{T}$ se skalárním součinem $\langle \cdot, \cdot \rangle$. Pak platí $\forall \mathbf{u}, \mathbf{v} \in \mathbf{V}$: $||\mathbf{u} + \mathbf{v}|| \leq ||\mathbf{u}|| + ||\mathbf{v}||$. Rovnost platí právě tehdy, pokud $(\mathbf{u}, \mathbf{v})$ je lineárně závislá.

Důkaz
$||\mathbf{u}+\mathbf{v}||^2 = \langle \mathbf{u} + \mathbf{v}, \mathbf{u} + \mathbf{v} \rangle = \langle \mathbf{u}, \mathbf{u} \rangle + \langle \mathbf{v}, \mathbf{u} \rangle + \langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{v}, \mathbf{v} \rangle = ||\mathbf{u}||^2 + \langle \mathbf{u}, \mathbf{v} \rangle + \overline{\langle \mathbf{u}, \mathbf{v} \rangle} + ||\mathbf{v}||^2 = ||\mathbf{u}||^2 + 2\Re(\langle \mathbf{u}, \mathbf{v} \rangle) + ||\mathbf{v}||^2 \leq ||\mathbf{u}||^2 + 2| \langle \mathbf{u}, \mathbf{v} \rangle | + ||\mathbf{v}||^2 \leq ||\mathbf{u}||^2 + 2 \cdot ||\mathbf{u}|| \cdot ||\mathbf{v}|| + ||\mathbf{v}||^2 = (||\mathbf{u}|| + ||\mathbf{v}||)^2$. □

Definice 1.7 (Kolmost)

Buď $\mathbf{V}$ VP se skalárním součinem $\langle \cdot, \cdot \rangle$ a $\mathbf{u}, \mathbf{v} \in \mathbf{V}$. Řekneme, že $\mathbf{u}$ a $\mathbf{v}$ jsou kolmé, značíme $\mathbf{u} \perp \mathbf{v}$, pokud $\langle \mathbf{u}, \mathbf{v} \rangle$.

Poznámka
Ze skoro symetrie (SSS) plyne, že relace jsou kolmé je symetrická.

Definice 1.8 (Kolmost množin)

Množina nebo posloupnost M vektorů VP $\mathbf{V}$ s $\langle \cdot, \cdot \rangle$ se nazývá ortogonální, pokud každá dvojice různých prvků M je kolmá. Nazývá se ortonormální, pokud je ortogonální a každý prvek má normu 1.

Důsledek
Kanonická báze je ortonormální. Normovaná (tj. každý prvek vydělíme normou) ortogonální množina / posloupnost je ortonormální.

Tvrzení 1.3 (Pythagorova věta)

$\mathbf{V}$ vektorový prostor se $\langle \cdot, \cdot \rangle$, buďte $\mathbf{u}, \mathbf{v} \in \mathbf{V}$ kolmé vektory. Pak

$$||\mathbf{u} + \mathbf{v}||^2 = ||\mathbf{u}||^2 + ||\mathbf{v}||^2.$$

Důkaz

$$||\mathbf{u}+\mathbf{v}||^2 = \langle \mathbf{u} + \mathbf{v}, \mathbf{u} + \mathbf{v} \rangle = \langle \mathbf{u}, \mathbf{u} \rangle + \langle \mathbf{v}, \mathbf{u} \rangle + \langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{v}, \mathbf{v} \rangle = \langle \mathbf{u}, \mathbf{u} \rangle + 0 + 0 + \langle \mathbf{v}, \mathbf{v} \rangle = ||\mathbf{u}||^2 + ||\mathbf{v}||^2.$$

□

Důsledek
Je-li $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ ortogonální posloupnost, pak $||\mathbf{v}_1 + \ldots + \mathbf{v}_k||^2 = ||\mathbf{v}_1||^2 + \ldots + ||\mathbf{v}_k||^2$.

Důkaz
Indukcí triviálně. □

Tvrzení 1.4

Buď $\mathbf{V}$ vektorový prostor s $\langle \cdot, \cdot \rangle$ a $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ ortogonální posloupnost nenulových vektorů. Pak je $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ LN.

Důkaz
Předpokládejme, že $0 = a_1 \mathbf{v}_1 + \ldots + a_k \mathbf{v}_k$, kde $a_1, \ldots, a_k \in \mathbb{T}$ ($\mathbb{T} = \mathbb{R} \vee \mathbb{T} = \mathbb{C}$). Chceme ukázat, že $a_1 = \ldots = a_k = 0$.

$$\forall i \in [k] : 0 = \langle v_i, \mathbf{o} \rangle = \langle \mathbf{v}_i, a_1 \mathbf{v}_1 + \ldots + a_k \mathbf{v}_k \rangle = a_1 \langle \mathbf{v}_i, \mathbf{v}_1 \rangle + \ldots + a_k \langle \mathbf{v}_i, \mathbf{v}_k \rangle = a_i \cdot ||\mathbf{v}_i||^2 \implies a_i = 0.$$

□

1.1 Ortonormální báze a vyjádření vektorů vzhledem k nim

Tvrzení 1.5

$\mathbf{V}$ VP s $\langle \cdot, \cdot \rangle$, $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ ortonormální báze. Pak pro každý $\mathbf{u} \in \mathbf{V}$ platí:

$$\mathbf{u} = \langle \mathbf{v}_1, \mathbf{u} \rangle \cdot \mathbf{v}_1 + \ldots + \langle \mathbf{v}_n, \mathbf{u} \rangle \cdot \mathbf{v}_n.$$

To jest

$$[\mathbf{u}]_B = (\langle \mathbf{v}_1, \mathbf{u} \rangle, \ldots, \langle \mathbf{v}_k, \mathbf{u} \rangle)^T.$$

Důkaz

Vezmeme $a_1, \ldots, a_n \in \mathbb{T}$ tak, aby $\mathbf{u} = a_1\mathbf{v}_1 + \ldots + a_n\mathbf{v}_n$. Máme $\langle \mathbf{v}_i, \mathbf{u} \rangle = \langle \mathbf{v}_i, a_1\mathbf{v}_1 + \ldots + a_n\mathbf{v}_n \rangle = a_1 \cdot 0 + \ldots + a_i + \ldots + a_n \cdot 0 = a_i$. □

Poznámka

Kdyby B byla jen ortogonální, pak $[\mathbf{u}]_B = (\frac{\langle \mathbf{v}_1, \mathbf{u} \rangle}{||\mathbf{v}_1||}, \ldots, \frac{\langle \mathbf{v}_k, \mathbf{u} \rangle}{||\mathbf{v}_k||})^T$.

