Lineární algebra pro fyziky

Zápisky z přednášek, ZS 17/18

Verze z 23. ledna 2018, obsahově kompletní

Najdete-li chybu, napište mi mail! Díky!

Dalibor Šmíd

Obsah

KAPITOLA 1

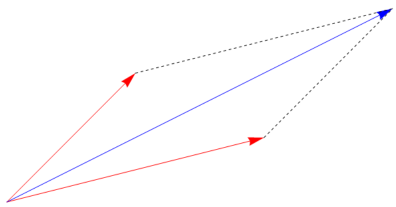
Vektory a zobrazení v $\mathbb{R}^n$

1. Vektory v $\mathbb{R}^n$

Vektor v rovině můžeme zapsat jako uspořádanou dvojici reálných čísel

$$\mathbf{x} := \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.$$

Takové vektory tradičně znázorňujeme jako úsečky s počátkem ve zvoleném počátku kartézských souřadnic v rovině a šipkou v druhém krajním bodě o souřadnicích (x_1, x_2). Sčítání vektorů odpovídá konstrukci úhlopříčky rovnoběžníka jimi svíraného:



Z obrázku je vidět, že souřadnice modré šipky jsou součtem souřadnic šipek červených, součet vektorů tedy můžeme definovat i algebraicky

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} := \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \end{pmatrix}$$

Podobně *po složkách* definujeme i násobek vektoru skalárem (číslem $r \in \mathbb{R}$):

$$r \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} := \begin{pmatrix} rx_1 \\ rx_2 \end{pmatrix}$$

I tato definice odpovídá tradiční geometrické konstrukci: škálování vektoru uvnitř jím přímky, ve které leží.

Algebraickou definici operací snadno zobecníme na vektory v prostoru (uspořádané trojice) nebo rovnou na uspořádané n-tice, tedy vektory z $\mathbb{R}^n \equiv \underbrace{\mathbb{R} \times \ldots \times \mathbb{R}}_{n}$:

$$\mathbf{x} + \mathbf{y} \equiv \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} := \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}$$

$$r\mathbf{x} \equiv r \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} := \begin{pmatrix} rx_1 \\ \vdots \\ rx_n \end{pmatrix}$$

Čísla x_i jsou *složky* vektoru $\mathbf{x}$. Vektor, jehož všechny složky jsou nulové, označujeme $\mathbf{o}$ (*nulový vektor*), vektor $-\mathbf{x} := (-1)\mathbf{x}$ je *opačný vektor*. Množině $\mathbb{R}^n$ budeme říkat *n-rozměrný prostor*.

2. Skalární součin

Skalární součin dvojice vektorů v rovině je definován předpisem

$$\mathbf{x}.\mathbf{y} := x_1y_1 + x_2y_2$$

Pomocí tohoto předpisu lze zapsat *velikost (normu)* vektoru

$$\|\mathbf{x}\| := \sqrt{\mathbf{x}.\mathbf{x}} \equiv \sqrt{x_1^2 + x_2^2}$$

TVRZENÍ 1. *Je-li* $\phi \in \langle 0, \pi\rangle$ *úhel mezi vektory* $\mathbf{x}, \mathbf{y} \in \mathbb{R}^2$, *pak*

$$\mathbf{x}.\mathbf{y} = \|\mathbf{x}\|\|\mathbf{y}\|\cos\phi$$

DŮKAZ. Označme orientovaný úhel mezi nezápornou částí první souřadné osy a polopřímkou sestávající z nezáporných násobků vektoru $\mathbf{x}$ symbolem $\alpha \in \langle 0, 2\pi)$ a podobně zaveďme $\beta \in \langle 0, 2\pi)$ pro vektor $\mathbf{y}$. Definujme $\phi' := \beta - \alpha$. Pro složky vektoru $\mathbf{x}$ platí $x_1 = \|\mathbf{x}\|\cos\alpha$, $x_2 = \|\mathbf{x}\|\sin\alpha$, podobně pro složky $\mathbf{y}$.

Dosaďte do definice skalárního součinu:

$$\mathbf{x}.\mathbf{y} = \|\mathbf{x}\|\|\mathbf{y}\|(\cos\alpha\cos\beta + \sin\alpha\sin\beta) = \|\mathbf{x}\|\|\mathbf{y}\|\cos\phi'$$

Pokud $\phi' = \beta - \alpha \in \langle 0, \pi\rangle$, pak je úhel mezi vektory ϕ roven ϕ', tedy tvrzení platí. Pokud $\phi' \in (\pi, 2\pi)$, pak je $\phi = 2\pi - \phi'$, tedy $\cos\phi = \cos\phi'$. Pokud $\phi' \in (-2\pi, 0)$, pak úhel $-\phi' \in (0, 2\pi)$ má stejný cosinus a podle předchozí úvahy buď $-\phi'$ nebo $2\pi + \phi'$ je rovno ϕ, stále se stejnou hodnotou cosinu. □

Zavedeme skalární součin a normu vektoru analogicky i na $\mathbb{R}^n$:

$$\mathbf{x}.\mathbf{y} := \sum_{i=1}^{n} x_iy_i, \quad \|\mathbf{x}\| := \sqrt{\mathbf{x}.\mathbf{x}}$$

V třírozměrném prostoru platí stejné tvrzení o souvislosti skalárního součinu a úhlu mezi vektory (viz cvičení). V obecném $\mathbb{R}^n$ nevíme, co to úhel mezi vektory je, ale můžeme jej (pro nenulové vektory $\mathbf{x}$, $\mathbf{y}$) zadefinovat jako $\phi := \arccos\frac{\mathbf{x}.\mathbf{y}}{\|\mathbf{x}\|\|\mathbf{y}\|}$. Aby tato definice byla korektní, potřebujeme vědět, že

$$-1 \leq \frac{\mathbf{x}.\mathbf{y}}{\|\mathbf{x}\|\|\mathbf{y}\|} \leq 1.$$

To je důsledkem následující věty:

VĚTA 1 (Schwarzova nerovnost). *Pro každé dva vektory* $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ *platí*

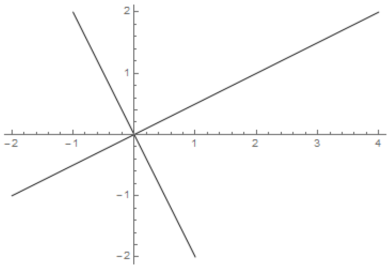
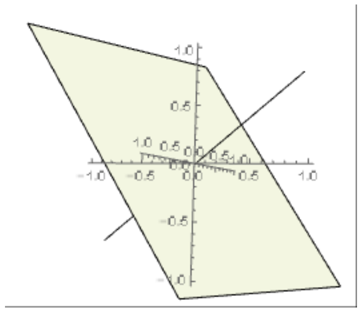
$$|\mathbf{x}.\mathbf{y}| \leq \|\mathbf{x}\|\|\mathbf{y}\|,$$

přičemž rovnost je splněna právě když je jeden z vektorů násobkem druhého.

Než větu dokážeme, je užitečné zavést některé další pojmy. Dva vektory prohlásíme za *kolmé* (značíme $\mathbf{x} \perp \mathbf{y}$), právě když $\mathbf{x}.\mathbf{y} = 0$, tedy když je jeden z nich nulový nebo když svírají úhel $\phi = \frac{\pi}{2}$. Množina

$$\mathbf{x}^{\perp} := \{\mathbf{y} \in \mathbb{R}^n | \mathbf{x}.\mathbf{y} = 0\}$$

všech vektorů $\mathbf{y}$ kolmých na vektor $\mathbf{x}$ se nazývá *ortogonální doplněk vektoru* $\mathbf{x}$. V $\mathbb{R}^2$ je to přímka, v $\mathbb{R}^3$ rovina, obě procházejí počátkem:

Množinám tvaru $\{\mathbf{y} \in \mathbb{R}^n | \mathbf{x}.\mathbf{y} = c\}$ říkáme obecně *nadroviny*. Nadrovina obsahuje vektor $\mathbf{o}$, právě když $c = 0$.

3. Vektorový součin

Vedle skalárního součinu známe ze středoškolské matematiky ještě součin vektorový. Pro $\mathbf{x}, \mathbf{y} \in \mathbb{R}^3$ je $\mathbf{v} \times \mathbf{y}$ vektor definovaný po složkách jako

$$(\mathbf{x} \times \mathbf{y})_k = \sum_{i=1}^{3} \sum_{j=1}^{3} \varepsilon_{ijk} x_i y_j,$$

kde $\varepsilon_{123} = \varepsilon_{231} = \varepsilon_{312} = 1$, $\varepsilon_{213} = \varepsilon_{321} = \varepsilon_{132} = -1$ a $\varepsilon_{ijk} = 0$, jsou-li dva indexy stejné. Díky tomu z devíti členů dvojité sumy přežijí jen dva, tedy

$$\begin{aligned} \mathbf{x} \times \mathbf{y} &= (\varepsilon_{231} x_2 y_3 + \varepsilon_{321} x_3 y_2, \varepsilon_{132} x_1 y_3 + \varepsilon_{312} x_3 y_1, \varepsilon_{123} x_1 y_2 + \varepsilon_{213} x_2 y_1) \\ &= (x_2 y_3 - x_3 y_2, -x_1 y_3 + x_3 y_1, x_1 y_2 - x_2 y_1) \end{aligned}$$

TVRZENÍ 2. *Nechť* $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{R}^3$, $r, s \in \mathbb{R}$, $\mathbf{x}$ *a* $\mathbf{y}$ *svírají úhel* ϕ. *Pak*

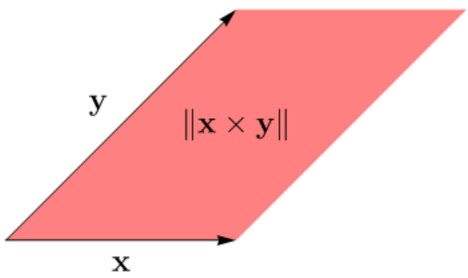
(1) $\mathbf{x} \times \mathbf{y} = -\mathbf{y} \times \mathbf{x}$, *speciálně* $\mathbf{x} \times \mathbf{x} = 0$
(2) $\mathbf{x} \times (r\mathbf{y} + s\mathbf{z}) = r(\mathbf{x} \times \mathbf{y}) + s(\mathbf{x} \times \mathbf{z})$
(3) $\|\mathbf{x} \times \mathbf{y}\| = \|\mathbf{x}\| \|\mathbf{y}\| |\sin\phi|$
(4) $|(\mathbf{x} \times \mathbf{y}).\mathbf{z}|$ *je objem rovnoběžnostěnu definovaného vektory* $\mathbf{x}, \mathbf{y}, \mathbf{z}$, *speciálně* 0 *pro* $z = r\mathbf{x} + s\mathbf{y}$.

Důkaz nyní nebudeme provádět, návod k němu je ve cvičení 1. Z druhé části posledního bodu plyne, že $\mathbf{x} \times \mathbf{y}$ je kolmý na rovinu definovanou $\mathbf{x}$ a $\mathbf{y}$.

Oproti skalárnímu součinu se nenabízí žádné přímočaré zobecnění vektorového součinu do libovolné dimenze n. V $\mathbb{R}^2$ lze vektoru $\mathbf{x}$ přiřadit vektor

$$\tilde{\mathbf{x}} := \begin{pmatrix} \mathbf{x} \\ 0 \end{pmatrix} \in \mathbb{R}^3$$

a definovat $\mathbf{x} \times \mathbf{y} := (\tilde{\mathbf{x}} \times \tilde{\mathbf{y}})_3 \in \mathbb{R}$. Pak je $\|\mathbf{x} \times \mathbf{y}\|$ obsah rovnoběžníka definovaného $\mathbf{x}$ a $\mathbf{y}$:



Plyne to ze třetí části tvrzení 2, protože $\|\mathbf{y}\| |\sin\phi|$ je výška rovnoběžníka.

POZNÁMKA 1. Při zobecnění do dimenze $n > 3$ chceme, aby vektorový součin dál počítal objemy rovnoběžnostěnů, což lze splnit definicí

$$(\mathbf{x}_1 \times \mathbf{x}_2 \times \ldots \times \mathbf{x}_{n-1})_{k_n} := \sum_{k_1=1}^{n} \sum_{k_2=1}^{n} \cdots \sum_{k_{n-1}=1}^{n} \varepsilon_{k_1 k_2 \ldots k_n} x_{1k_1} x_{2k_2} \ldots x_{n-1,k_{n-1}},$$

kde symbol ε je opět definován tak, aby měnil znaménko při výměně libovolné dvojice indexů a aby $\varepsilon_{12\ldots n} = 1$. Zobecněný vektorový součin tedy již není funkce dvou, ale $n-1$ vektorových argumentů, výsledkem je opět vektor. Jsou ale splněny analogie vlastností $1, 2$ a 4 z tvrzení 2. Například objem rovnoběžnostěnu určeného vektory $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d} \in \mathbb{R}^4$ je roven

$$|(\mathbf{a} \times \mathbf{b} \times \mathbf{c}).\mathbf{d}| = \left| \sum_{i=1}^{4} \sum_{j=1}^{4} \sum_{k=1}^{4} \sum_{l=1}^{4} \varepsilon_{ijkl} a_i b_j c_k d_l \right|$$

Cvičení 1

Dokážeme tvrzení 2:

(1) Dokažte body 1 a 2 přímým dosazením z definice.

(2) Definujme veličinu

$$V(\mathbf{x}, \mathbf{y}, \mathbf{z}) := \sum_{i=1}^{3} \sum_{j=1}^{3} \sum_{k=1}^{3} \varepsilon_{ijk} x_i y_j z_k$$

S pomocí bodu 2 ukažte, že $V(\mathbf{x}, \mathbf{y}, \mathbf{z}) = V(\mathbf{x} + s\mathbf{y}, \mathbf{y}, \mathbf{z})$. Rozmyslete si, že rovnoběžnostěn definovaný vektory $\mathbf{x}, \mathbf{y}, \mathbf{z}$ má stejný objem jako rovnoběžnostěn definovaný vektory $\mathbf{x} + s\mathbf{y}, \mathbf{y}, \mathbf{z}$.

(3) Buď $x_1 = y_1 = z_1 = 0$, nebo je alespoň jedno z těchto čísel nenulové. Ukažte, že

$$V(\mathbf{x}, \mathbf{y}, \mathbf{z}) = -V(\mathbf{y}, \mathbf{x}, \mathbf{z}) = V(\mathbf{z}, \mathbf{x}, \mathbf{y})$$

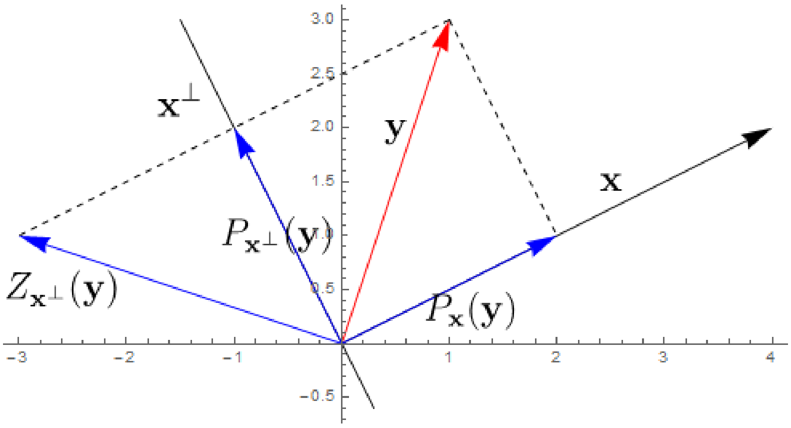
a odvoďte z toho, že v druhém případě bez újmy na obecnosti $x_1 \neq 0$. Pak lze pomocí předchozího bodu převést vektory $\mathbf{x}, \mathbf{y}, \mathbf{z}$ na takové, že $y_1' = z_1' = 0$, aniž by se změnila hodnota V nebo objem rovnoběžnostěnu. Rozeberte případ $x_1 = y_1 = z_1 = 0$.