Poznámka

$a_1, \ldots, a_n$ se někdy nazývají Fourierovy koeficienty.

Tvrzení 1.6

$\mathbf{V}$ VP s $\langle \cdot, \cdot \rangle$, $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ ortonormální báze, $\mathbf{u}, \mathbf{w} \in \mathbf{V}$. Pak $\langle \mathbf{u}, \mathbf{w} \rangle = [\mathbf{u}]_B \cdot [\mathbf{w}]_B = [\mathbf{u}]_B^*[\mathbf{w}]_B$.

Důkaz

Buď $[\mathbf{u}]_B = (a_1, \ldots, a_n)^T$, $[\mathbf{w}]_B = (b_1, \ldots, b_n)^T$. Pak $\langle \mathbf{u}, \mathbf{v} \rangle = \langle a_1\mathbf{v}_1 + \ldots + a_n\mathbf{v}_n, b_1\mathbf{v}_1 + \ldots + b_n\mathbf{v}_n \rangle = \sum_{i=1}^n \sum_{j=1}^n \overline{a_i} \cdot b_j \cdot \langle \mathbf{v}_i, \mathbf{v}_j \rangle = \sum_{i=1}^n \overline{a_i} b_i \cdot \langle \mathbf{v}_i, \mathbf{v}_i \rangle = [\mathbf{u}]_B^*[\mathbf{w}]_B$. □

1.2 Kolmost množin

Definice 1.9 (Kolmost množin)

$\mathbf{V}$ VP s $\langle \cdot, \cdot \rangle$, $\mathbf{v} \in \mathbf{V}$, $M, N \subseteq \mathbf{V}$. Pak řekneme, že $\mathbf{v}$ je kolmý k M, značíme $\mathbf{v} \perp M$, pokud $\mathbf{v} \perp \mathbf{w}\ \forall \mathbf{w} \in M$, a řekneme, že M je kolmá k N, značíme $M \perp N$, pokud $\mathbf{v} \perp \mathbf{w}\ \forall \mathbf{v} \in M\ \forall \mathbf{w} \in N$.

Definice 1.10

Buď $\mathbf{V}$ VP s $\langle \cdot, \cdot \rangle$ a buď $\mathbf{W} \leq \mathbf{v}$. Je-li $\mathbf{v} \in \mathbf{V}$, ortogonální projekcí vektoru $\mathbf{v}$ na podprostor $\mathbf{W}$ rozumíme vektor $\mathbf{w}$ takový, že $\mathbf{w} \in \mathbf{W}$ a $\mathbf{v} - \mathbf{w} \perp \mathbf{w}$.

Věta 1.7

Buď $\mathbf{V}$ VP s $\langle \cdot, \cdot \rangle$, buď $\mathbf{W} \leq \mathbf{V}$, $\mathbf{v} \in \mathbf{V}$ a $\mathbf{w} \in \mathbf{W}$ ortogonální projekce $\mathbf{v}$ na $\mathbf{W}$. Potom pro každý vektor $\mathbf{u} \in \mathbf{W}$ různý od $\mathbf{w}$ platí: $||\mathbf{v} - \mathbf{w}|| < ||\mathbf{v} - \mathbf{u}||$.

Speciálně existuje-li ortogonální projekce $\mathbf{v}$ na $\mathbf{W}$, pak je určena jednoznačně.

Důkaz
Z předpokladu $\mathbf{w}, \mathbf{u}$, a tedy i $\mathbf{w} - \mathbf{u}$ jsou vektory $\mathbf{W}$. Tudíž $\mathbf{v} - \mathbf{w} \perp \mathbf{w} - \mathbf{u}$ ($\mathbf{v} - \mathbf{w} \perp \mathbf{W}$). Z Pythagorovy věty: $||\mathbf{v} - \mathbf{u}||^2 = ||\mathbf{v} - \mathbf{w}||^2 + ||\mathbf{w} - \mathbf{u}||^2 > ||\mathbf{v} - \mathbf{w}||^2$. □

Tvrzení 1.8

Buď $\mathbf{V}$ VP s $\langle \cdot, \cdot \rangle$ a buďte $M, N \subseteq \mathbf{V}$. Pak $M \perp N \Leftrightarrow M \perp \mathrm{LO}(N)$ ($\Leftrightarrow \mathrm{LO}(M) \perp \mathrm{LO}(N)$).

Důkaz
$\Leftarrow$: Triviální (protože $N \subseteq \mathrm{LO}(N)$).

$\Longrightarrow$: Předpokládejme, že $M \perp N$. Vezměme $\mathbf{v} \in M$ a $\mathbf{w} = a_1\mathbf{w}_1 + \ldots + a_n\mathbf{w}_n \in \mathrm{LO}(N)$. Pak $\langle \mathbf{v}, \mathbf{w} \rangle = a_1 \langle \mathbf{v}_1, \mathbf{w}_1 \rangle + \ldots + a_n \langle \mathbf{v}_n, \mathbf{w}_n \rangle = 0$. □

Tvrzení 1.9

Buď $\mathbf{V}$ VP s $\langle \cdot, \cdot \rangle$ a $\mathbf{W} \leq \mathbf{V}$, který má ortonormální bázi $B = (\mathbf{u}_1, \ldots, \mathbf{u}_n)$. Pak pro libovolné $\mathbf{v} \in \mathbf{V}$ je

$$\mathbf{w} := \langle \mathbf{u}_1, \mathbf{v} \rangle \cdot \mathbf{u}_1 + \langle \mathbf{u}_2, \mathbf{v} \rangle \mathbf{u}_2 + \ldots + \langle \mathbf{u}_k, \mathbf{v} \rangle \cdot \mathbf{u}_k$$

ortogonální projekcí do $\mathbf{W}$.

Důkaz
Zjevně $\mathbf{w} \in \mathrm{LO}(B) = \mathbf{W}$. Chceme ukázat, že $\mathbf{v} - \mathbf{w} \perp \mathbf{W}$. Podle tvrzení výše stačí ukázat, že $\mathbf{v} - \mathbf{w} \perp \mathbf{u}_i, \forall i \in [k]$. Označme $a_i := \langle \mathbf{u}_i, \mathbf{v} \rangle$.

$$\langle \mathbf{u}_i, \mathbf{v} - \mathbf{w} \rangle = \langle \mathbf{u}_i, \mathbf{v} - a_1\mathbf{u}_1 - a_2\mathbf{u}_2 - \ldots - a_k\mathbf{u}_k \rangle = a_i - a_1 \cdot 0 - \ldots - a_i \cdot 1 - \ldots - a_k \cdot 0 = \mathbf{o}.$$

□

Definice 1.11 (Gramova-Schmidtova ortogonalizace)

Postup, který vezme LN posloupnost $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ z VP s $\langle \cdot, \cdot \rangle$ a vytvoří ortonormální posloupnost $(\mathbf{u}_1, \ldots, \mathbf{u}_k)$ taková, že $\forall i \in [k] : \mathrm{LO}\{\mathbf{v}_1, \ldots, \mathbf{v}_i\} = \mathrm{LO}\{\mathbf{u}_1, \ldots, \mathbf{u}_i\}$.

1) $\mathbf{u}_1 := \frac{\mathbf{v}_1}{||\mathbf{v}_1||}$. 2) Pro každé $i = 2, \ldots, k$ spočítáme $\mathbf{w}_i = \langle \mathbf{u}_1, \mathbf{v}_i \rangle \cdot \mathbf{u}_1 + \ldots + \langle \mathbf{u}_{i-1}, \mathbf{v}_i \rangle \cdot \mathbf{u}_{i-1}$ a položíme $\mathbf{u}_i = \frac{\mathbf{v}_i - \mathbf{w}_i}{||\mathbf{v}_i - \mathbf{w}_i||}$.

Důkaz

To, že $(\mathbf{u}_1, \ldots, \mathbf{u}_i)$ je ortonormální $\forall i \in [k]$ dokážeme triviálně indukcí.

Stejně tak, že $\text{LO}\{\mathbf{v}_1, \ldots, \mathbf{v}_i\} = \text{LO}\{\mathbf{u}_1, \ldots, \mathbf{u}_i\}$.

$$\mathbf{u}_i = \frac{\mathbf{v}_i}{||\ldots||} - \frac{\mathbf{w}_i}{||\ldots||}, \frac{\mathbf{w}_i}{||\ldots||} \in \text{LO}\{\mathbf{u}_1, \ldots, \mathbf{u}_{i-1}\} \stackrel{\text{IP}}{=} \text{LO}\{\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}\}.$$

$\mathbf{v}_i$ také z definice.

Nakonec musíme ukázat, že nikdy nedělíme nulou (naopak, pokud dostaneme špatný (= LZ) vstup, tak dělíme). Ukáže se, že kdybychom dělili, tak nějaké $\mathbf{u}_i \in \text{LO}\{\mathbf{u}_1, \ldots, \mathbf{u}_{i-1}\}$. □

Věta 1.10

Máme-li $\mathbf{V}$ VP s $\langle\cdot,\cdot\rangle$ a aplikujeme-li GS ortogonalizaci na LN posloupnost vektorů z $\mathbf{V}$, pak dostaneme ortonormální posloupnost, že se jejich LO rovnají.

Důkaz

Viz předchozí důkaz. □

Důsledek

Každý konečně generovaný VP se skalárním součinem má ortonormální bázi.

Důsledek

Máme-li $\mathbf{V}$ konečně generovaný VP s $\langle\cdot,\cdot\rangle$ a ortonormální posloupnost $(\mathbf{u}_1, \ldots, \mathbf{u}_k)$, můžeme ji doplnit na ortonormální bázi.

Důkaz

Doplníme na bázi a aplikujeme GS ortogonalizaci, kde si rozmyslíme, že nám nezmění původní posloupnost. □

Důsledek

Je-li $\mathbf{V}$ konečně generovaný VP s ortonormální bází $B = (\mathbf{u}_1, \ldots, \mathbf{u}_n)$ a s $\langle\cdot,\cdot\rangle$, pak existuje isomorfismus $\mathbf{V} \to T^n$ takový, že $\forall \mathbf{v}, \mathbf{w} : \langle \mathbf{v}, \mathbf{w}\rangle = f(\mathbf{v}) \cdot f(\mathbf{w})$.

Poznámka

Aplikováním GS ortogonalizace na $\mathbb{T}^n$ dostaneme tzv. QR - rozklad matice, kde $A = Q \cdot R$ a A má za sloupce původní vektory, Q má ortonormální posloupnost sloupců a R je horní trojúhelníková s nezápornými reálnými čísly na diagonále.

1.3 Ortogonální doplněk, Gramova matice

Definice 1.12

Buď $\mathbf{V}$ VP s $\langle\cdot,\cdot\rangle$ nad $\mathbb{T}=\mathbb{R}$ nebo $\mathbb{C}$. Je-li $M\subseteq\mathbf{V}$ množina vektorů, pak ortogonálním doplňkem k M ve $\mathbf{V}$, rozumíme

$$M^\perp=\{\mathbf{v}\in\mathbf{v}|\mathbf{v}\perp M\}=\{\mathbf{v}\in\mathbf{V}|(\forall\mathbf{u}\in M:\langle\mathbf{v},\mathbf{u}\rangle=0)\}\,.$$

Důsledek
$M\perp M^\perp$ a $M^\perp$ je největší taková množina vzhledem k inkluzi.