(4) Ukažte, že vektory lze dále převést na trojici $\mathbf{x}, \mathbf{y}', \mathbf{z}''$, kde $z_1'' = z_2'' = 0$ a V ani objem rovnoběžnostěnu se nezměnily. Dále ukažte, že $V(\mathbf{x}, \mathbf{y}', \mathbf{z}'') = x_1 y_2' z_3''$ a že $|x_1 y_2' z_3''|$ je právě objem rovnoběžnostěnu definovaného vektory $\mathbf{x}, \mathbf{y}', \mathbf{z}''$. Tím je dokázán bod 4.

(5) Z bodu 4 ukažte, že $\|\mathbf{x} \times \mathbf{y}\|$ je obsah podstavy rovnoběžnostěnu definované vektory $\mathbf{x}, \mathbf{y}$. Odtud odvoďte bod 3.

4. Ortogonální projekce a zrcadlení

Pomocí skalárního součinu můžeme vyjádřit kolmý průmět (*ortogonální projekci*) vektoru $\mathbf{y}$ do směru jiného (nenulového) vektoru $\mathbf{x}$, kolmý průmět do směru jeho ortogonálního doplňku a vektor zrcadlený podle nadroviny $\mathbf{x}^{\perp}$.



$$P_{\mathbf{x}}(\mathbf{y}) = \|\mathbf{y}\| \cos\phi \frac{\mathbf{x}}{\|\mathbf{x}\|} = \frac{\mathbf{x}.\mathbf{y}}{\|\mathbf{x}\|^2}\mathbf{x}$$
$$P_{\mathbf{x}^\perp}(\mathbf{y}) = \mathbf{y} - P_{\mathbf{x}}(\mathbf{y}) = \mathbf{y} - \frac{\mathbf{x}.\mathbf{y}}{\|\mathbf{x}\|^2}\mathbf{x}$$
$$Z_{\mathbf{x}^\perp}(\mathbf{y}) = \mathbf{y} - 2P_{\mathbf{x}}(\mathbf{y}) = \mathbf{y} - 2\frac{\mathbf{x}.\mathbf{y}}{\|\mathbf{x}\|^2}\mathbf{x}$$

Stejné vzorce lze použít jako definice projekce a zrcadlení i v obecné dimenzi n. Pak platí

TVRZENÍ 3. *Nechť* $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, $\mathbf{x} \neq \mathbf{o}$. *Pak*

(1) $P_{\mathbf{x}}(\mathbf{x}) = \mathbf{x}$
(2) $P_{\mathbf{x}}(\mathbf{y}) = 0$ *právě když* $\mathbf{x} \perp \mathbf{y}$
(3) $P_{\mathbf{x}^\perp}(\mathbf{y}) \perp \mathbf{x}$
(4) $\forall r, s \in \mathbb{R}, \forall \mathbf{y}, \mathbf{z} \in \mathbb{R}^n : P_{\mathbf{x}}(r\mathbf{y} + s\mathbf{z}) = rP_{\mathbf{x}}(\mathbf{y}) + sP_{\mathbf{x}}(\mathbf{z})$
(5) *Vektor* $\mathbf{y}$ *lze jednoznačně zapsat jako* $\mathbf{y}_\parallel + \mathbf{y}_\perp$, *kde* $\mathbf{y}_\parallel$ *je násobkem vektoru* $\mathbf{x}$ *a* $\mathbf{y}_\perp$ *je kolmý na* $\mathbf{x}$. *Navíc pak* $\mathbf{y}_\parallel = P_{\mathbf{x}}(\mathbf{y})$ *a* $\mathbf{y}_\perp = P_{\mathbf{x}^\perp}(\mathbf{y})$.

DŮKAZ. První čtyři tvrzení plynou přímo z definic skalárního součinu, kolmosti a normy. Například třetí plyne z

$$\mathbf{x}.(\mathbf{y} - P_{\mathbf{x}}(\mathbf{y})) = \mathbf{x}.\mathbf{y} - \frac{\mathbf{x}.\mathbf{y}}{\|\mathbf{x}\|^2}\mathbf{x}.\mathbf{x} = 0$$

Z definic $P_{\mathbf{x}}$ a $P_{\mathbf{x}^\perp}$ a třetí části tvrzení plyne, že každý vektor $\mathbf{y}$ se dá zapsat jako

$$\mathbf{y} = P_{\mathbf{x}}(\mathbf{y}) + P_{\mathbf{x}^\perp}(\mathbf{y}) \equiv r\mathbf{x} + \mathbf{z},$$

kde r je nějaký skalár a $\mathbf{z} \in \mathbf{x}^\perp$. Kdyby bylo možné zapsat vektor $\mathbf{y}$ jako $s\mathbf{x} + \mathbf{z}'$, kde $\mathbf{z}' \in \mathbf{x}^\perp$, pak by $(r - s)\mathbf{x} = \mathbf{z}' - \mathbf{z}$. Vektor $\mathbf{z}' - \mathbf{z}$ je kolmý na $\mathbf{x}$, tedy $(r - s)\mathbf{x}.\mathbf{x} = 0$. Protože $\mathbf{x} \neq \mathbf{o}$, musí být $r = s$ a tedy i $\mathbf{z} = \mathbf{z}'$. Rozklad vektoru $\mathbf{y}$ na paralelní a kolmou část je tedy jednoznačný. □

$P_{\mathbf{x}}$ lze chápat jako *zobrazení*, tedy jakousi „mašinku“, do které se vloží libovolný prvek $\mathbf{y} \in \mathbb{R}^n$ a ona mu přiřadí jednoznačně určený prvek $P_{\mathbf{x}}(\mathbf{y}) \in \mathbb{R}^n$. Čtvrtá část tvrzení znamená, že toto zobrazení zachovává součty a násobení skalárem, geometricky tedy převede každý rovnoběžník opět na rovnoběžník. O takovém zobrazení říkáme, že je *lineární*. Snadno se lze přesvědčit, že i $P_{\mathbf{x}^\perp}, Z_{\mathbf{x}^\perp} : \mathbb{R}^n \to \mathbb{R}^n$ jsou lineární zobrazení, realizující projekci, resp. zrcadlení podle nadroviny $\mathbf{x}^\perp$.

Nyní můžeme konečně dokázat Schwarzovu nerovnost:

DŮKAZ. Předpokládejme, že alespoň jeden z vektorů je nenulový, jinak je tvrzení triviální. Nechť je to $\mathbf{x}$. Pak lze díky pátému bodu tvrzení 3 zapsat $\mathbf{y}$ jako součet $\mathbf{y}_{\parallel} + \mathbf{y}_{\perp}$. Protože $\mathbf{y}_{\parallel} \perp \mathbf{y}_{\perp}$, platí

$$\|\mathbf{y}\|^2 = (\mathbf{y}_{\parallel} + \mathbf{y}_{\perp}).(\mathbf{y}_{\parallel} + \mathbf{y}_{\perp}) = \|\mathbf{y}_{\parallel}\|^2 + \|\mathbf{y}_{\perp}\|^2 \geq \|\mathbf{y}_{\parallel}\|^2$$

Z pátého bodu tvrzení 3 rovněž víme, že $\mathbf{y}_{\parallel} = P_{\mathbf{x}}(\mathbf{y})$. Dosazením z definice ortogonální projekce a algebraickou úpravou dostaneme, že

$$\|\mathbf{y}\|^2\|\mathbf{x}\|^2 \geq (\mathbf{x}.\mathbf{y})^2$$

Protože normy jsou nezáporné, stačí po odmocnění přidat absolutní hodnotu jen na pravou stranu nerovnosti. Rovnost nastává právě když $\|\mathbf{y}_{\perp}\|^2 = 0$, tedy právě když jsou všechny složky $\mathbf{y}_{\perp}$ nulové. To nastane právě když $\mathbf{y} = \mathbf{y}_{\parallel}$, tedy je-li $\mathbf{y}$ násobkem $\mathbf{x}$. □

5. Rotace v $\mathbb{R}^2$ a $\mathbb{R}^3$, dilatace a posunutí

Otočení (*rotaci*) vektoru $\mathbf{y} \in \mathbb{R}^2$ okolo počátku o úhel ϕ proti směru hodinových ručiček lze zapsat jako zobrazení

$$\mathbf{y} := \begin{pmatrix} \|y\|\cos(\alpha) \\ \|y\|\sin(\alpha) \end{pmatrix} \mapsto R_\phi(\mathbf{y}) := \begin{pmatrix} \|y\|\cos(\alpha+\phi) \\ \|y\|\sin(\alpha+\phi) \end{pmatrix}$$

Po aplikaci součtových vzorců máme vyjádření ve složkách:

$$R_\phi(\mathbf{y}) := \begin{pmatrix} y_1\cos\phi - y_2\sin\phi \\ y_1\sin\phi + y_2\cos\phi \end{pmatrix} = \cos\phi \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} + \sin\phi \begin{pmatrix} -y_2 \\ y_1 \end{pmatrix}$$

Několik pozorování:

- R_ϕ je lineární zobrazení.
- $R_0(\mathbf{y}) = \mathbf{y}$, tedy $R_0 = \mathrm{Id}$ (*identita*).
- Složení dvou rotací $R_\phi \circ R_\psi$ je rotace $R_{\phi+\psi}$. Na pořadí složení zde nezáleží, říkáme, že R_ϕ a R_ψ *komutují*.
- $R_{-\phi} \circ R_\phi = R_\phi \circ R_{-\phi} = R_0 = \mathrm{Id}$, tedy zobrazení $R_{-\phi}$ je *inverzní* k R_ϕ, $R_{-\phi} = (R_\phi)^{-1}$.

Rotaci vektoru $\mathbf{y} \in \mathbb{R}^3$ okolo osy dané vektorem $\mathbf{v}$ ($\|\mathbf{v}\| = 1$) můžeme zapsat například pomocí Rodriguesovy formule:

$$R_{\mathbf{v},\phi}(\mathbf{y}) = \cos\phi\ \mathbf{y} + (1-\cos\phi)(\mathbf{v}.\mathbf{y})\mathbf{v} + \sin\phi\ \mathbf{v} \times \mathbf{y}.$$

Návod k jejímu odvození naleznete ve cvičeních.

Rotace v $\mathbb{R}^3$ komutují, pokud mají společnou osu, jindy komutovat nemusí. Vektory

$$\mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \mathbf{e}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \mathbf{e}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

a jejich přímočará zobecnění do $\mathbb{R}^n$ se nazývají *prvky kanonické báze*. Nekomutativita rotací se projeví třeba na příkladu

$$R_{\mathbf{e}_2,\frac{\pi}{2}} \circ R_{\mathbf{e}_3,\frac{\pi}{2}}(\mathbf{e}_3) = R_{\mathbf{e}_2,\frac{\pi}{2}}(\mathbf{e}_3) = \mathbf{e}_1$$
$$R_{\mathbf{e}_3,\frac{\pi}{2}} \circ R_{\mathbf{e}_2,\frac{\pi}{2}}(\mathbf{e}_3) = R_{\mathbf{e}_3,\frac{\pi}{2}}(\mathbf{e}_1) = \mathbf{e}_2$$

POZNÁMKA 2. Rotaci v $\mathbb{R}^n$ je možné definovat podobně jako v $\mathbb{R}^3$, pouze „osa" již nebude přímka, ale bude mít dimenzi $n-2$. Příkladem rotace v $\mathbb{R}^4$ fixující rovinu vektorů $\mathbf{e_1}$ a $\mathbf{e_4}$ (značíme $\langle \mathbf{e}_1, \mathbf{e}_4 \rangle$) je

$$R_{\langle \mathbf{e}_1,\mathbf{e}_4\rangle,\phi}(\mathbf{y}) := \begin{pmatrix} y_1 \\ y_2\cos\phi - y_3\sin\phi \\ y_2\sin\phi + y_3\cos\phi \\ y_4 \end{pmatrix}$$

Dalším příkladem lineárního zobrazení z $\mathbb{R}^n$ do $\mathbb{R}^n$ je roztažení(*dilatace*) faktorem $\lambda \in \mathbb{R}$:

$$D_\lambda(\mathbf{y}) := \lambda \mathbf{y}$$

Naopak posunutí (*translace*) o nenulový vektor $\mathbf{b} \in \mathbb{R}^n$

$$T_{\mathbf{b}}(\mathbf{y}) := \mathbf{y} + \mathbf{b}$$

lineárním zobrazením není. Lineární zobrazení F totiž musí splňovat $F(\mathbf{o}) = F(0.\mathbf{x} + 0.\mathbf{y}) = 0F(\mathbf{x}) + 0F(\mathbf{y}) = \mathbf{o}$, pro translaci ale $T_{\mathbf{b}}(\mathbf{o}) = \mathbf{b}$.

6. Matice lineárního zobrazení

Jak tedy poznáme, že je nějaké zobrazení $F : \mathbb{R}^n \to \mathbb{R}^n$ lineární?

Každý vektor $\mathbf{x} \in \mathbb{R}^n$ lze zapsat jako

$$\mathbf{x} = x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + \ldots + x_n\mathbf{e}_n,$$

neboli jako *lineární kombinaci* prvků kanonické báze. Z linearity zobrazení F plyne, že

$$\begin{aligned} F(\mathbf{x}) &= F(x_1\mathbf{e}_1 + \ldots + x_n\mathbf{e}_n) = x_1F(\mathbf{e}_1) + \ldots + x_nF(\mathbf{e}_n) \\ &= x_1\mathbf{a}_1 + \ldots + x_n\mathbf{a}_n, \end{aligned}$$

kde jsme jako $\mathbf{a}_j \in \mathbb{R}^n$ označili obraz $F(\mathbf{e}_j)$ vektoru $\mathbf{e}_j$. Označíme-li i-tou složku vektoru $\mathbf{a}_j$ jako a_{ij}, je to dohromady n^2 reálných čísel, která společně zobrazení F jednoznačně určují. Tato čísla souhrnně označujeme jako *matici lineárního zobrazení* a značíme $A \equiv (a_{ij})$.

Zobrazení určené maticí A označujeme symbolem F_A. Pak tedy můžeme zavést zápis lineárního zobrazení pomocí jeho *matice*:

$$\begin{aligned} F_A(\mathbf{x}) &:= x_1 \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n1} \end{pmatrix} + x_2 \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{n2} \end{pmatrix} + \ldots + x_n \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{nn} \end{pmatrix} \\ &=: \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \equiv A\mathbf{x} \end{aligned}$$

Druhou rovností jsme jednak zavedli standardní zápis matice jako tabulky čísel, v níž první index čísluje řádky a druhý sloupce. Zároveň jsme také zadefinovali *součin matice a vektoru.*

Součin matice A a vektoru $\mathbf{x}$ je vlastně lineární kombinací sloupců matice A s koeficienty rovnými složkám vektoru $\mathbf{x}$. Užívá se proto také *sloupcový zápis matice* $A = (\mathbf{a}_1|\mathbf{a}_2|\ldots|\mathbf{a}_n)$. Zobrazení s maticí

$$E := (\mathbf{e}_1|\ldots|\mathbf{e}_n) \equiv \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix}$$

přiřazuje každému vektoru $\mathbf{x}$ vektor

$$F_E(\mathbf{x}) = E\mathbf{x} = x_1\mathbf{e}_1 + \ldots + x_n\mathbf{e}_n = \mathbf{x},$$

je to tedy identita $F_E = \mathrm{Id}$. Matici E se říká *jednotková matice.*

Označíme-li symbolem

$$\tilde{\mathbf{a}}_i := \begin{pmatrix} a_{i1} \\ a_{i2} \\ \vdots \\ a_{in} \end{pmatrix}$$

i-tý řádek matice A, zapsaný ovšem jako sloupcový vektor, pak i-tá složka obrazu vektoru $\mathbf{x}$ v zobrazení F_A je

$$F_A(\mathbf{x})_i \equiv (A\mathbf{x})_i = a_{i1}x_1 + a_{i2}x_2 + \dots a_{in}x_n \equiv \sum_{j=1}^{n} a_{ij}x_j,$$

což lze interpretovat jako skalární součin vektorů $\tilde{\mathbf{a}}_i$ a $\mathbf{x}$. Pokud tedy $F_A(\mathbf{x})_i = 0$, je vektor $\mathbf{x}$ kolmý na $\tilde{\mathbf{a}}_i$. Podobně pokud $F_A(\mathbf{x})_i = c$, leží $\mathbf{x}$ v nadrovině s rovnicí $\tilde{\mathbf{a}}_i.\mathbf{x} = c$.

KAPITOLA 2

Matice

V této kapitole se podíváme na matice jako na samostatné objekty a zavedeme na nich operace, jejichž vlastnosti vyplývají z vlastností zobrazení. Začneme ale tím, že se podíváme, jak hledání vzoru určitého vektoru v daném lineárním zobrazení vede na soustavu lineárních rovnic.

1. Lineární zobrazení a soustavy rovnic

PŘÍKLAD 1. Uvažujme matici a vektor

$$A = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}, \mathbf{b} = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$$

Zajímá nás, na jaký vektor zobrazí F_A vektor $\mathbf{b}$ a které vektory se naopak zobrazí na něj. V prvním případě snadno spočteme, že

$$F_A(\mathbf{b}) = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} -1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1.(-1) + 2.1 \\ 1.(-1) + 3.1 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

V druhém hledáme obecný tvar vektoru $\mathbf{x}$, pro který

$$F_A(\mathbf{x}) \equiv \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \equiv \begin{pmatrix} x_1 + 2x_2 \\ x_1 + 3x_2 \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \end{pmatrix},$$

což je vlastně soustava dvou rovnic pro dvě neznámé x_1 a x_2. Každá rovnice je rovnicí přímky v $\mathbb{R}^2$, jsou různoběžné, jediným řešením (a tedy i jediným vzorem vektoru $\mathbf{b}$ v zobrazení F_A) je jejich průsečík, vektor

$$\mathbf{x} = \begin{pmatrix} -5 \\ 2 \end{pmatrix}$$

Co kdybychom hledali průsečnici dvou rovin v $\mathbb{R}^3$? Soustavu

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 &= b_1 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 &= b_2 \end{aligned}$$

lze opět interpretovat jako rovnost vektorů

$$x_1 \begin{pmatrix} a_{11} \\ a_{21} \end{pmatrix} + x_2 \begin{pmatrix} a_{12} \\ a_{22} \end{pmatrix} + x_3 \begin{pmatrix} a_{13} \\ a_{23} \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$$

Lineární kombinace na levé straně odpovídá definici součinu matice a vektoru, až na to, že matice A nemá stejný počet řádků jako sloupců. Pojďme tedy tuto definici rozšířit.

DEFINICE 1. Nechť $m, n \in \mathbb{N}$ a $\mathbf{a}_1, \ldots, \mathbf{a}_n$ jsou vektory z $\mathbb{R}^m$, $\mathbf{x} \in \mathbb{R}^n$. Pak definujme matici $A = (\mathbf{a}_1 | \ldots | \mathbf{a}_n)$ a její součin s vektorem $\mathbf{x}$

$$A\mathbf{x} := x_1\mathbf{a}_1 + \ldots + x_n\mathbf{a}_n \in \mathbb{R}^m$$

Matice s m řádky a n sloupci se označuje jako matice $m \times n$. Pokud $m = n$, říká se jí *čtvercová*. Pokud $\mathbf{a}$ je nějaký vektor

$$\mathbf{a} := \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in \mathbb{R}^n,$$

pak rovnici nadroviny $\mathbf{a}.\mathbf{x} = c$ můžeme zapsat pomocí matice $1 \times n$ jako

$$\begin{pmatrix} a_1 & \dots & a_n \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = c$$

Matice vzniklá z matice A výměnou řádků za sloupce se nazývá *matice transponovaná k matici* A:

$$A^T \equiv \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}^T := \begin{pmatrix} a_{11} & \dots & a_{m1} \\ a_{12} & \ddots & a_{m2} \\ \vdots & & \vdots \\ a_{1n} & \dots & a_{mn} \end{pmatrix}$$

S pomocí operace transponování můžeme rovnici nadroviny napsat také jako $\mathbf{a}^T\mathbf{x} = c$, přičemž sloupcový vektor $\mathbf{a}$ interpretujeme jako matici $n \times 1$.

Příklad 2. Vraťme se k hledání průsečnice rovin a vezměme nějakou konkrétní matici A a konkrétní *vektor pravých stran* $\mathbf{b}$:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 4 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Řešíme tedy *soustavu lineárních rovnic* (*SLR*)

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

Nahradíme-li druhou rovnici soustavy rozdílem druhé a první rovnice, množina řešení se nezmění (cvičení 2). Novou soustavu

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

vyřešíme položením $x_3 := t \in \mathbb{R}$ a dosazením do druhé a poté do první rovnice:

$$\mathbf{x} \equiv \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1-t \\ -t \\ t \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + t \begin{pmatrix} -1 \\ -1 \\ 1 \end{pmatrix}.$$

To je v souladu s očekáváním přímka procházející bodem $(1, 0, 0)^T$ a mající směrový vektor $(-1, -1, 1)^T$.

Příklad 3. Podobně můžeme najít i *parametrické vyjádření* roviny $x_1 + 2x_2 + 3x_3 = 1$. Položíme neznámé $x_2 := t$, $x_3 := s$ rovny dvěma libovolným parametrům a dopočteme $x_1 = 1 - 2t - 3s$. Vektorově lze množinu řešení zapsat jako

$$\left\{ \mathbf{x} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + t \begin{pmatrix} -2 \\ 1 \\ 0 \end{pmatrix} + s \begin{pmatrix} -3 \\ 0 \\ 1 \end{pmatrix} \middle| t, s \in \mathbb{R} \right\},$$

tedy jako množinu „bod plus lineární kombinace směrových vektorů". Takový tvar má množina řešení každé SLR (cvičení 3).

Cvičení 2

Nechť $(x_1,\dots,x_n)^T$ je n-tice čísel splňujících SLR1

$$\begin{array}{ccccccccc} a_1x_1 & + & a_2x_2 & + & \dots & + & a_nx_n & = & c \\ b_1x_1 & + & b_2x_2 & + & \dots & + & b_nx_n & = & d \end{array}$$

Vyvoďte z toho, že $(x_1,\dots,x_n)^T$ splňuje také SLR2

$$\begin{array}{ccccccccc} a_1x_1 & + & a_2x_2 & + & \dots & + & a_nx_n & = & c \\ (b_1+ra_1)x_1 & + & (b_2+ra_2)x_2 & + & \dots & + & (b_n+ra_n)x_n & = & d+rc \end{array}$$

pro libovolné $r\in\mathbb{R}$. Obdobně dokažte, že každé řešení SLR2 je i řešením SLR1. Celkově tedy přičtení násobku první rovnice do druhé rovnice nemění množinu řešení.

Cvičení 3

Nechť $\mathbf{x}_P=(x_{P1},\dots,x_{Pn})^T$ je řešením SLR1

$$\begin{array}{ccccccccc} a_1x_1 & + & a_2x_2 & + & \dots & + & a_nx_n & = & c \\ b_1x_1 & + & b_2x_2 & + & \dots & + & b_nx_n & = & d \end{array}$$

a $\mathbf{x}_H=(x_{H1},\dots,x_{Hn})^T,\mathbf{y}=(x_{H1},\dots,x_{Hn})^T$ je řešením SLR2

$$\begin{array}{ccccccccc} a_1x_1 & + & a_2x_2 & + & \dots & + & a_nx_n & = & 0 \\ b_1x_1 & + & b_2x_2 & + & \dots & + & b_nx_n & = & 0\text{'} \end{array}$$

která vznikne ze SLR1 nahrazením pravých stran nulami. Ukažte, že $\mathbf{x}_P+\mathbf{x}_H$ je řešením SLR1 a že libovolná lineární kombinace $r\mathbf{x}_H+s\mathbf{y}_H$ je řešením SLR2. K důkazu tvrzení, že množina řešení každé SLR je „bod plus lineární kombinace směrových vektorů“ se potřebujeme ještě seznámit s pojmem báze, viz definice 16.

2. Skládání zobrazení a součin matic

Uvažujme dvě zobrazení $F_A:\mathbb{R}^n\to\mathbb{R}^m$ a $F_B:\mathbb{R}^m\to\mathbb{R}^p$. Složené zobrazení $F_B\circ F_A:\mathbb{R}^n\to\mathbb{R}^p$ je opět lineární (ověřte sami) a jeho matici můžeme určit tak, že spočítáme obrazy vektorů $\mathbf{e}_1,\dots,\mathbf{e}_n\in\mathbb{R}^n$:

$$(F_B\circ F_A)(\mathbf{e}_i)=F_B(A\mathbf{e}_i)=F_B(\mathbf{a}_i)=B\mathbf{a}_i,$$

tedy pro obecný vektor $\mathbf{x}\in\mathbb{R}^n$

$$(F_B\circ F_A)(\mathbf{x})=(B\mathbf{a}_1|\dots|B\mathbf{a}_n)\mathbf{x}$$

To nám dává návod, jak definovat *součin matic*:

Definice 2. Nechť A je matice $m\times n$ a B je matice $p\times m$. Pak definujme

$$BA:=(B\mathbf{a}_1|\dots|B\mathbf{a}_n)$$

Z definice automaticky plyne, že $F_B\circ F_A=F_{BA}$. BA je matice $p\times n$, tedy má stejně sloupců jako A a řádků jako B.

Výhoda této definice je, že je konzistentní s dříve definovaným součinem matice a vektoru, chápeme-li vektor jako matici o jednom sloupci. Element matice BA na pozici ij je

$$b_{i1}a_{1j}+b_{i2}a_{2j}+\dots+b_{im}a_{mj}\equiv\sum_{k=1}^{m}b_{ik}a_{kj},$$

což je vlastně skalární součin $\tilde{\mathbf{b}}_i^T.\mathbf{a}_j$ i-tého řádku matice B a j-tého sloupce matice A. Odtud je jednoduše vidět, že

$$E_mA=AE_n=A,$$

kde E_m, E_n značí jednotkovou matici $m\times m$, resp. $n\times n$.

Označme množinu všech $m\times n$ matic symbolem $\mathbb{R}^{m\times n}$.

Tvrzení 4. *Nechť* $m, n, p, q \in \mathbb{N}$, $A \in \mathbb{R}^{m\times n}$, $B \in \mathbb{R}^{n\times p}$, $C \in \mathbb{R}^{p\times q}$. *Pak*

$$(AB)C = A(BC),$$

tedy součin matic je asociativní.

Důkaz. Pro libovolný $\mathbf{x} \in \mathbb{R}^q$ platí

$$\begin{aligned}((AB)C)\mathbf{x} = (F_{AB} \circ F_C)(\mathbf{x}) = F_{AB}(F_C(\mathbf{x})) = \\ = F_A(F_B(F_C(\mathbf{x}))) = (F_A \circ F_{BC})(\mathbf{x}) = (A(BC))\mathbf{x},\end{aligned}$$

Pokud za $\mathbf{x}$ dosadíme prvek $\mathbf{e}_i$, získáme rovnost mezi i-tým sloupcem matice $(AB)C$ a matice $A(BC)$. Obě matice jsou typu $m \times q$, tedy se musejí rovnat. □

Definice 3. Nechť $A, B \in \mathbb{R}^{m\times n}$. Pak *součet matic* $A + B$ definujeme jako

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{m1} & \dots & b_{mn} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & \dots & a_{1n}+b_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1}+b_{m1} & \dots & a_{mn}+b_{mn} \end{pmatrix}$$

a násobek matice skalárem $r \in \mathbb{R}$ jako

$$r\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} = \begin{pmatrix} ra_{11} & \dots & ra_{1n} \\ \vdots & \ddots & \vdots \\ ra_{m1} & \dots & ra_{mn} \end{pmatrix}$$

Je to přirozená definice, protože je v případě matic s jediným sloupcem v souladu s definicí součtu vektorů a jejich násobení skalárem. Pojmem *nulová matice* označujeme matici, jejíž všechny elementy jsou 0, obvykle ji stejným symbolem i značíme.

Další důležitou vlastností součinu matic je jeho *distributivita*.

Tvrzení 5. *Nechť* $m, n, p \in \mathbb{N}$, $A, B \in \mathbb{R}^{m\times n}$, $C, D \in \mathbb{R}^{n\times p}$. *Pak*

$$\begin{aligned}(A + B)C &= AC + BC \\ A(C + D) &= AC + AD,\end{aligned}$$

Důkaz. Nejprve si uvědomme, že $\forall \mathbf{x} \in \mathbb{R}^n$

$$(F_A + F_B)(\mathbf{x}) = F_A(\mathbf{x}) + F_B(\mathbf{x}) = A\mathbf{x} + B\mathbf{x}$$

Odtud ověříme, že $F_A + F_B$ je lineární (dosazením $\mathbf{x} = r\mathbf{y} + s\mathbf{z}$ a rozepsáním pravé strany) a že má matici $A + B$ (dosazením $\mathbf{x} = \mathbf{e}_i$ jako při hledání matice součinu a dokazování asociativity). Tedy $F_A + F_B = F_{A+B}$. Pak, opět jako při dokazování asociativity, ukážeme, že

$$\begin{aligned}((A + B)C)\mathbf{x} = (F_{A+B} \circ F_C)(\mathbf{x}) = F_{A+B}(F_C(\mathbf{x})) = \\ = (F_A + F_B)(F_C(\mathbf{x})) = F_A(F_C(\mathbf{x})) + F_B(F_C(\mathbf{x})) = AC\mathbf{x} + BC\mathbf{x}\end{aligned}$$

Rozmyslete si, z jakých přesných důvodů platí jednotlivé rovnosti! Jako v důkazu asociativity vede dosazení $\mathbf{x} = \mathbf{e}_i$ k rovnosti $(A+B)C = AC+BC$. Druhá rovnost v tvrzení se dokáže analogicky. □

Maticový součin ale určitě není komutativní. Je-li definován součin BA, součin AB definován být nemusí, případně nemusí být stejného typu:

$$\begin{pmatrix} b_1 & \dots & b_n \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \sum_{i=1}^{n} b_i a_i$$

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \begin{pmatrix} b_1 & \dots & b_n \end{pmatrix} = \begin{pmatrix} a_1 b_1 & \dots & a_1 b_n \\ \vdots & \ddots & \vdots \\ a_n b_1 & \dots & a_n b_n \end{pmatrix}$$

I v případě, že jsou A i B čtvercové matice $n \times n$ a tudíž jsou stejného typu i jejich součiny AB a BA, obvykle se tyto součiny nerovnají. Příklad už jsme viděli u rotací v prostoru, ale každý si snadno může vyrobit vlastní vygenerováním nějakých dvou „náhodných“ matic, stačí i 2×2.