Tvrzení 1.11

$\mathbf{V}$ *VP s* $\langle\cdot,\cdot\rangle$, $M\subseteq\mathbf{V}$. *Pak* $M^\perp=(\mathrm{LO}\,M)^\perp$, $M^\perp$ *je podprostor* $\mathbf{V}$, $M\subseteq N\implies N^\perp\subseteq M^\perp$.

Důkaz

$$\mathbf{v}\in M^\perp\Leftrightarrow\mathbf{v}\perp M\Leftrightarrow\mathbf{v}\perp\mathrm{LO}\,M\Leftrightarrow\mathbf{v}\in(\mathrm{LO}\,M)^\perp.$$

Vezmeme $\mathbf{w}_1,\mathbf{w}_2\in M^\perp$ a $t\in\mathbb{T}$, pak $\forall\mathbf{v}\in M:\langle\mathbf{v},\mathbf{w}_1+\mathbf{w}_2\rangle=\langle\mathbf{v},\mathbf{w}_1\rangle+\langle\mathbf{v},\mathbf{u}_2\rangle=0+0=0$ a $\langle\mathbf{v},t\cdot\mathbf{w}_1\rangle=t\cdot\langle\mathbf{v},\mathbf{w}_1\rangle=t\cdot 0=0\implies\mathbf{w}_1+\mathbf{w}_2,t\cdot\mathbf{w}_1\in M^\perp$.

Ať $M\subseteq N$. Pak $\mathbf{v}\in N^\perp\Leftrightarrow\mathbf{v}\perp N\implies\mathbf{v}\perp M\Leftrightarrow\mathbf{v}\in M^\perp$. □

Věta 1.12

Buď $\mathbf{V}$ *VP s* $\langle\cdot,\cdot\rangle$ *nad* $\mathbb{R}$ *nebo* $\mathbb{C}$. *Buď* $\mathbf{W}\leq\mathbf{V}$ *konečně generovaný. Pak platí:*

$$1)\mathbf{V}=\mathbf{W}\oplus\mathbf{W}^\perp.$$

$$2)(\mathbf{W}^\perp)^\perp=\mathbf{W}.$$

3) Každý vektor $\mathbf{v}\in\mathbf{V}$ *má (jednoznačnou) ortogonální projekci jak na* $\mathbf{W}$, *tak ne* $\mathbf{W}^\perp$.
4) Je-li $\mathbf{V}$ *konečně generovaný dimenze* n, *pak* $n=\dim\mathbf{W}+\dim\mathbf{W}^\perp$.

Důkaz
1) Triviálně $\mathbf{W} \cap \mathbf{W}^\perp = \{\mathbf{o}\}$. Navíc použitím toho, že existuje ortogonální projekce (a toho, že je kolmá) na $\mathbf{W}$ máme, že $\mathbf{W} + \mathbf{W}^\perp = \mathbf{V}$.

2) $\mathbf{W} \subseteq (\mathbf{W}^\perp)^\perp$: je-li $\mathbf{w} \in \mathbf{W}$, pak $w \perp (\mathbf{W}^\perp)$, tj. $w \in (\mathbf{w}^\perp)^\perp$. Naopak $(\mathbf{W}^\perp)^\perp \subseteq \mathbf{W}$: vezměme $\mathbf{v} \in (\mathbf{W}^\perp)^\perp$. Uvažujme ortogonální projekci $\mathbf{v}$ na $\mathbf{W}$:

$$(\mathbf{W}^\perp)^\perp \ni \mathbf{v} = \mathbf{w} + (\mathbf{v} - \mathbf{w}) \wedge \mathbf{v} - \mathbf{w} \in (\mathbf{W}^\perp)^\perp \implies (\mathbf{v} - \mathbf{w}) \perp (\mathbf{v} - \mathbf{w}) \implies \mathbf{v} - \mathbf{w} = \mathbf{o} \implies \mathbf{v} = \mathbf{w} \in \mathbf{W}.$$

Víme, že ortogonální projekce na $\mathbf{W}$ existuje. Je-li tedy $\mathbf{v} \in \mathbf{V}$, pak můžeme psát $\mathbf{v} = \mathbf{w} + (\mathbf{v} - \mathbf{w}) = (\mathbf{v} - \mathbf{w}) + \mathbf{w}$, potom $(\mathbf{v} - \mathbf{w}) \in \mathbf{W}^\perp$ je podle definice ortogonální projekce na $\mathbf{W}^\perp$. ($\mathbf{w} \in (\mathbf{W}^\perp)^\perp$.)

Použijeme 1) a větu o dimenzi součtu a průniku podprostorů. □

Definice 1.13 (Gramova matice)

Buď $\mathbf{V}$ VP s $\langle \cdot, \cdot \rangle$ nad $\mathbb{R}$ nebo $\mathbb{C}$. Buď $(\mathbf{u}_1, \ldots, \mathbf{u}_k)$ posloupnost vektorů. Pak Gramovu matici posloupnosti $(\mathbf{u}_1, \ldots, \mathbf{u}_k)$ definujeme jako:

$$(\langle \mathbf{u}_i, \mathbf{u}_j \rangle)_{k \times k}.$$

Tvrzení 1.13

Buď $\mathbf{V}$ *VP s* $\langle \cdot, \cdot \rangle$*,* $(\mathbf{u}_1, \ldots, \mathbf{u}_k)$ *posloupnost vektorů* $\mathbf{V}$*,* B *Gramova matice. Vezměme* $\mathbf{v} \in \mathbf{V}$ *a* $\mathbf{w} = a_1\mathbf{u}_1 + \ldots + a_k\mathbf{u}_k \in \mathbf{W} := \mathrm{LO}\{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$*. Pak následující je ekvivalentní:*
1) $\mathbf{w}$ *je ortogonální projekce* $\mathbf{v}$ *na* $\mathbf{W}$*.*
2) $B \cdot (a_1, \ldots, a_k)^T = (\langle \mathbf{u}_1, \mathbf{v} \rangle, \ldots, \langle \mathbf{u}_k, \mathbf{v} \rangle)$*.*

Důkaz
1) $\Leftrightarrow \mathbf{v} - \mathbf{w} \perp \mathbf{W} \Leftrightarrow \forall i \in [k] :\Leftrightarrow \mathbf{u}_i \perp \mathbf{v} - \mathbf{w} \Leftrightarrow \forall i \in [k] : \langle \mathbf{u}_i, \mathbf{v} - \mathbf{w} \rangle = 0 \Leftrightarrow \forall [k] : \langle \mathbf{u}_i, \mathbf{w} \rangle = \langle \mathbf{u}_i, \mathbf{v} \rangle \Leftrightarrow \forall i \in [k] : \langle \mathbf{u}_i, \mathbf{u}_1 \rangle \cdot a_1 + \langle \mathbf{u}_i, \mathbf{u}_k \rangle \cdot a_k = \langle \mathbf{u}_i, \mathbf{v} \rangle \Leftrightarrow$ 2). □

Důsledek
Buď A matice typu $n \times k$ nad $\mathbb{R}$ nebo $\mathbb{C}$. Buď $\mathbf{v} \in \mathbb{R}^n$ nebo $\mathbb{C}^n$ a $x \in \mathbb{C}^k$ nebo $\mathbb{R}^k$. Pak následující je ekvivalentní:
1) Ax je ortogonální projekce $\mathbf{v}$ na $\Im A$.
2) $A^* A \cdot x = A^* \cdot \mathbf{v}$.

Tvrzení 1.14 (8.80)

Buď $(\mathbf{u}_1, \ldots, \mathbf{u}_k)$ *posloupnost vektorů ve VP* $\mathbf{V}$ *s* $\langle \cdot, \cdot \rangle$ *a buď* $B \in T^{k \times k}$ *gramova matice. Pak platí:*
1) B *je regulární* $\Leftrightarrow (\mathbf{u}_1, \ldots, \mathbf{u}_k)$ *LN.*
2) B *je hermitovská (v reálném případě symetrická). 3) Je-li* $(\mathbf{u}_1, \ldots, \mathbf{u}_k)$ *LN, pak* B *je pozitivně definitní.*

Důkaz
1) aplikujeme tvrzení výše na $\mathbf{v} = \mathbf{o}$. První podmínka se přepíše na $0 = a_1\mathbf{u}_1 + \ldots + a_k\mathbf{u}_k \Leftrightarrow B \cdot (a_1, \ldots, a_k)^T = \mathbf{o} \Leftrightarrow (a_1, \ldots, a_k)^T \in \operatorname{Ker} B$. Ale jádro je $\{\mathbf{o}\} \Leftrightarrow B$ je regulární.

2) Plyne z rovnosti: $\langle \mathbf{u}_i, \mathbf{u}_j \rangle = \overline{\langle \mathbf{u}_j, \mathbf{u}_i \rangle}$.

3) Vezměme ortonormální bázi C prostoru LO $\{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$ a položme $A = ([\mathbf{u}_1]_C | \ldots | [\mathbf{u}_k]_C)$. Pak A je regulární, tj. A^*A je pozitivně definitní. □

1.4 Unitární a ortogonální matice

Definice 1.14 (Unitární a ortogonální matice)

Čtvercová matice nad $\mathbb{R}$ se nazývá ortogonální, pokud má ortonormální posloupnost sloupců vzhledem ke standardnímu skalárnímu součinu.

Čtvercová matice nad $\mathbb{C}$ se nazývá unitární, pokud má ortonormální posloupnost sloupců vzhledem ke standardnímu skalárnímu součinu.

Tvrzení 1.15

Buď Q čtvercová komplexní matice řádu n. Pak následující je ekvivalentní: 1) Q je unitární, 2) $Q^* \cdot Q = I_n$, 3) Q^* je unitární, 4) $Q \cdot Q^* = I_n$, 5) Q^T je unitární, 6) f_Q zachovává standardní skalární součin, tj. $\forall \mathbf{u}, \mathbf{v} \in \mathbb{C}^n : f(\mathbf{u}) \cdot f(\mathbf{v}) = \mathbf{u} \cdot \mathbf{v}$.

Speciálně je každá unitární matice regulární a $Q^{-1} = Q^*$.

Důkaz
1) $\Leftrightarrow$ 2), 3) $\Leftrightarrow$ 4): z definice. 2) $\implies$ 4): 2) $\implies$ Q má levou inverzi Q^* $\implies$ Q regulární a $Q^{-1} = Q^* \implies Q \cdot Q^{-1} = Q \cdot Q^* = I_n$. 4) $\implies$ 2): analogicky.

3) $\Leftrightarrow$ 5): 5) říká, že Q má ortonormální posloupnost řádků, 3) říká, že když komplexně sdružíme všechny prvky Q, pak dostaneme ortonormální posloupnost řádků. Z toho to už jednoduše dostaneme.

2) $\implies$ 6): Předpokládejme 2), uvažujme $\mathbf{u}, \mathbf{v} \in \mathbb{C}^n$. Pak $f_Q(\mathbf{u}) \cdot f_Q(\mathbf{v}) = (Q\mathbf{u})^*(Q\mathbf{v}) = \mathbf{u}^*(Q^*Q)\mathbf{v} = \mathbf{u}^*\mathbf{v}$.

6) $\implies$ 1) $Q = (f_Q(e_1)| \ldots |f_Q(e_n)) \implies (f_Q(e_1), \ldots, f_Q(e_n))$ ortonormální $\implies Q$ unitární. □

Důsledek
Součin unitárních matic stejného řádu je unitární matice.

Důkaz
$(AB)^*(AB) = B^*A^*AB = B^*B = I_n$. □

Tvrzení 1.16

Je-li A regulární komplexní matice a $Q_1R_1 = A = Q_2R_2$ jsou 2 QR rozklady, pak nutně $Q_1 = Q_2$ a $R_1 = R_2$.