TVRZENÍ 6. *Je-li A matice $m \times n$ a B matice $n \times p$, pak $(AB)^T = B^T A^T$.*

DŮKAZ. Označme $C = AB$, pak $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$. Pak

$$c_{ji}^T = c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} = \sum_{k=1}^{n} a_{ki}^T b_{jk}^T = \sum_{k=1}^{n} b_{jk}^T a_{ki}^T$$

Poslední suma je právě ji-tý element matice $B^T A^T$. □

Cvičení 4

Součin matic umožňuje definovat také mocninu čtvercové matice A^k jako k-násobný součin matice A se sebou samou. Dále definujeme $A^0 = E$. Spočtěte všechny přirozené mocniny matice

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Na základě předchozího výpočtu se pokuste najít příklady matic, pro které $A^k = 0$, ale $A^{k-1} \neq 0$ pro libovolné $k \in \mathbb{N}$.

3. Inverzní matice

Chceme-li nalézt inverzní zobrazení k $F_A : \mathbb{R}^n \to \mathbb{R}^n$, můžeme se pokusit jej hledat ve tvaru F_B pro nějakou matici B. Podmínka

$$\forall \mathbf{x} \in \mathbb{R}^n : (F_B \circ F_A)(\mathbf{x}) = \mathbf{x} \ \wedge \ (F_A \circ F_B)(\mathbf{x}) = \mathbf{x}$$

znamená, že $BA = AB = E$ (dosaďte opět $\mathbf{x} := \mathbf{e}_i$). Naopak pokud taková matice B existuje, pak $F_B \circ F_A = F_A \circ F_B = \mathrm{Id}$, takže F_B je inverzní zobrazení k F_A.

DEFINICE 4. Nechť $A \in \mathbb{R}^{n \times n}$. Matice A^{-1}, která splňuje $AA^{-1} = A^{-1}A = E$, se nazývá *matice inverzní k A*. Pokud matice A inverzní matici má, nazývá se *regulární*, jinak *singulární*.

TVRZENÍ 7. *Nechť $A, B, C \in \mathbb{R}^{n \times n}$ splňují $BA = AC = E$. Pak $B = C$.*

DŮKAZ. Plyne z asociativity součinu:

$$B = BE = B(AC) = (BA)C = EC = C$$

. □

Z tohoto tvrzení plyne, že inverzní matice k A může existovat nejvýše jedna.

PŘÍKLAD 4. Zkusme si inverzní matici spočítat pro konkrétní volbu matice

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

Hledejme 3×3 matici B s vlastností $AB = E$. Pak její i-tý sloupec splňuje rovnici $A\mathbf{b}_i = \mathbf{e}_i$. Pro $i = 1$ to znamená

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix},$$

kde jsme označili $\mathbf{x} := \mathbf{b}_1$.

Soustavu lineárních rovnic je zvykem zapisovat ve tvaru *rozšířené matice soustavy*

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

Každý řádek matice odpovídá rovnici roviny v $\mathbb{R}^3$, celá soustava pak hledání průniku tří rovin. Podobně jako dříve při hledání průsečnice můžeme první rovnici odečíst od druhé. V rozšířené matici se to projeví jako přičtení (-1)-násobku prvního řádku do druhého. Následně provedeme stejnou úpravu i se třetím řádkem.

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

Symbol $\sim$ se čte „se převede ekvivalentní úpravou na". *Ekvivalentní úpravy* jsou ty, které zachovávají množinu řešení.

Po přičtení dvojnásobku druhého řádku do třetího dostáváme soustavu

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 0 & 1 & 1 & -1 \\ 0 & 0 & 1 & -3 \end{array}\right) \quad \leftrightarrow \quad \begin{aligned} x_1 + 2x_2 + 3x_3 &= 1 \\ x_2 + x_3 &= -1 \\ x_3 &= -3 \end{aligned}$$

Z ní postupným dosazením získáme $x_3 = -3$, $x_2 = 2$, $x_1 = 6$. Můžeme také dosazování nahradit dalšími ekvivalentními úpravami:

$$\sim \left(\begin{array}{ccc|c} 1 & 2 & 0 & 10 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & -3 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0 & 0 & 6 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & -3 \end{array}\right)$$

Získali jsme tak $\mathbf{x} = \mathbf{b}_1$, první sloupec inverzní matice. Stejný výpočet s pravými stranami $\mathbf{e}_2$ a $\mathbf{e}_3$ dá zbývající dva. Pravé strany nemají vliv na to, které ekvivalentní úpravy volíme, můžeme tedy řešit všechny tři soustavy naráz, symbolicky

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 1 & 3 & 4 & 0 & 1 & 0 \\ 1 & 0 & 2 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 6 & -4 & -1 \\ 0 & 1 & 0 & 2 & -1 & -1 \\ 0 & 0 & 1 & -3 & 2 & 1 \end{array}\right)$$

Zjistili jsme tedy, že matice za svislou čarou je jediná, která splňuje rovnost $AB = E$. Vynásobením snadno ověříme, že i $BA = E$, tedy $B = A^{-1}$.

Víme ale, že tímto postupem získaná matice bude vždy dávat jednotkovou matici i při vynásobení z druhé strany? A že lze vždy buď najít ekvivalentní úpravy, kterými lze A^{-1} najít, nebo ukázat, že neexistuje?

Cvičení 5

Dokažte, že pokud $A, B \in \mathbb{R}^{n \times n}$ jsou regulární matice, pak matice $B^{-1}A^{-1}$ je inverzní maticí k matici AB, a tedy i AB je regulární matice.

Cvičení 6

Dokažte, že pokud A je regulární matice, pak A^T je také regulární matice, a její inverzní matice $(A^T)^{-1}$ je $(A^{-1})^T$, tedy matice transponovaná k A^{-1}.

KAPITOLA 3

Soustavy lineárních rovnic

V minulé kapitole jsme se setkali s několika úlohami vedoucími na soustavy lineárních rovnic:

- hledání průsečnice rovin (či obecně průniku nadrovin)
- hledání lineární kombinace vektorů $\mathbf{a}_1, \ldots, \mathbf{a}_n$, která dává vektor $\mathbf{b}$
- hledání vzoru vektoru $\mathbf{b}$ v zobrazení F_A.
- hledání sloupců inverzní matice

Další příklady jsou řešení rovnic vyplývajících z Kirchhoffových zákonů pro elektrické obvody, chemických rovnic, numerické aproximace řešení diferenciálních rovnic, proložení bodů polynomem nebo jinou funkcí či křivkou a mnoho dalších.

Řešení soustav lineárních rovnic je nejdůležitější úloha lineární algebry. Pokusíme se jí proto co nejlépe porozumět.

1. Odstupňovaný tvar matice

Definice 5. *Elementární řádkovou úpravou* (*EŘÚ*) matice rozumíme buď

(1) prohození dvou řádků
(2) přičtení libovolného násobku nějakého řádku do jiného řádku
(3) vynásobení nějakého řádku nenulovým číslem

Elementární maticí rozumíme matici, která vznikne z jednotkové matice elementární řádkovou úpravou.

Příklad 5. Příklady 4×4 elementárních matic jednotlivých úprav jsou

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ r & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & s & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

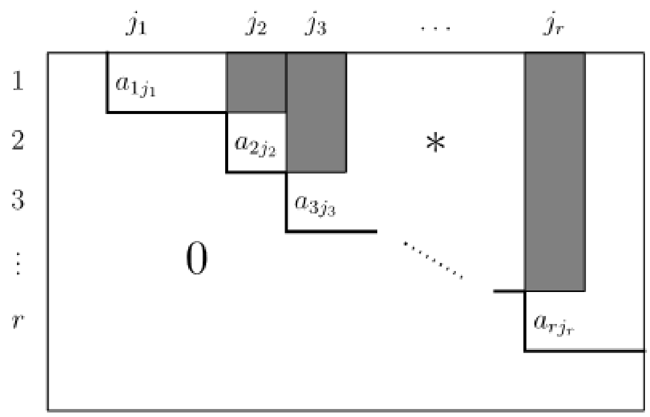
kde $s \neq 0$. Vyzkoušejte si, že pokud libovolnou matici A vynásobíme některou z těchto matic zleva, má to stejný efekt jako provedení příslušné elementární řádkové úpravy přímo na matici A.

Tvrzení 8. *Elementární řádková úprava rozšířené matice soustavy* $(A|\mathbf{b})$ *nemění množinu řešení. Pokud B je matice této EŘÚ, pak upravená matice je* $(BA|B\mathbf{b})$.

Důkaz. Každou EŘÚ lze vrátit zpět opět pomocí EŘÚ, například přičtení r-násobku i-tého řádku do j-tého se odstraní přičtením $-r$-násobku i-tého řádku do j-tého. Stačí tedy pro jednotlivé typy EŘÚ ukázat, že každé řešení $(A|\mathbf{b})$ je také řešením upravené soustavy. Tvar upravené matice vyplývá z toho, že součin matic je definován po sloupcích. Pokud tedy vektor $\mathbf{x}$ splňuje rovnost $A\mathbf{x} = \mathbf{b}$, pak splňuje i $BA\mathbf{x} = B\mathbf{b}$, tedy soustavu s maticí $(BA|B\mathbf{b})$. □

Řešení soustavy lineárních rovnic spočívá v převedení její rozšířené matice posloupností elementárních řádkových úprav do jednoduššího, tzv. odstupňovaného tvaru. Množina řešení se tím nezmění, ale je možné ji z odstupňovaného tvaru snáze získat.

Definice 6. První nenulový prvek každého řádku matice se nazývá *pivot.* Matice A je v *odstupňovaném tvaru,* pokud má každý pivot vyšší sloupcový index než pivot předchozího řádku. Sloupce, v nichž jsou v odstupňovaném tvaru pivoty, se nazývají *pivotní sloupce.* Matice je v *redukovaném odstupňovaném tvaru,* pokud jsou navíc všechny pivoty rovny 1 a všechny ostatní elementy pivotních sloupců jsou rovny 0.



Na obrázku jsou a_{1j_1} až a_{rj_r} pivoty, nalevo od nich a pod nimi jsou v matici nuly, napravo od nich a nad nimi může být obecně cokoliv. V redukovaném odstupňovaném tvaru jsou na místě tmavých obdélníků nuly.

Tvrzení 9. *Je-li rozšířená matice soustavy $(A|\mathbf{b})$ v odstupňovaném tvaru, pak má soustava rovnic řešení, právě když sloupec pravých stran není pivotní.*

Důkaz. Předpokládejme, že rozšířená matice má r nenulových řádků a pivoty mají sloupcové indexy $j_1 < j_2 < \ldots < j_r$. Pokud je sloupec pravých stran pivotní, pak je součástí soustavy také rovnice, která má na levé straně 0 a na pravé nenulový pivot b_r. Taková rovnice nemá řešení a tedy ani celá soustava. Pokud sloupec pravých stran pivotní není, pak je jedním z řešení vektor $\mathbf{x}$, v němž $\forall k \in \{1, \ldots, r\}$ je $x_{j_k} = b_k$ a ostatní složky $\mathbf{x}$ jsou nulové. $\square$

Obecné řešení SLR v odstupňovaném tvaru získáme, pokud položíme každou nepivotní složku rovnu nějakému reálnému parametru a zpětným dosazením dopočítáme složky pivotní. Nejlépe je to vidět na maticích v redukovaném odstupňovaném tvaru:

$$\left(\begin{array}{cccccc|c} 1 & 0 & -2 & -2 & 0 & -3 & 9 \\ 0 & 1 & 3 & -1 & 0 & -3 & 2 \\ 0 & 0 & 0 & 0 & 1 & -2 & 4 \end{array}\right)$$

Zvolíme $x_6 = t$, $x_4 = s$ a $x_3 = r$ a dopočteme

$$\begin{aligned} x_5 &= 4 + 2t \\ x_2 &= 2 - 3r + s + 3t \\ x_1 &= 9 + 2r + 2s + 3t \end{aligned}$$

Přepsáno do vektorového tvaru

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix} = \begin{pmatrix} 9 \\ 2 \\ 0 \\ 0 \\ 4 \\ 0 \end{pmatrix} + r \begin{pmatrix} 2 \\ -3 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + s \begin{pmatrix} 2 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + t \begin{pmatrix} 3 \\ 3 \\ 0 \\ 0 \\ 2 \\ 1 \end{pmatrix}$$

Všimněme si, že vektor **b** pravých stran nemá žádný vliv na koeficienty u parametrů r, s, t. Řešení SLR s maticí $(A|\mathbf{o})$ (*příslušné homogenní soustavy*) je tedy

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix} = r \begin{pmatrix} 2 \\ -3 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + s \begin{pmatrix} 2 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + t \begin{pmatrix} 3 \\ 3 \\ 0 \\ 0 \\ 2 \\ 1 \end{pmatrix}$$

2. Řešení soustav a podprostory

Vztah mezi řešením nehomogenní soustavy rovnic a příslušné soustavy homogenní se netýká jen soustav v odstupňovaném tvaru:

TVRZENÍ 10. *Nechť $\mathbf{x}_P$ je nějaké řešení SLR $(A|\mathbf{b})$. Pak vektor $\mathbf{x}_P + \mathbf{x}_H$ je řešením soustavy $(A|\mathbf{b})$ právě tehdy, když je $\mathbf{x}_H$ řešením příslušné homogenní soustavy.*

DŮKAZ. Pokud $\mathbf{x}_P + \mathbf{x}_H$ je řešením soustavy, pak $A(\mathbf{x}_P + \mathbf{x}_H) = \mathbf{b}$. Z distributivity maticového násobení plyne

$$A(\mathbf{x}_P + \mathbf{x}_H) = A\mathbf{x}_P + A\mathbf{x}_H = \mathbf{b} + A\mathbf{x}_H$$

Tedy $A\mathbf{x}_H = \mathbf{o}$. Pokud naopak $A\mathbf{x}_H = \mathbf{o}$, pak dosazením do rovnosti výše dostáváme $A(\mathbf{x}_P + \mathbf{x}_H) = \mathbf{b}$. □

Vektoru $\mathbf{x}_P$ říkáme *partikulární řešení nehomogenní soustavy*. Množině všech řešení homogenní soustavy $(A|\mathbf{o})$ pak *jádro matice A*, značíme $\operatorname{Ker} A$. Množina řešení nehomogenní soustavy se v duchu tvrzení zapisuje ve tvaru $\mathbf{x}_P + \operatorname{Ker} A$.

Jádro matice má význačné vlastnosti, které si zaslouží zavedení nového pojmu:

DEFINICE 7. Množina $W \subset \mathbb{R}^n$, která s každými vektory $\mathbf{x}, \mathbf{y} \in W$ obsahuje i všechny jejich lineární kombinace $r\mathbf{x} + s\mathbf{y}$, se nazývá *podprostor*. Množina tvaru $\mathbf{x} + W$, kde $\mathbf{x} \in \mathbb{R}^n$ a W je podprostor v $\mathbb{R}^n$, se nazývá *afinní podprostor*.