Důkaz
Z regularity $Q_1R_1 = Q_2R_2 \implies Q_2^*Q_1 = Q_2^{-1}Q_1 = R_2R^{-1} =: (\mathbf{c}_1|\ldots|\mathbf{c}_n)$. Chceme ukázat, ze $\mathbf{c}_i = e_i \forall i$. To ukážeme indukcí podle i. Víme, že $R_2R_1^{-1}$ je horní trojúhelníková, tedy každé $\mathbf{c}_i$ musí mít kladný prvek na i-té pozici a zároveň všude výše musí mít nulu, aby byl kolmý ke všem předchozím (o kterých z IP víme, že jsou to jednotkové vektory). □

Definice 1.15

Buď $\mathbf{V}$ komplexní VP s $\langle\cdot,\cdot\rangle_{\mathbf{V}}$ a $\mathbf{W}$ komplexní VP s $\langle\cdot,\cdot\rangle_{\mathbf{W}}$. Pak lineární zobrazení $f : \mathbf{V} \to \mathbf{W}$ se nazývá unitární, pokud $\forall \mathbf{u}, \mathbf{v} \in \mathbf{V} : \langle f(\mathbf{v}), f(\mathbf{w})\rangle_{\mathbf{W}} = \langle \mathbf{u}, \mathbf{v}\rangle_{\mathbf{V}}$.

Tvrzení 1.17

Buď $f : \mathbf{V} \to \mathbf{W}$ lineární zobrazení, $\mathbf{V}$, $\mathbf{W}$ komplexní VP se skalárním součinem, pak následující je ekvivalentní: 1) f je unitární, 2) $\forall \mathbf{u} \in \mathbf{V} : ||f(\mathbf{u})_{\mathbf{W}} = ||\mathbf{u}||_{\mathbf{V}}$ (f zachovává normu), 3) f zobrazí každou ortonormální posloupnost $(\mathbf{u}_1, \ldots, \mathbf{u}_k)$ na ortonormální posloupnost $(f(\mathbf{u}_1, \ldots, f(\mathbf{u}_k)))$, 4) f zobrazuje jednotkové vektory na jednotkové vektory.

Speciálně: každé unitární zobrazení je prosté.

Důkaz
Ve skriptech. Dodatek plyne z 2) a f prosté $\Leftrightarrow$ $\operatorname{Ker} f = \{\mathbf{o}\}$. 1) $\implies$ 2) $\implies$ 4), 1) $\implies$ 3) $\implies$ 4) jednoduché. 4) $\implies$ 2): $\mathbf{o} \neq \mathbf{v} \in \mathbf{V}$, pak $\mathbf{v} = t\mathbf{u}$ pro $t = ||\mathbf{v}||_{\mathbf{V}}$, $\mathbf{u}$ jednokový. $||f(\mathbf{v})||_{\mathbf{W}} = t \cdot ||f(\mathbf{u})||_{\mathbf{W}} = t = ||\mathbf{v}||_{\mathbf{V}}$.

2) $\implies$ 1): Polarizační identity: $\Re\langle \mathbf{u}, \mathbf{v}\rangle, \Im\langle \mathbf{u}, \mathbf{v}\rangle = \frac{1}{2}(\ldots)$. □

Poznámka
Unitární zobrazení může zobrazovat i do prostoru větší dimenze.

1.5 Přibližné řešení SLR metodou nejmenších čtverců

Definice 1.16

Vektor $\mathbf{c} \in \mathbb{C}^n$ je přibližné řešení SLR $A\mathbf{x} = \mathbf{b}$ metodou nejmenších čtverců, pokud

$$||A\mathbf{c} - \mathbf{b}|| = \min_{\mathbf{x} \in \mathbb{C}^n} ||A\mathbf{x} - \mathbf{b}||.$$

Důsledek
$\mathbf{c}$ je ortogonální projekce $\mathbf{b}$ do $\operatorname{Im} A$.

Poznámka
Používá se například, když chybou měření soustava nemá řešení, ale my víme, že řešení mít má.

Jmenuje se podle čtverců ve výpočtu normy.

Tvrzení 1.18

$\mathbf{c}$ *je přibližné řešení* $A\mathbf{x} = \mathbf{b}$ *metodou nejmenších čtverců, právě když* $A^* A\mathbf{x} = A^*\mathbf{b}$.

2 Lineární dynamické systémy, vlastní čísla a vlastní vektory

Definice 2.1 (Vlastní čísla a vlastní vektory)

Buď $\mathbb{T}$ těleso, A čtvercová matice řádu n (tj. máme $f_a : \mathbb{T}^n \to \mathbb{T}^n$). $\lambda \in \mathbb{T}$ se nazývá vlastní číslo matice A, pokud $\exists \mathbf{v} \in T^n, \mathbf{v} \neq \mathbf{o}$ takový, že $A \cdot \mathbf{V} = \lambda \cdot \mathbf{v}$. Je-li $\lambda \in \mathbb{T}$ vlastní číslo matice A, pak $\mathbf{w} \in \mathbb{T}^n$ je vlastním vektorem příslušným k λ, pokud $A \cdot \mathbf{w} = \lambda \cdot \mathbf{w}$.

Definice 2.2 (Vlastní čísla a vlastní vektory)

Buď $\mathbb{T}$ těleso, $\mathbf{V}$ VP nad $\mathbb{T}$ a $f : \mathbf{V} \to \mathbf{V}$ lineární operátor. $\lambda \in \mathbb{T}$ se nazývá vlastní číslo operátoru f, pokud $\exists \mathbf{v} \in \mathbf{V}, \mathbf{v} \neq \mathbf{o}$ takový, že $f(\mathbf{V}) = \lambda \cdot \mathbf{v}$. Je-li $\lambda \in \mathbb{T}$ vlastní číslo operátoru f, pak $\mathbf{w} \in \mathbf{V}$ je vlastním vektorem příslušným k λ, pokud $f(\mathbf{w}) = \lambda \cdot \mathbf{w}$.

Pozorování
A má vlastní číslo $0 \Leftrightarrow \operatorname{Ker} A \neq \{\mathbf{o}\} \Leftrightarrow$ (pro čtvercové) A je singulární $\Leftrightarrow \det A = 0$.

f má vlastní číslo $0 \Leftrightarrow \operatorname{Ker} f \neq \{\mathbf{o}\}$.

Navíc množina vlastních vektorů příslušných k 0 je přesně $\operatorname{Ker} A$ ($\operatorname{Ker} f$).

Pozorování
A má vlastní číslo $\lambda \Leftrightarrow \mathrm{Ker}(A - \lambda I_n) \neq \{\mathbf{o}\} \Leftrightarrow A - \lambda I_n$ singulární $\Leftrightarrow \det(A - \lambda I_n) = 0$.

f má vlastní číslo $\lambda \Leftrightarrow \mathrm{Ker}(f - \lambda \cdot \mathrm{id}_{\mathbf{V}}) \neq \{\mathbf{o}\}$.

Navíc množina M_λ vlastních vektorů A (resp. f) příslušných k λ je v tom případě rovna $\mathrm{Ker}(A - \lambda I_n)$ (resp. $\mathrm{Ker}(f - \lambda \cdot \mathrm{id}_{\mathbf{V}})$). Speciálně $M_\lambda \leq \mathbb{T}^n$ (resp. $M_\lambda \leq \mathbf{V}$).

Definice 2.3 (Charakteristický polynom)

Buď A čtvercová matice nad $\mathbb{T}$. Potom charakteristickým polynomem A rozumíme polynom v λ:

$$p_A(\lambda) = \det(A - \lambda I_n).$$

Tvrzení 2.1

Buď $A = (a_{ij})$ matice řadu n nad $\mathbb{T}$. A $p_A(\lambda)$ charakteristický polynom. Pak

1. *$p_A(\lambda)$ je polynom stupně n.*
2. *Koeficient u λ^n je roven $(-1)^n$.*
3. *Koeficient u λ^{n-1} je roven $(-1)^{n-1} \cdot (a_{11} + \ldots + a_{nn})$ (tzv. stopa matice $\cdot(-1)^{n-1}$).*
4. *Absolutní člen je roven* $\det A$.

Definice 2.4 (Podobné matice)

Čtvercové matice X a Y jsou podobné, pokud $Y = RXR^{-1}$ pro R regulární.

Tvrzení 2.2

X, Y podobné $\implies p_X(\lambda) = p_Y(\lambda)$.

Definice 2.5 (Diagonalizovatelný operátor)

$\mathbb{T}$ těleso, $\mathbf{V}$ konečně generovaný vektorový prostor. $f : \mathbf{V} \to \mathbf{V}$ lineární operátor. Pak f je diagonalizovatelný, pokud $\exists$ báze B prostoru $\mathbf{V}$ taková, že $[f]_B^B$ je diagonální.

Poznámka (Značení)

$$\mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n) := \begin{pmatrix} \lambda_1 & & \ldots & \\ & \lambda_2 & \ldots & \\ \vdots & \vdots & \ddots & \\ & & & \lambda_n \end{pmatrix}.$$

Tvrzení 2.3

Buď $f : \mathbf{V} \to \mathbf{V}$ lineární operátor na konečně generovaném VP $\mathbf{V}$ nad $\mathbb{T}$ a buď $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ nějaká báze. Pak:

$$[f]_B^B = \operatorname{diag}(\lambda_1, \ldots, \lambda_n) \Leftrightarrow \forall i : \mathbf{v}_i \textit{ je vlastní vektor příslušný k } \lambda_i.$$

Důsledek
Za stejných předpokladů: f diagonalizovatelný $\Leftrightarrow$ $\mathbf{V}$ má bázi z vlastních vektorů f.

Definice 2.6 (Diagonalizovatelnost pro matice)

Buď $\mathbb{T}$ těleso a A čtvercová matice řádu n nad $\mathbb{T}$. Pak A je diagonalizovatelná, pokud je $f_A : \mathbb{T}^n \to T^n$ diagonalizovatelný lineární operátor.

Důsledek
A je diagonalizovatelná $\Leftrightarrow$ $\mathbb{T}^n$ má bázi z vlastních vektorů A.

Tvrzení 2.4

Buď $A \in \mathbb{T}^{n \times n}$. Pak následující tvrzení jsou ekvivalentní:

1. *A je diagonalizovatelná.*
2. *$\mathbb{T}^n$ má bázi z vlastních vektorů matice A.*
3. *A je podobná diagonální matici.*

2.1 Lineární nezávislost vlastních vektorů

Věta 2.5

Buď $\mathbb{T}$ těleso a $f : \mathbf{V} \to \mathbf{V}$ lineární operátor na VP $\mathbf{V}$ nad $\mathbb{T}$. Je-li $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ posloupnost vlastních vektorů f popořadě příslušných k vlastním číslům $(\lambda_1, \ldots, \lambda_n)$ a $\lambda_1, \ldots, \lambda_n$ jsou po dvou různá, pak je $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ LN.

Důkaz
Indukcí podle n. $n = 1$ je triviální ($\mathbf{v}_1 \neq 0$). $n > 1$: Uvažujme $a_1, \ldots, a_{n-1} \in \mathbb{T}$ taková, že $a_1\mathbf{v}_1 + \ldots + a_n\mathbf{v}_n = \mathbf{o}$. $a_1 f(\mathbf{v}_1) + \ldots + a_n f(\mathbf{v}_n) = 0 \Leftrightarrow \lambda_1 a_1 \mathbf{v}_1 + \ldots + \lambda_n a_n \mathbf{v}_n = 0$. Také můžeme původní rovnici vynásobit λ_n: $\lambda_n a_1 \mathbf{v}_1 + \ldots + \lambda_n a_n \mathbf{v}_n = 0$. Následně můžeme odečíst tyto rovnice od sebe a dostaneme $(\lambda_1 - \lambda_n) a_1 \mathbf{v}_1 + \ldots + (\lambda_{n-1} - \lambda_n) a_{n-1} \mathbf{v}_{n-1} = 0$. Ale z IP $(\lambda_1 - \lambda_n) a_1 = \ldots = (\lambda_{n-1} - \lambda_n) a_{n-1} = 0$. Ale vlastní čísla jsou po dvou různá, tedy $a_1 = \ldots = a_{n-1} = 0$. □

Důsledek
Má-li lineární operátor $f : \mathbf{V} \to \mathbf{V}$ na prostoru dimenze n n po 2 různých vlastních čísel, pak je f diagonalizovatelný.