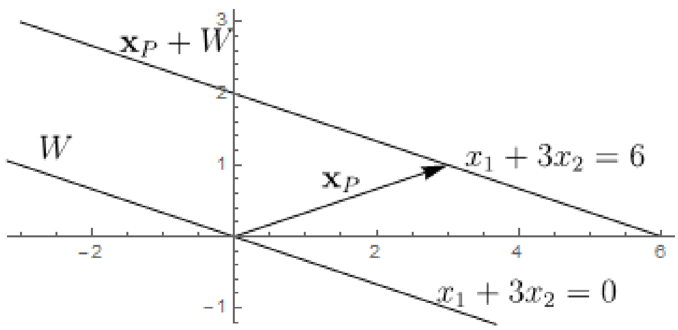
TVRZENÍ 11. *Jádro každé matice A typu $m \times n$ je podprostor v $\mathbb{R}^n$.*

DŮKAZ. Pokud $\mathbf{x}, \mathbf{y} \in \operatorname{Ker} A$, pak $A\mathbf{x} = A\mathbf{y} = \mathbf{o}$. Pak ale

$$A(r\mathbf{x} + s\mathbf{y}) = rA\mathbf{x} + sA\mathbf{y} = r\mathbf{o} + s\mathbf{o} = \mathbf{o},$$

tedy i $r\mathbf{x} + s\mathbf{y} \in \operatorname{Ker} A$. □

Každý podprostor musí obsahovat nulový vektor, stačí zvolit $r = s = 0$. Opačná implikace, tedy že podmnožina $\mathbb{R}^n$ obsahující nulový vektor je nutně podprostorem, neplatí (najděte protipříklad!). Afinní podprostor $\mathbf{x} + W$ obsahující $\mathbf{o}$ ovšem už podprostorem být musí. To nastává právě tehdy, když $\mathbf{x} \in W$. Homogenní a nehomogenní soustavy se tedy liší právě tím, že řešením prvních je vždy podprostor, řešením druhých nikdy není podprostor, pouze afinní podprostor:



3. Gaussova eliminace

Každou matici A typu $m \times n$ lze převést do (redukovaného) odstupňovaného tvaru postupem zvaným *Gaussova eliminace*:

(1) Najdeme první nenulový sloupec, jeho index označíme j. Pokud neexistuje, je matice nulová, tedy v redukovaném odstupňovaném tvaru.
(2) Pokud je $a_{1j} = 0$, pak prohodíme 1. řádek s libovolným řádkem i, v němž $a_{ij} \neq 0$.
(3) Pro každé $i = 2, 3, \dots, m$ přičteme $(-a_{ij}/a_{1j})$-násobek prvního řádku do i-tého řádku.
(4) Opakujeme postup pro matici bez prvního řádku. Proces se zastaví buď v bodě 1, nebo tím, že dojdou nenulové řádky. Pokud v každém průchodu bodu 1 zaznamenáme index j do proměnné j_k, dostaneme posloupnost $j_1 < j_2 < \dots j_r$ indexů pivotních sloupců, přičemž řádky $r+1$ až m jsou nulové.
(5) Pro každé $i = 1, \dots, r$ vynásobíme i-tý řádek číslem $1/a_{ij_i}$ a poté pro každé $k < i$ přičteme jeho $(-a_{kj_i})$-násobek do k-tého řádku.

Příklad 6. Ukažme si Gaussovu eliminaci na příkladě rozšířené matice SLR:

$$\left(\begin{array}{rrrrr|r} 0 & 3 & -6 & 6 & 4 & -5 \\ 3 & -7 & 8 & -5 & 8 & 1 \\ 3 & -9 & 12 & -9 & 6 & 3 \end{array}\right) \sim \left(\begin{array}{rrrrr|r} 3 & -9 & 12 & -9 & 6 & 3 \\ 3 & -7 & 8 & -5 & 8 & 1 \\ 0 & 3 & -6 & 6 & 4 & -5 \end{array}\right) \sim$$
$$\left(\begin{array}{rrrrr|r} 3 & -9 & 12 & -9 & 6 & 3 \\ 0 & 2 & -4 & 4 & 2 & -2 \\ 0 & 3 & -6 & 6 & 4 & -5 \end{array}\right) \sim \left(\begin{array}{rrrrr|r} 3 & -9 & 12 & -9 & 6 & 3 \\ 0 & 2 & -4 & 4 & 2 & -2 \\ 0 & 0 & 0 & 0 & 1 & -2 \end{array}\right)$$

První úpravě, tedy hledání vhodného pivota, se říká *pivotace*. Po dvou průchodech body 1,2,3,4 jsme dospěli zpět do 1 a nemáme už žádné nenulové řádky. Bod 5, tedy přechod do redukovaného tvaru, je efektivnější provádět odspodu:

$$\left(\begin{array}{rrrrr|r} 3 & -9 & 12 & -9 & 0 & 15 \\ 0 & 2 & -4 & 4 & 0 & 2 \\ 0 & 0 & 0 & 0 & 1 & -2 \end{array}\right) \sim \left(\begin{array}{rrrrr|r} 1 & 0 & -2 & 3 & 0 & 8 \\ 0 & 1 & -2 & 2 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & -2 \end{array}\right)$$

Množina řešení soustavy má tvar

$$\mathbf{x}_P + \operatorname{Ker} A = \begin{pmatrix} 8 \\ 1 \\ 0 \\ 0 \\ -2 \end{pmatrix} + \left\{ s \begin{pmatrix} 2 \\ 2 \\ 1 \\ 0 \\ 0 \end{pmatrix} + t \begin{pmatrix} -3 \\ -2 \\ 0 \\ 1 \\ 0 \end{pmatrix} \middle| s, t \in \mathbb{R} \right\}$$

Množina všech lineárních kombinací nějaké množiny vektorů $M \subset \mathbb{R}^n$ se značí $\langle M \rangle$ a říká se jí *lineární obal*. S tímto značením můžeme řešení zapsat poněkud úsporněji jako

$$(8, 1, 0, 0, -2)^T + \langle (2, 2, 1, 0, 0)^T, (-3, -2, 0, 1, 0)^T \rangle$$

Často se v zápise vynechává i symbol transponování.

První 4 kroky Gaussovy eliminace převedou do odstupňovaného tvaru libovolnou matici. To plyne jednoduše matematickou indukcí podle počtu nenulových řádků v matici. Je-li jich nula, pak je matice zjevně v odstupňovaném tvaru. Pokud je jich $k > 0$, pak po provedení prvních 3 kroků získáme sloupcový index j_1 prvního pivotu, který je menší než sloupcový index všech nenulových prvků všech ostatních řádků. Z indukčního předpokladu plyne, že matice vzniklá vynecháním prvního řádku se prvními 4 kroky Gaussovy eliminace převede do odstupňovaného tvaru, přičemž sloupcové indexy pivotů $j_2 < \dots < j_r$ musí být větší než j_1. Výsledná matice je tedy v odstupňovaném tvaru a bod 5 ji převede do redukovaného odstupňovaného tvaru.

4. Izomorfismus

Následující pojmosloví se užívá pro libovolná zobrazení, nikoli nutně lineární. Zobrazení $f : X \to Y$ se nazývá

- *prosté* (*injektivní*), pokud má každý prvek z Y nejvýše jeden vzor, tedy pokud $f(a) = f(b)$, pak $a = b$.
- *na* (*surjektivní*), pokud má každý prvek z Y alespoň jeden vzor
- *vzájemně jednoznačné* (*bijektivní*), pokud má každý prvek z Y právě jeden vzor, tedy pokud existuje inverzní zobrazení $f^{-1} : Y \to X$.

V případě, že f je navíc lineární, používají se pojmy *monomorfismus*, *epimorfismus* a *izomorfismus*. Z lineárních zobrazení, kterými jsme se zabývali, jsou zrcadlení $Z_{\mathbf{x}^\perp}$, dilatace D_λ pro $\lambda \neq 0$ i rotace izomorfismy (jak vypadají inverzní zobrazení?. Projekce $P_\mathbf{x} : \mathbb{R}^n \to \mathbb{R}^n$ není prosté zobrazení, protože libovolný vektor z nadroviny $\mathbf{x}^\perp$ se zobrazí na $\mathbf{o}$, a není ani zobrazení na, protože $P_\mathbf{x}(\mathbf{y})$ leží vždy v $\langle \mathbf{x} \rangle$. Podobně pro $P_{\mathbf{x}^\perp}$.

Definice 8. Nechť $f : X \to Y$ je zobrazení. Pak množina všech prvků $p \in Y$, pro které existuje $a \in X$ takové, že $f(a) = p$, se nazývá *obraz* zobrazení f a značí se $\operatorname{Im} f$.

Obrazu se někdy říká také *obor hodnot*. Zobrazení f je na, právě když $\operatorname{Im} f = Y$.

Zobrazení $F_A : \mathbb{R}^n \to \mathbb{R}^m$ je prosté právě tehdy, když rovnice $A\mathbf{x} = \mathbf{b}$ má pro všechna $\mathbf{b}$ nejvýše jedno řešení, tedy když $\operatorname{Ker} A = \{\mathbf{o}\}$. To nastává právě tehdy, když jsou po převodu A na odstupňovaný tvar všechny sloupce pivotní, neboli přejde-li A v redukovaném odstupňovaném tvaru na jednotkovou matici, případně doplněnou o nějaké nulové řádky. Soustava $A\mathbf{x} = \mathbf{b}$ má řešení, pakliže $\mathbf{b}$ lze zapsat jako

$$(\mathbf{a}_1|\dots|\mathbf{a}_n)\mathbf{x} = x_1\mathbf{a}_1 + \dots x_n\mathbf{a}_n,$$

neboli $\operatorname{Im} A = \langle \mathbf{a}_1, \dots, \mathbf{a}_n \rangle$. Zobrazení F_A je tedy na, právě když $\langle \mathbf{a}_1, \dots, \mathbf{a}_n \rangle = \mathbb{R}^m$. Lineárnímu obalu sloupců se říká *sloupcový prostor* matice A (analogicky definujeme *řádkový prostor*, ten je roven $\operatorname{Im} A^T$). Rovnost $\langle \mathbf{a}_1, \dots, \mathbf{a}_n \rangle = \mathbb{R}^m$ formulujeme také tak, že sloupce matice A prostor $\mathbb{R}^m$ *generují*.

Tvrzení 12. *Zobrazení $f_A : \mathbb{R}^n \to \mathbb{R}^m$ je bijektivní, právě když A je čtvercová a existuje matice X, pro kterou $AX = E$.*

Důkaz. Je-li f_A bijektivní, pak pro každou pravou stranu $\mathbf{b}$ má SLR $A\mathbf{x} = \mathbf{b}$ právě jedno řešení. Nemůže tedy být $m < n$, protože pak by po převodu na odstupňovaný tvar nemohly být všechny sloupce pivotní a tedy $\operatorname{Ker} A \neq \{\mathbf{o}\}$. Nemůže být ani $m > n$, protože pak by bylo možné najít pravou stranu $\mathbf{b}$ takovou, že po eliminaci matice $(A|\mathbf{b})$ bude sloupec pravých stran pivotní. Tedy A je čtvercová. Pro pravou stranu $\mathbf{e}_i$ označme $\mathbf{x}_i$ řešení soustavy $A\mathbf{x} = \mathbf{e}_i$. Pak $X = (\mathbf{x}_1|\dots|\mathbf{x}_n)$ splňuje $AX = E$. Tím je dokázána první implikace.

Dokažme nyní druhou. Pokud existuje matice X splňující $AX = E$, pak $\mathbf{x} := X\mathbf{b}$ je řešením soustavy rovnic $A\mathbf{x} = \mathbf{b}$. Tedy f_A je na. Uvažujme eliminaci rozšířené matice $(A|E)$ elementárními úpravami s maticemi $B_1, \dots, B_k$. Pak

$$(A|E) \sim (B_k \dots B_1 A | B_k \dots B_1 E) = (C | B_k \dots B_1),$$

kde matice C je v redukovaném odstupňovaném tvaru. Pokud by měla nulový řádek, neplatilo by, že $(A|\mathbf{b})$ má řešení pro každé $\mathbf{b}$. Protože je čtvercová, musí tedy mít n pivotních sloupců, neboli být jednotkovou maticí. Pak ale j-tý sloupec součinu

$B_k \dots B_1$ je jediným řešením soustavy rovnic $A\mathbf{x} = \mathbf{e}_j$, jejímž řešením je i j-tý sloupec X. Tedy $B_k \dots B_1 = X$ a $XA = E$. Tedy X je inverzní matice k A a tudíž i f_X inverzní zobrazení k f_A. $\square$

Připomeňme, že čtvercovou matici A, která má inverzní matici, nazýváme *regulární*. Z tvrzení a jeho důkazu plyne, že regulární jsou právě ty matice, pro které je f_A bijektivní, a že stačí ověřovat jen podmínku $AX = E$, tedy inverznost zprava.

KAPITOLA 4

Vektorové prostory

V prvních třech přednáškách jsme se zabývali vektory v $\mathbb{R}^n$ a setkali se při tom mimo jiné s pojmy lineární kombinace, (afinního) podprostoru, lineárního zobrazení a kanonické báze. Tyto pojmy je možné a užitečné zobecnit na další typy objektů, které lze mezi sebou sčítat a násobit je skalárem. Například levá strana rovnosti

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

je lineární kombinací 2×2 matic, levá strana rovnosti

$$(3x+1) + 2(-x^3 + x^2 - x + 2) + (2x^3 - 1) = 2x^2 + x + 4$$

je lineární kombinací polynomů. V obou případech rovnosti říkají, že matice/polynom na pravé straně je v podprostoru generovaném maticemi/polynomy na levé straně. Označíme-li

$$K_M := \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}, K_P := \{1, x, x^2, x^3\},$$

můžeme každou matici, resp. polynom stupně nejvýše 3 jednoznačně zapsat jako lineární kombinaci prvků množiny K_M, resp. K_P. Tyto množiny tedy pro matice/polynomy hrají podobnou roli jako kanonická báze $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ pro $\mathbb{R}^n$. Rovnost výše pak intuitivně vyjadřuje totéž jako vztah

$$\begin{pmatrix} 0 \\ 0 \\ 3 \\ 1 \end{pmatrix} + 2\begin{pmatrix} -1 \\ 1 \\ -1 \\ 2 \end{pmatrix} + \begin{pmatrix} 2 \\ 0 \\ 0 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \\ 1 \\ 4 \end{pmatrix},$$

pro vektory z $\mathbb{R}^4$.

Podobně můžeme zacházet s mnoha dalšími objekty, například komplexními čísly, maticemi $m \times n$, spojitými funkcemi na daném intervalu, nekonečnými posloupnostmi čísel a mnoha dalšími. Tyto podobnosti vybízejí k tomu, abychom potřebné vlastnosti vektorů abstrahovali a všechny související pojmy zaváděli naráz a obecně pro tyto abstraktní vektory. Dokázaná tvrzení pak budou mít také obecnou platnost. Ještě předtím musíme ale zavést pojem tělesa, což je množina, jejíž prvky jsou abstrakcí pojmu skaláru, a pojem grupy, který se v definici tělesa i vektorového prostoru vyskytuje a který má i sám o sobě pro matematiku a fyziku velkou důležitost.

1. Grupa a těleso

Definice 9 (Grupa). Nechť $\circ : G \times G \to G$ je binární operace na množině G. Pak *grupou* nazýváme dvojici $(G, \circ)$, která splňuje

(1) $\forall a, b, c \in G : (a \circ b) \circ c = a \circ (b \circ c)$ (asociativita)
(2) $\exists e \in G : \forall a \in G : a \circ e = e \circ a = a$ (neutrální prvek)
(3) $\forall a \in G : \exists a^{-1} \in G : a \circ a^{-1} = a^{-1} \circ a = e$ (inverzní prvky)

Pokud navíc $\forall a, b \in G : a \circ b = b \circ a$, pak je $(G, \circ)$ *komutativní grupa.*

Pod označením $\circ$ se může skrývat jakákoli binární operace, nemusí jít nutně o skládání zobrazení. Zároveň mnoho příkladů grup jsou grupy zobrazení s operací jejich skládání. Například množina všech rotací okolo počátku v rovině $\mathbb{R}^2$

$$(\{R_\phi : \mathbb{R}^2 \to \mathbb{R}^2 | \phi \in \langle 0, 2\pi)\}, \circ)$$

je uzavřená na skládání (tedy složení dvou rotací je zase rotace), obsahuje neutrální prvek $R_0 \equiv \mathrm{Id}$ i inverzní prvek $R_{-\phi}$ ke každému R_ϕ. Asociativita a v tomto případě i komutativita jsou splněny rovněž. Dalším typickým příkladem, který můžeme formulovat pomocí značení zavedeného v minulých kapitolách, je grupa

$$(\{\mathrm{Id}, R_{2\pi/3}, R_{-2\pi/3}, Z_{(1,0)^\perp}, Z_{(1,\sqrt{3})^\perp}, Z_{(-1,\sqrt{3})^\perp}\}, \circ)$$

všech zobrazení, která zachovávají rovnostranný trojúhelník s těžištěm v počátku a výškou orientovanou ve směru druhé souřadné osy. Podobné grupy symetrií geometrických útvarů v rovině a prostoru jsou základem disciplín jako krystalografie, spektroskopie, kvantová mechanika a dalších.

Pro nás jsou nyní důležitější grupy založené na množině čísel s nějakou aritmetickou operací. V případě sčítání to mohou být třeba grupy $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ (proč ne $(\mathbb{N}, +)$?) a grupami jsou také množiny vektorů $(\mathbb{R}^n, +)$ a matic $(\mathbb{R}^{m\times n}, +)$ se sčítáním zavedeným v minulých kapitolách. Neutrálním prvkem je zde 0, inverzním prvkem k x je opačné číslo $-x$.

Příklady grup s operací násobení jsou třeba $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$ nebo $(\{z \in \mathbb{C} |\ |z| = 1\}, \cdot)$. Neutrálním prvkem je zjevně 1, inverzním prvkem k a je $\frac{1}{a}$. Proto také v žádné z množin nemůže být 0.

Množiny matic typu 2×2 s operací násobení matic nám dávají mnoho příkladů nekomutativních grup. Například grupa

$$\left(\left\{\begin{pmatrix}\cos\phi & -\sin\phi \\ \sin\phi & \cos\phi\end{pmatrix} | \phi \in \langle 0, 2\pi)\right\}, \circ\right)$$

odpovídající maticím rotací komutativní je, ale pokud zkonstruujeme analogicky grupu matic symetrií rovnostranného trojúhelníka, zjistíme, že matice rotací a zrcadlení spolu nekomutují.

Definice 10 (Komutativní těleso). Množina T se nazývá *komutativní těleso*, pokud jsou na ní definovány dvě binární operace $+$ a $\cdot$, splňující

(1) $(T, +)$ je komutativní grupa.
(2) Označíme-li neutrální prvek $(T, +)$ symbolem 0, pak $(T \setminus \{0\}, \cdot)$ je komutativní grupa.
(3) $\forall a, b, c \in T : a \cdot (b + c) = a \cdot b + a \cdot c$ (distributivita)

Název „těleso“ nijak nesouvisí s tělesy geometrickými, je jen překladem slova Zahlenkörper z němčiny. Klasickými příklady těles jsou množiny $\mathbb{Q}$, $\mathbb{R}$ nebo $\mathbb{C}$ s operacemi sčítání a násobení. V algebře a informatice nacházejí uplatnění *konečná tělesa*, jejichž základním příkladem je $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ s operacemi sčítání a násobení modulo prvočíslo p. Tělesa jsou je také klíčová pro teorii řešení algebraických rovnic vyšších stupňů, s níž přišel Évariste Galois v roce 1832. Většina jeho matematického dědictví pochází z dopisu, který napsal dva dny před tím, než zahynul v souboji.

Pokud nepožadujeme, aby bylo násobení komutativní, zachováme ostatní axiomy a doplníme pravostrannou distributivitu $(b + c) \cdot a = b \cdot a + c \cdot a$, pak definici splňují např. tzv. kvaterniony, používané pro elegantní popis rotací v $\mathbb{R}^3$.

Prvky T hrají v lineární algebře roli skalárů. Většina textů buduje lineární algebru nad obecnými tělesy, což znamená strávit nějaký čas odvozováním důsledků definice tělesa a zaváděním některých pojmů, zejména tzv. charakteristiky tělesa, která zhruba řečeno pomáhá od sebe odlišit tělesa s nekonečným počtem prvků jako

$\mathbb{R}$ nebo $\mathbb{C}$ a tělesa konečná. Protože počítání s konečnými tělesy není v matematické fyzice příliš často k vidění, omezíme na T rovné buď $\mathbb{R}$ nebo $\mathbb{C}$ a budeme místo pojmu (komutativní) těleso používat pojem *množina skalárů*. Standardně budeme množinu skalárů značit $\mathbb{F}$, což vychází z výrazu *field*, který se pro komutativní těleso používá v angličtině.

2. Vektorový prostor

DEFINICE 11 (Vektorový prostor). Nechť $\mathbb{F}$ je množina skalárů. Množinu V nazveme *vektorovým prostorem nad* $\mathbb{F}$, pokud je na ní definována operace *sčítání vektorů*

$$+ : V \times V \to V$$

taková, že $(V, +)$ je komutativní grupa, a operace *násobení skalárem*

$$\cdot : \mathbb{F} \times V \to V,$$

jejíž výsledek pro $r \in \mathbb{F}$ a $v \in V$ označíme rv, a tyto operace splňují $\forall u, v \in V$ a $\forall r, s \in \mathbb{F}$

(1) $1v = v$ (násobení jednotkou)
(2) $r(sv) = (rs)v$ (asociativita)
(3) $(r + s)v = rv + sv$ (distributivita sčítání skalárů)
(4) $r(u + v) = ru + rv$ (distributivita sčítání vektorů)

Neutrální prvek ve $(V, +)$ značíme o (*nulový vektor*) a inverzní prvek k $v \in V$ značíme $-v$ (*opačný vektor*).

TVRZENÍ 13. *Nechť V je vektorový prostor nad $\mathbb{F}$. Pak $\forall v \in V$, $\forall r \in \mathbb{F}$ platí*

(1) $0v = o$
(2) $(-1)v = -v$
(3) $ro = o$

DŮKAZ. Pro libovolný vektor $v \in V$ platí

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

kde jsme použili nejprve vlastnost násobení jednotkou z definice vektorového prostoru, pak vlastnost nuly jako neutrálního prvku v množině skalárů (tělese), pak distributivitu sčítání skalárů a nakonec znovu násobení jednotkou. Protože $(V, +)$ je grupa, musí mít v opačný vektor $-v$ a s užitím asociativity sčítání v grupě plyne, že

$$o = (-v) + v = (-v) + (v + 0.v) = ((-v) + v) + 0.v = o + 0.v = 0.v,$$

čímž je dokázáno první tvrzení. Zbylá dvě necháváme čtenáři za cvičení. □

Základním příkladem vektorového prostoru je $\mathbb{F}^n$ nad $\mathbb{F}$, tedy množina všech uspořádaných n-tic prvků z $\mathbb{F}$, ve které se sčítá a násobí skalárem po složkách. Doposud jsme vektorem rozuměli prvek $\mathbb{R}^n$ a zapisovali ho jako sloupec čísel. Od nynějška pro nás slovo vektor znamená prvek nějakého vektorového prostoru. Vektorům v původním smyslu budeme od nynějška říkat *aritmetické vektory* a vektorovému prostoru $\mathbb{F}^n$ *aritmetický vektorový prostor*.

Symbolem $\mathbb{F}^{m \times n}$ označujeme vektorový prostor všech $m \times n$ matic s elementy z $\mathbb{F}$. Podobně jako u aritmetického vektoru se snadno ověří, že je to vektorový prostor nad $\mathbb{F}$ s operacemi sčítání matic a násobení matice skalárem, tak jak jsme je dříve zavedli.

Množina $F(X, \mathbb{F})$ všech funkcí z množiny X do $\mathbb{F}$ s operacemi

$$(f + g)(x) := f(x) + g(x)$$
$$(rf)(x) := rf(x),$$

je vektorový prostor nad $\mathbb{F}$. Jaký je vlastně význam tohoto předpisu? První řádka definuje funkci $f+g$ její hodnotou v bodě x, a to tak, že pro libovolné $x \in X$ je tato hodnota součtem hodnot funkcí f a g v x. Druhá obdobně definuje násobek funkce. Pro $X = \mathbb{R}$ to dává prostor všech funkcí jedné reálné proměnné, pro $X = \mathbb{N}$ prostor všech nekonečných posloupností, pro $X = \{1, \dots, n\}$ je to prostor všech n-prvkových posloupností, které se sčítají po složkách, což vlastně není nic jiného než aritmetický vektorový prostor $\mathbb{F}^n$.

Množinu $\mathbb{C}$ můžeme chápat jako vektorový prostor nad sebou samou, nebo jako vektorový prostor nad $\mathbb{R}$. Je v tom rozdíl, protože v prvním případě je každý nenulový vektor násobkem každého jiného nenulového vektoru, v druhém ale 1 a i nejsou skalárním násobkem jeden druhého. Intuitivně se tedy první verze podobá více přímce a druhá více rovině. Analogicky má každý vektorový prostor V nad $\mathbb{C}$ svého „dvojníka“, ve kterém je dovoleno násobit jen reálnými čísly. Pokud ale v dalším napíšeme $\mathbb{C}^n$, rozumíme tím vždy vektorový prostor nad $\mathbb{C}$.

Většina dalších zajímavých příkladů vektorových prostorů vzniká jako podprostory jiných vektorových prostorů. Obecná definice podprostoru se prakticky neliší od té, kterou už jsme měli v $\mathbb{R}^n$:

Definice 12. Nechť V je vektorový prostor nad $\mathbb{F}$ a W je neprázdná podmnožina V taková, že $\forall v, w \in W$, $\forall r, s \in \mathbb{F}$ platí $rv + sw \in W$. Pak nazýváme W *podprostorem* vektorového prostoru V, značíme $W \leq V$.

Tvrzení 14. *Neprázdná podmnožina $W \subset V$ je podprostorem ve V, právě když je uzavřená na součty a na násobení libovolným skalárem.*

Důkaz. Pokud je W uzavřená na součty a na násobení skalárem, pak s každými vektory $v, w \in W$ jsou ve W i rv, sw a $rv + sw$, pro libovolné $r, s \in \mathbb{F}$. Pro důkaz opačné implikace stačí volit $r = s = 1$, resp. r libovolné a $s = 0$. $\square$

Každý vektorový prostor V má dva tzv. *triviální podprostory*, $0 := \{o\}$ (*nulový podprostor*) a sebe sama. Symbol 0 se užívá i pro vektorový prostor obsahující jediný prvek, který samozřejmě musí být totožný s neutrálním prvkem v tomto prostoru, tedy nulovým vektorem.

Podprostor W nějakého vektorového prostoru V je opět vektorový prostor. Tím myslíme, že splňuje axiomy z definice vektorového prostoru. Pro ověření je klíčové, že nám definice podprostoru zaručuje uzavřenost operací, tedy že všechny součty a násobky skalárem, které se v axiomech vyskytují, jsou opět prvky W, a to včetně neutrálního prvku a opačných prvků, které díky prvnímu a druhému bodu tvrzení 13 vzniknou také jako násobky prvku z W skalárem.

Definice 13. Nechť V je vektorový prostor nad $\mathbb{F}$ a $r_1, \dots, r_n \in \mathbb{F}$, $v_1, \dots, v_n \in V$. Výraz $\sum_{i=1}^n r_i v_i$ se nazývá *lineární kombinace* vektorů v_i s koeficienty r_i. Pro neprázdnou $M \subset V$ značí $\langle M \rangle$ množinu všech lineárních kombinací prvků M, neboli její *lineární obal*. Pro $M = \emptyset \subset V$ definujeme jako její lineární obal nulový podprostor $0 \leq V$.

Tvrzení 15. *Nechť V je vektorový prostor nad $\mathbb{F}$ a $M \subset V$. Pak $\langle M \rangle \leq V$.*

Důkaz. Stačí si uvědomit, že součet lineárních kombinací prvků W je opět lineární kombinace prvků W a podobně i pro násobek skalárem. $\square$

Definice 14. Nechť V je vektorový prostor nad $\mathbb{F}$, $W \leq V$, $v \in V$. Množinu $v + W$, jejímiž prvky jsou všechny součty vektoru v s nějakým prvkem podprostoru W, nazýváme *afinní podprostor* ve V, podprostor W nazýváme *zaměřením* tohoto afinního podprostoru.

Afinní podprostor je podprostorem, právě když $v \in W$. Důkaz ponecháváme opět za cvičení.

3. Generování, lineární (ne)závislost, báze

Nechť W je vektorový prostor (který může a nemusí být podprostorem jiného vektorového prostoru). O množině $M \subset W$, pro kterou $\langle M \rangle = W$, říkáme, že prostor W *generuje*, případně, že M je *množinou generátorů* prostoru W.

Typicky existuje mnoho různých množin generujících stejný vektorový prostor:

$$\left\{\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix}\right\},\left\{\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix},\begin{pmatrix}2\\3\end{pmatrix}\right\},\mathbb{R}^2,\mathbb{R}^2\setminus\left\{\begin{pmatrix}1\\2\end{pmatrix},\begin{pmatrix}3\\4\end{pmatrix}\right\}$$

jsou všechno množiny generátorů prostoru $\mathbb{R}^2$. Přirozenou otázkou je, jak najít pro daný podprostor množinu generátorů co nejmenší.

Definice 15. Lineární kombinace se nazývá *netriviální*, pokud má alespoň jeden koeficient nenulový. Podmožina M vektorového prostoru V nad $\mathbb{F}$ je *lineárně závislá*, pokud existují vektory $v_1, \dots, v_n \in M$ a jejich netriviální lineární kombinace $\sum_{i=1}^n r_i v_i$ se rovná nulovému vektoru o. V opačném případě je M *lineárně nezávislá*.