Má-li čtvercová matice A řádu n n po 2 různých vlastních čísel, pak je A diagonalizovatelná.

2.2 Geometrická násobnost vlastních čísel

Definice 2.7 (Geometrická násobnost)

Buď A čtvercová matice řádu n nad $\mathbb{T}$, $\lambda \in \mathbb{T}$ vlastní číslo. Uvažujme podprostor

$$M_\lambda := \{\mathbf{v} \in \mathbb{T}^n | A\mathbf{v} = \lambda\mathbf{v}\} \leq \mathbb{T}^n.$$

Pak geometrickou násobností λ rozumíme $\dim M_\lambda$.

Tvrzení 2.6

Máme-li lineární operátor $f : \mathbf{V} \to \mathbf{V}$ na konečně dimenzionálním vektorovém prostoru $\mathbf{V}$ nad $\mathbb{T}$ a máme-li vlastní číslo λ operátoru f, pak geometrická násobnost $\lambda \leq$ algebraická násobnost λ.

Tvrzení 2.7 (Pomocné tvrzení o determinantech)

Buď $\mathbb{T}$ těleso, $1 \leq k < n$ a buď A matice blokově trojúhelníkovéůo tvaru, tj. $a_{ij} = 0$ pro $i > k \geq j$. Pak $\det A = (\det B) \cdot (\det D)$, kde B je prvních k sloupců a řádků, D je posledních $n - k$ sloupců a řádků.

Důkaz
Indukcí podle k: $k = 1$: Rozvoj $\det A$ podle 1. sloupce nám dá chtěnou rovnost. $k > 1$: taktéž vezmeme rozvoj podle prvního sloupce: $\det A = a_{11} \det M_{11} - a_{21} \det M_{21} + \ldots$. M_{ij} jsou ale takové matice pro $k \leftarrow k-1$. Tedy je spočítáme: $\det A = a_{11}(\det B_{11})(\det D) - a_{21}(\det B_{21})(\det D) + \ldots = (\det B) \cdot (\det D)$. □

Důkaz
Buď k geometrická násobnost vlastního čísla λ. Tj. $\dim M_\lambda = k$, kde $M_\lambda = \{\mathbf{v} \in \mathbf{V} | f(v) = \lambda\mathbf{v}\} \leq \mathbf{V}$. Vezmeme si bázi $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ prostoru M_λ a doplníme na bázi $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ prostoru $\mathbf{V}$. $A = [f]_B^B$ splňuje předpoklady předchozího tvrzení ($B = \mathrm{diag}(\lambda, \ldots, \lambda)$). Tedy $\det A - \mu \cdot I_n = (\lambda - \mu)^k \cdot \det D$. Tedy λ je minimálně k-násobným kořenem $\det A - \mu \cdot I_n$, tedy má algebraickou násobnost $\geq$ geometrické. □

Věta 2.8

Buď $f : \mathbf{V} \to \mathbf{V}$ lineární operátor na VP dimenze n nad $\mathbb{T}$. Pak následující tvrzení jsou ekvivalentní:

1. *f je diagonalizovatelný.*
2. *f má n vlastních čísel včetně algebraických násobností a současně geometrická násobnost každého vlastního čísla je rovna jeho algebraické násobnosti.*

Důkaz

1) $\implies$ 2): f je diagonalizovatelný, tedy máme bázi $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ z vlastních vektorů. Řekněme, že $\mathbf{V}_1, \ldots, \mathbf{v}_{m_1}$ jsou vlastní vektory příslušné vlastnímu číslu λ_1, ..., $\mathbf{v}_{m_1+m_2+\ldots+m_{k-1}+1}, \ldots, \mathbf{v}_{v_n}$ jsou vlastní vektory příslušné vlastnímu číslu λ_k. $\forall i \in [k]$: Geometrická násobnost i algebraická násobnost λ_i je $\geq m_i$. Na druhou stranu součet algebraických násobností je nejvýše n, tedy násobnosti λ_i jsou m_i.

2) $\implies$ 1): Buďte $\lambda_1, \ldots, \lambda_k$ po dvou různá vlastní čísla, m_i algebraická (tj. i geometrická) násobnost $\lambda_i = \dim M_{\lambda_i}$ a $n = m_1 + \ldots + m_k$. Zvolme si bázi M_{λ_i} $B_i = (\mathbf{v}^i_1, \ldots, \mathbf{v}^i_{m_i})$. Ukáže se, že $B = (\mathbf{v}^1_1, \ldots, v^k_{m_k})$ je báze $\mathbf{V}$. B má $n = \dim \mathbf{V}$ prvků, tedy stačí dokázat, že B je LN. Uvažujme $0 = a^1_1 \mathbf{v}^1_1 + \ldots + a^k_{m_k} \mathbf{v}^k_{m_k}$. Součty násobků prvků jednotlivých prostorů M_{λ_i} jsou zase v M_{λ_i}, takže jsou (až na právě ty nulové) LN, protože jsou to vlastní vektory příslušné po dvou různým vlastním číslům. Tedy musí být všechny nulové, ale v jednotlivých M_{λ_i} byla $(\mathbf{v}^i_1, \ldots, \mathbf{v}^i_{m_i})$ báze, tedy všechny koeficienty musí být nulové. $\square$