Příklad 7. Množina

$$\left\{\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix},\begin{pmatrix}2\\3\end{pmatrix}\right\}$$

je lineárně závislá, protože lze z vektorů vytvořit lineární kombinaci s koeficienty $-2, -3, 1$, která je netriviální a dává nulový vektor v $\mathbb{R}^2$. Množina

$$\left\{\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix}\right\}$$

je lineárně nezávislá, protože lineární kombinace

$$r\begin{pmatrix}1\\0\end{pmatrix}+s\begin{pmatrix}0\\1\end{pmatrix}$$

může být rovna nulovému vektoru pouze pro $r = s = 0$. Prázdná množina $\emptyset$ je lineárně nezávislá. Množina $\{1, i\} \subset \mathbb{C}$ je lineárně nezávislá v $\mathbb{C}$ nad $\mathbb{R}$, ale lineárně závislá v $\mathbb{C}$ nad $\mathbb{C}$.

Tvrzení 16. *Nechť V je vektorový prostor nad $\mathbb{F}$. Pak platí:*

(1) *$M \subset V$ mající alespoň dva prvky je lineárně závislá, právě když existuje $v \in M$, který lze vyjádřit jako lineární kombinaci ostatních prvků M.*
(2) *Nechť M generuje V. Pak M je lineárně závislá, právě když existuje vlastní podmnožina $N \subset M$, která generuje V.*

Důkaz. Nechť existuje netriviální lineární kombinace $\sum_{i=1}^n r_i v_i = o$, kde v_i jsou z M. Vektory v_i si můžeme libovolně přečíslovat, předpokládejme tedy, že $r_1 \neq 0$. Pak $v_1 = \sum_{i=2}^n \frac{-r_i}{r_1} v_i$, tedy v_1 lze vyjádřit jako lineární kombinaci ostatních vektorů. Naopak, pokud lze nějaký $v_1 \in M$ zapsat jako lineární kombinaci ostatních vektorů $\sum_{i=2}^n s_i v_i$, stačí položit $s_1 = -1$ a máme lineární kombinaci $\sum_{i=1}^n s_i v_i = o$ rovnou nulovému vektoru. Tím je dokázán první bod.

Pro druhý bod vyberme v M vektor v, který je dle bodu 1 lineární kombinací ostatních $v = \sum_{i=1}^k r_i v_i$. Definujme $N := M \setminus \{v\}$. Pak můžeme každý vektor u, který je lineární kombinací $u = \sum_{j=1}^n s_j u_j$ vektorů $u_j \in M$, zapsat jako lineární kombinaci vektorů z N. Pokud žádný z vektorů u_j není roven v, je to zřejmé. Pokud některý je roven v, stačí jej nahradit v lineární kombinaci sumou $\sum_{i=1}^k r_i v_i$ a u je pak vyjádřen jen pomocí vektorů z N. Naopak, pokud $N \subset M$, N i M obě generují V a $v \in M \setminus N$, pak lze v zapsat jako lineární kombinaci prvků N a tedy podle bodu 1 je M lineárně závislá. $\square$

Definice 16. Nechť V je vektorový prostor nad $\mathbb{F}$. Množina M, která generuje V a zároveň je lineárně nezávislá, se nazývá *báze vektorového prostoru V*.

Základním příkladem báze je kanonická báze $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ v $\mathbb{F}^n$. Je hned vidět, že je lineárně nezávislá a generuje $\mathbb{F}^n$.

Podle předchozího tvrzení je báze V taková množina generátorů V, která po odebrání libovolného vektoru už množinou generátorů V není.

TVRZENÍ 17. *Nechť V je vektorový prostor nad $\mathbb{F}$. Množina M je bází V, právě když lze každý vektor z V vyjádřit jako lineární kombinací prvků M právě jedním způsobem.*

DŮKAZ. Pokud je M bází V, pak V i generuje, a tedy každý vektor z V lze vyjádřit jako lineární kombinaci prvků M alespoň jedním způsobem. Pokud by nějaký $v \in V$ měl dvojí vyjádření $\sum_{i=1}^n r_i v_i = \sum_{i=1}^n s_i v_i$, kde alespoň jeden koeficient $r_i \neq s_i$, pak by rozdíl těchto vyjádření byl netriviální lineární kombinací $\sum_{i=1}^n (r_i - s_i) v_i$ rovnou nulovému vektoru.

Je-li naopak každý vektor vyjádřen nejvýše jedním způsobem, platí to i pro nulový vektor, jenž je pomocí vektorů z M vyjádřen triviální lineární kombinací (či kombinacemi). Pak ale nemůže být vyjádřen zároveň i netriviální lineární kombinací, a tedy je M lineárně nezávislá. Zároveň je každý vektor vyjádřen alespoň jedním způsobem, tedy M generuje V. M je tedy bází V. $\square$

Předpokládejme, že $M = \{v_1, \ldots, v_n\}$ je báze vektorového prostoru V nad $\mathbb{F}$. Každému vektoru $v \in V$ lze podle předchozího tvrzení přiřadit jednoznačně n-tici $(r_1, \ldots, r_n)$ prvků $\mathbb{F}$. Když tedy určíme nějaké pořadí prvků M, přiřazujeme vlastně vektoru v z V aritmetický vektor $\mathbf{r}$ z $\mathbb{F}^n$. Tomuto vektoru se říká *vektor souřadnic vektoru v vzhledem k bázi M* nebo též *reprezentace vektoru v vzhledem k bázi M*. Pokud například

$$M = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

je báze $\mathbb{R}^{2\times 2}$, pak je matice $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ reprezentována vzhledem k M vektorem $(1, 2, 3, 4)^T$. Počítání v rozličných vektorových prostorech můžeme takto převést na výpočty s vektory aritmetickými. Ale jak tyto výpočty ovlivňuje to, jakou bázi ve V si zvolíme? Budou mít vždy příslušné aritmetické vektory stejný počet složek? A dá se vždy najít báze s konečně mnoha prvky? Odpovědi nalezneme v příští kapitole.

KAPITOLA 5

Báze a dimenze

V minulé kapitole jsme definovali bázi jako takovou podmnožinu vektorového prostoru V, která je zároveň lineárně nezávislá a zároveň tento prostor generuje. Báze nemusí být nutně konečná množina.

PŘÍKLAD 8. Množina $M := \{1, x, x^2, x^3, \dots, x^i, \dots\}$ ve vektorovém prostoru $P(x, \mathbb{R})$ všech reálných polynomů v proměnné x je jeho bází, neboť každý polynom $p(x) = \sum_{i=0}^{k} a_i x^i$ lze zapsat jednoznačně jako lineární kombinaci monomů x^i. Nějakou jinou konečnou bázi prostor $P(x, \mathbb{R})$ mít nemůže, protože v lineárním obalu konečné množiny polynomů N mohou být jen polynomy, jejichž stupeň není vyšší než nejvyšší stupeň v N zastoupený.

DEFINICE 17. Vektorový prostor V nad $\mathbb{F}$ se nazývá *prostorem konečné dimenze*, pokud v něm existuje konečná báze.

TVRZENÍ 18. *Nechť V je vektorový prostor nad $\mathbb{F}$. Pak jsou následující tvrzení ekvivalentní:*

(1) *V je konečné dimenze.*
(2) *Ve V existuje konečná množina generátorů.*
(3) *Z každé množiny generátorů V lze vybrat konečnou bázi V.*

DŮKAZ. Implikace $1 \Rightarrow 2$ a $3 \Rightarrow 1$ jsou zřejmé, stačí tedy dokázat $2 \Rightarrow 3$. Máme-li ve V konečnou množinu generátorů M a nějakou (ne nutně konečnou) množinu generátorů N, pak lze každý prvek M vyjádřit jako lineární kombinaci prvků N. Označme N' množinu všech prvků N, u kterých je ve vyjádření některého prvku M nenulový koeficient. Množina N' je konečná a libovolný prvek V lze vyjádřit jako lineární kombinaci prvků N'. Podle druhé části tvrzení 16 je N' buď lineárně nezávislá, nebo z ní lze odebrat prvky, aniž by se změnil lineární obal. Tedy odebráním konečného počtu prvků lze nalézt podmnožinu $N'' \subset N'$, která je bází V. □

Ze třetího bodu tvrzení plyne, že v prostoru V konečné dimenze musejí být všechny báze konečné. Dokážeme-li ještě, že všechny báze V musejí mít stejný počet prvků, budeme moci zadefinovat pojem dimenze V právě jako tento počet. Ještě před tím ale mírně redefinujme pojem báze, aby součástí definice bylo i uspořádání:

DEFINICE 18. Nechť $V \neq 0$ je vektorový prostor nad $\mathbb{F}$ konečné dimenze, pak posloupnost $B = (v_1, \dots, v_n)$ nazveme *bází* V, pokud pro každý vektor $v \in V$ existuje jednoznačně určený aritmetický vektor $[v]^B := (r_1, r_2, \dots, r_n)^T$ takový, že $v = \sum_{i=1}^{n} r_i v_i$. Bází prostoru 0 je prázdná posloupnost. Vektor $[v]^B$ nazýváme *reprezentace vektoru v vzhledem k bázi B*.

POZNÁMKA 3. Zavést bázi jako posloupnost bychom mohli i u některých prostorů nekonečné dimenze, jako je $P(x, \mathbb{R})$. Reprezentací polynomu $p(x) = \sum_{i=0}^{k} a_i x^i$ by pak nebyl aritmetický vektor, ale nekonečná posloupnost $(a_0, a_1, \dots, a_k, 0, 0, \dots)^T$. Protože lineární kombinace jsou vždy konečné součty, bude mít každá taková reprezentace pouze konečný počet nenulových složek.

Zatím hovoříme pouze o „prostorech konečné dimenze“ a „prostorech nekonečné dimenze“, ale samotný pojem dimenze definován nemáme. K tomu potřebujeme následující velmi důležitou větu:

VĚTA 2 (O počtu prvků báze). *Všechny báze vektorového prostoru V konečné dimenze mají stejný počet prvků.*

DEFINICE 19. Nechť V je vektorový prostor nad $\mathbb{F}$. Je-li V prostor konečné dimenze, pak definujeme nezáporné celé číslo $\dim V$ jako počet prvků libovolné báze V. Pokud není, píšeme $\dim V = \infty$. V obou případech nazýváme tuto hodnotu *dimenzí* vektorového prostoru V.

PŘÍKLADY 1.
- $\dim \mathbb{F}^n = n$
- V $\mathbb{F}^{m\times n}$ je báze např. $(E_{ij}, i \in \{1,\dots,m\}, j \in \{1,\dots,n\})$, kde E_{ij} označuje matici s jednou jedničkou na pozici ij a nulami všude jinde. Tedy $\dim \mathbb{F}^{m\times n} = mn$.
- Posloupnost
$$\left(\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}i\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}0\\i\end{pmatrix}\right)$$
je báze prostoru $\mathbb{C}^2$ nad $\mathbb{R}$. Obecně je dimenze $\mathbb{C}^n$ nad $\mathbb{R}$ rovna $2n$.
- Označme $U_n(\mathbb{F}) = \{A \in \mathbb{F}^{n\times n} | \forall i, j, i > j : a_{ij} = 0\}$ podprostor všech horních trojúhelníkových $n \times n$ matic. Pak $(E_{ij} | i, j \in \{1,\dots,n\}, j \geq i)$ je bází $U_n(\mathbb{F})$. Tedy $\dim U_n(\mathbb{F}) = 1 + 2 + \ldots + n = \frac{n(n+1)}{2}$
- Označme $P^n(x, \mathbb{F})$ podprostor všech polynomů stupně nejvýše n v $P(x, \mathbb{F})$. Jeho bází je třeba $(1, x, x^2, \dots, x^n)$, tedy $\dim P^n(x, \mathbb{F}) = n + 1$.

POZNÁMKA 4. Z teorie množin je známo, že nekonečné množiny mohou být spočetné nebo nespočetné. Má-li vektorový prostor spočetnou bázi, pak je možné tuto bázi seřadit do posloupnosti a zacházet s bázemi a reprezentacemi podobně jako u prostoru $P(x, \mathbb{R})$ výše. Prostory, které spočetnou bázi nemají, typicky prostory funkcí, se studují jinými metodami. Obvykle se na nich nějak zavede pojem normy vektoru, který podobně jako na $\mathbb{R}^n$ umožňuje definovat vzdálenost vektorů. Se vzdáleností máme definovanou i konvergenci posloupnosti vektorů a tedy i (některé) nekonečné lineární kombinace. Například k popisu prostoru všech spojitých reálných funkcí na uzavřeném intervalu $[0, 2\pi]$ je možné použít množinu funkcí $\{1\} \cup \{\cos nx | n \in \mathbb{N}\} \cup \{\sin nx | n \in \mathbb{N}\}$, jejíž konvergentní nekonečné lineární kombinace se nazývají Fourierovými řadami a samotná množina pak Fourierovou bází, ačkoli to dle naší definice báze daného vektorového prostoru není.

V tomto kurzu se od nynějška budeme zabývat pouze vektorovými prostory konečné dimenze, aniž bychom to nadále explicitně vypisovali. Tyto prostory ale mohou být zadány i jako podprostory nějakého prostoru dimenze nekonečné, jako například když je prostor $P^n(x, \mathbb{R})$ všech polynomů stupně nejvýše n podprostorem $P(x, \mathbb{R})$.

Věta o počtu prvků báze plyne z tzv. Steinitzova lemmatu o výměně:

LEMMA 1 (Steinitz). *Nechť V je vektorový prostor nad $\mathbb{F}$, M jeho n-prvková množina generátorů a $N = \{v_1, \dots, v_k\}$ lineárně nezávislá množina ve V. Pak $k \leq n$ a prvky M lze uspořádat do posloupnosti $(u_1, u_2, \dots, u_n)$ tak, že množina $\{v_1, \dots, v_k, u_{k+1}, \dots u_n\}$ generuje V.*

Nejprve ukažme, jak z lemmatu plyne věta:

DŮKAZ VĚTY. Označme $|M|$ počet prvků množiny M. Aplikujeme-li lemma na dvě báze B a C ve V, $|B| = p$, $|C| = q$, pak $p \leq q$, protože B je lineárně nezávislá a C generuje V. Zároveň i $q \leq p$, protože C je lineárně nezávislá a B generuje V. Tedy $p = q$. □

DŮKAZ LEMMATU. Budeme postupovat indukcí podle k. Pokud $k = 1$, pak $N = \{v_1\}$, kde $v_1 \neq 0$. Kdyby $n = 0$, je M prázdná množina, tedy $\langle M \rangle = 0$. Protože V obsahuje nenulový vektor v_1, není $M = \emptyset$ množinou generátorů V. Musí tedy být $n \geq 1 = k$, čímž je dokázána první část tvrzení.

Seřaďme M do posloupnosti $(u'_1, u'_2, \dots, u'_n)$. Protože M generuje V, existují čísla r'_i taková, že $v_1 = \sum_{i=1}^n r'_i u'_i$, a protože $v_1 \neq 0$, musí pro některý index j být $r'_j \neq 0$. Vyměňme v posloupnosti $(u'_1, u'_2, \dots, u'_n)$ prvek s indexem 1 a prvek s indexem j a označme nově uspořádanou posloupnost $(u_1, u_2, \dots, u_n)$, analogicky převeďme posloupnost koeficientů $(r'_1, \dots, r'_n)$ na posloupnost $(r_1, \dots, r_n)$ výměnou prvního a j-tého členu. Lze tedy psát

$$u_1 = -\frac{1}{r_1}\left(-v_1 + \sum_{i=2}^n r_i u_i\right)$$

Každý vektor, který je lineární kombinací vektorů z $\{u_1, \dots, u_n\}$, je tudíž také lineární kombinací vektorů z $\{v_1, u_2, \dots, u_n\}$, čili $\{v_1, u_2, \dots, u_n\}$ generuje V.

Nyní proveďme indukční krok, tedy předpokládejme, že $k > 1$ a tvrzení platí pro všechna přirozená čísla menší než k. Pokud $N = \{v_1, \dots, v_k\}$ je lineárně nezávislá, pak $\{v_1, \dots, v_{k-1}\}$ je lineárně nezávislá, a tudíž podle indukčního předpokladu $n \geq k-1$ a M lze uspořádat do posloupnosti $(u'_1, \dots, u'_n)$ tak, že $\{v_1, \dots, v_{k-1}, u'_k, \dots, u'_n\}$ generuje V. Kdyby $n = k - 1$, šlo by v_k zapsat jako lineární kombinaci vektorů $v_1, \dots, v_{k-1}$, což je spor s lineární nezávislostí N. Tedy $n \geq k$.

Vektor v_k lze pak zapsat jako

$$v_k = \sum_{i=1}^{k-1} r'_i v_i + \sum_{i=k}^{n} r'_i u'_i,$$

kde pro nějaké $j \geq k$ musí být $r'_j \neq 0$, jinak bychom opět dostali spor s lineární nezávislostí množiny $\{v_1, \dots, v_k\}$. Vyměňme v posloupnosti $(u'_1, \dots, u'_n)$ vektory k-tý a j-tý a označme toto nové uspořádání $(u_1, \dots, u_n)$, totéž s koeficienty lineární kombinace. Pak

$$u_k = -\frac{1}{r_k}\left(\sum_{i=1}^{k-1} r_i v_i - v_k + \sum_{i=k+1}^{n} r_i u_i\right)$$

Potom ale každý $v \in V$ je lineární kombinací vektorů z $\{v_1, \dots, v_k, u_{k+1}, \dots u_n\}$, a tedy tato množina generuje V. $\square$

PŘÍKLAD 9. Najděme bázi $W = \langle (1,1,1,1), (2,0,1,-1), (1,3,-3,1) \rangle$, která obsahuje vektory $(0,1,-2,0)$ a $(2,1,-1,-1)$. Nejprve ověříme, že

$$M := \{(1,1,1,1), (2,0,1,-1), (1,3,-3,1)\}$$

je báze W a vektory z $N := \{(0,1,-2,0), (2,1,-1,-1)\}$ jsou lineární kombinace jejích prvků (proveďte sami). Dle Steinitzova lemmatu lze v M nahradit dva vektory prvky lineárně nezávislé množiny N. Zkusme to konkrétně. Protože

$$(0,1,-2,0) = -\frac{1}{2}(1,1,1,1) + \frac{1}{2}(1,3,-3,1),$$

můžeme třeba nahradit $(1,3,-3,1)$ za $(0,1,-2,0)$. V druhém kole pak z rovnosti $(2,1,-1,-1) = (0,1,-2,0) + (2,0,1,-1)$ plyne, že za $(2,1,-1,-1)$ musíme vyjmout vektor $(2,0,1,-1)$. Získáváme tedy

$$W = \langle (0,1,-2,0), (2,1,-1,-1), (1,1,1,1) \rangle$$

Proč je posloupnost $((0,1,-2,0), (2,1,-1,-1), (1,1,1,1))$ báze W? Víme, že generuje, mohli bychom ověřit lineární nezávislost. Lepší ale bude opřít se o další důsledek Steinitzova lemmatu:

Důsledek 1. *Nechť V je vektorový prostor nad $\mathbb{F}$ dimenze n a $M \subset V$.*

(1) *Je-li M lineárně nezávislá, pak $|M| \leq n$.*
(2) *Pokud M generuje V, pak $|M| \geq n$*

Navíc platí-li v některém z případů $|M| = n$, pak je M bází V.

Důkaz. Pro první část stačí uvažovat nějakou bázi N prostoru V a použít ji v lemmatu jako množinu generátorů. Pokud navíc $|M| = |N|$, plyne z lemmatu, že $\langle M \rangle = \langle N \rangle = V$, a tedy že M je bází V. Pro druhou část naopak bude N hrát v lemmatu roli lineárně nezávislé množiny. Pokud $|M| = n$ a M by byla lineárně závislá, mohli bychom z ní vybrat bázi, která by musela mít méně než n prvků. To je ale v rozporu s Větou 2. □

Lemma 2. *Nechť V je vektorový prostor dimenze n a W jeho podprostor. Pak W je prostorem konečné dimenze a $\dim W \leq n$.*

Důkaz. Všechny lineárně nezávislé podmnožiny W jsou zároveň lineárně nezávislé podmnožiny V a mají tedy podle Důsledku 1 nanejvýš n prvků. Zvolme z nich nějakou $N = \{v_1, \dots, v_k\}$ s maximálním počtem prvků. Pokud by N negenerovala celé W, pak by existoval vektor $u \in W$, pro nějž $u \notin \langle N \rangle$. Každá netriviální lineární kombinace $ru + \sum_1^k s_i v_i = 0$ je v rozporu buď s $u \notin \langle N \rangle$, nebo s lineární nezávislostí množiny N, tedy $N \cup \{u\}$ je lineárně nezávislá podmnožina W. Má ale $k + 1$ prvků, což je ve sporu s předpokládanou maximalitou N. Tedy N generuje podprostor W, který má konečnou dimenzi $k \leq n = \dim V$. □

Podle dalšího důsledku lze bázi podprostoru vždy doplnit na bázi celého prostoru

Důsledek 2. *Nechť V je vektorový prostor dimenze n a W jeho podprostor, N báze W. Pak existuje množina $M \supset N$, která je bází V.*

Důkaz. Podle předchozího lemmatu je W prostor konečné dimenze a má tudíž bázi $N = \{v_1, \dots, v_k\}$. Zvolme ve V libovolnou bázi M, pak druhá část Steinitzova lemmatu říká, že množina $M' := \{v_1, \dots, v_k, u_{k+1}, \dots, u_n\}$, kde $u_{k+1}, \dots, u_n$ jsou nějaké prvky M, generuje V. Protože $|M'| = n$, musí to být dle Důsledku 1 báze V. □

Bude se nám hodit rozšířit pojem elementární úpravy (EÚ) z posloupnosti řádků nějaké matice na libovolnou posloupnost jakýchkoli vektorů. Řekneme, že posloupnost vznikne *elementární úpravou* posloupnosti vektorů $M = (v_1, \dots, v_m)$ z vektorového prostoru V nad $\mathbb{F}$, pokud má jeden z následujících tvarů:

$$\begin{aligned} M_1 =& (v_1, \dots, v_{k-1}, v_j, v_{k+1}, \dots, v_{j-1}, v_k, v_{j+1}, \dots, v_m) \\ M_2 =& (v_1, \dots, v_{k-1}, v_k + s v_j, v_{k+1}, \dots, v_m) \\ M_3 =& (v_1, \dots, v_{k-1}, r v_k, v_{k+1}, \dots, v_m) \end{aligned}$$

kde $r, s \in \mathbb{F}$, $r \neq 0$, $j, k \in \{1, \dots, m\}$, $j \neq k$.

Tvrzení 19. *Nechť C je posloupnost vektorů ve vektorovém prostoru V nad $\mathbb{F}$ a posloupnost D z ní vznikne elementární úpravou. Pak platí*

(1) *lineární obaly C a D jsou stejné*
(2) *C je lineárně nezávislá, právě když D je lineárně nezávislá*
(3) *C je bází V, právě když D je bází V*

Důkaz. Protože EÚ jsou vratné opět pomocí EÚ, stačí dokázat jen to, že každý prvek V, který lze vyjádřit jako lineární kombinaci prvků C, lze vyjádřit i jako lineární kombinaci prvků D. Uvažujme elementární úpravu typu 2 a $v =$

$\sum_{i=1}^{m} r_i v_i \in \langle C \rangle$. Pro pohodlnější zápis předpokládejme $k < j$. Pak lze sumu přepsat jako

$$v = \sum_{i=1}^{k-1} r_i v_i + r_k(v_k + s v_j) + \sum_{i=k+1}^{j-1} r_i v_i + (r_j - s r_k) v_j + \sum_{i=j+1}^{m} r_i v_i, \tag{1}$$

tedy v je lineární kombinací vektorů z D. Pro ostatní typy EÚ je postup analogický.

Dále ukážeme, že je-li D lineárně nezávislá, pak musí být i C. Uvažme nějaké vyjádření nulového vektoru ve tvaru lineární kombinace prvků C: $o = \sum_{i=1}^{n} r_i v_i$. Pravou stranu přepišme do stejného tvaru jako v rovnici 1. Z lineární nezávislosti D plyne, že všechny koeficienty v této lineární kombinaci jsou nulové. To ale znamená $r_i = 0$, pokud i není k ani j, dále $r_k = 0$, a díky tomu $r_j = r_j - s r_k = 0$. Tedy lineární kombinace $\sum_{i=1}^{m} r_i v_i$ musí být triviální, a tedy C je lineárně nezávislá. Ostatní typy EÚ opět přenecháváme čtenáři. $\square$

PŘÍKLAD 10. Určeme dimenzi lineárního obalu množiny $M = \{(3,-6,1,-1), (1,-2,3,1), (-2,4,0,1), (0,0,2,1)\}$ v $\mathbb{R}^4$. Sestavíme matici, která má tyto vektory jako řádky, a provádějme EŘÚ:

$$\begin{pmatrix} 1 & -2 & 3 & 1 \\ 3 & -6 & 1 & -1 \\ -2 & 4 & 0 & 1 \\ 0 & 0 & 2 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & -2 & 3 & 1 \\ 0 & 0 & -8 & -4 \\ 0 & 0 & 6 & 3 \\ 0 & 0 & 2 & 1 \end{pmatrix} \sim$$
$$\begin{pmatrix} 1 & -2 & 3 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 6 & 3 \\ 0 & 0 & -8 & -4 \end{pmatrix} \sim \begin{pmatrix} 1 & -2 & 3 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Řádky poslední matice jsou LZ, tedy i M je LZ. Lineární obal řádků se také zachovává, tedy $\langle M \rangle$ je roven lineárnímu obalu LN množiny $\{(1,-2,3,1),(0,0,2,1)\}$. Proto $\dim\langle M \rangle = 2$.

KAPITOLA 6

Hodnost matice

V této kapitole se vrátíme k maticím a soustavám lineárních rovnic. Elementy matic a koeficienty soustav lineárních rovnic budou prvky množiny skalárů $\mathbb{F}$. Všechny definice z kapitol 2 a 3 zůstávají stejné i pro matice z $\mathbb{F}^{m\times n}$, máme tedy definován součet a součin matic, nulovou matici, jednotkovou matici, pojem matice transponované, inverzní, čtvercové a regulární, matice elementární řádkové úpravy 5. Snadno se zobecní i všechna tvrzení, která jsme o těchto pojmech dokázali, tedy asociativita 4 a distributivita 5 maticových operací, nutná a postačující podmínka existence inverzní matice 12 i fakt, že Gaussova eliminace dovede každou matici do redukovaného odstupňovaného tvaru.

Stejně se definují i jádro a obraz matice:

Definice 20. Nechť $A = (\mathbf{a}_1|\ldots\mathbf{a}_n) \in \mathbb{F}^{m\times n}$, kde $\mathbf{a}_i \in \mathbb{F}^m$. Pak *jádrem matice* A rozumíme podprostor

$$\operatorname{Ker} A = \{\mathbf{x} \in \mathbb{F}^n | A\mathbf{x} = \mathbf{o}\} \leq \mathbb{F}^n$$

a jejím *obrazem* nebo též *sloupcovým prostorem* pak

$$\operatorname{Im} A = \langle \mathbf{a}_1, \ldots, \mathbf{a}_n \rangle \leq \mathbb{F}^m$$

Důkaz, že $\operatorname{Ker} A$ je podprostorem $\mathbb{F}^n$ je stejný jako v tvrzení 11. $\operatorname{Im} A$ lze definovat i jako obor hodnot zobrazení F_A. Protože $F_A(\mathbf{x}) = A\mathbf{x} = \sum_{i=1}^n x_i\mathbf{a}_i$, je vektor $\mathbf{y} \in \mathbb{F}^m$ v oboru hodnot F_A, právě když je v lineárním obalu sloupců matice A.

Transponování převádí řádky na sloupce, můžeme proto označit podprostor $\operatorname{Im} A^T \leq \mathbb{F}^n$, čili lineární obal řádků matice A, jako její *řádkový prostor*. Čtveřici význačných podprostorů, jejichž vlastnostmi se v této kapitole budeme zabývat, doplňuje *jádro transponované matice* $\operatorname{Ker} A^T \leq \mathbb{F}^m$.

Elementární řádkovou úpravu matice lze realizovat násobením elementární maticí zleva. Elementární matice jsou regulární a stejně tak jsou i součiny elementárních matic mezi sebou. Následující tvrzení tedy jen zobecňuje již dokázané vlastnosti elementárních úprav, totiž že zachovávají množinu řešení homogenní soustavy rovnic (tvrzení 8 to říká dokonce i pro nehomogenní) a řádkový prostor (první bod tvrzení 19):

Tvrzení 20. *Nechť $A = (\mathbf{a}_1|\ldots\mathbf{a}_n) \in \mathbb{F}^{m\times n}$, $R \in \mathbb{F}^{m\times m}$ regulární. Pak*

(1) $\operatorname{Ker}(RA) = \operatorname{Ker} A$
(2) $\operatorname{Im}(RA)^T = \operatorname{Im} A^T$

Důkaz. Pokud $A\mathbf{x} = \mathbf{o}$, pak $RA\mathbf{x} = R\mathbf{o} = \mathbf{o}$, tedy $\operatorname{Ker} A \subset \operatorname{Ker} RA$. Protože R je regulární, existuje k ní inverzní matice R^{-1}, která je také regulární. Pak $\operatorname{Ker} RA \subset \operatorname{Ker} R^{-1}(RA) = \operatorname{Ker} A$. Tím je dokázána i opačná implikace.

Každý řádek matice RA je lineární kombinací řádků matice A s koeficienty v řádcích matice R, tedy $\operatorname{Im}(RA)^T \subset \operatorname{Im} A^T$. Druhá inkluze plyne opět z $A = R^{-1}(RA)$. □

Elementární sloupcové úpravy (ESÚ) lze definovat jako ty, které lze realizovat násobením elementární maticí zprava. Opět je jednodušší vzít místo elementární matice libovolnou regulární a dokázat, že násobení zprava nemění sloupcový prostor a jádro transponované matice:

Tvrzení 21. *Nechť* $A = (\mathbf{a}_1|\dots\mathbf{a}_n) \in \mathbb{F}^{m\times n}$, $Q \in \mathbb{F}^{n\times n}$ *regulární. Pak*
(1) $\operatorname{Ker}(AQ)^T = \operatorname{Ker} A^T$
(2) $\operatorname{Im}(AQ) = \operatorname{Im} A$

Na příkladu

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

je vidět, že $\operatorname{Im}(RA)$ a $\operatorname{Im} A$ se rovnat nemusejí a stejně tak $\operatorname{Ker}(RA)^T$ a $\operatorname{Ker} A^T$. Řádkové úpravy tedy sloupcový prostor nezachovávají. Ukážeme ale, že zachovávají jeho dimenzi. První část tvrzení 20 můžeme přeformulovat jako

Lemma 3. *Nechť* $A = (\mathbf{a}_1|\dots\mathbf{a}_n) \in \mathbb{F}^{m\times n}$, $R \in \mathbb{F}^{m\times m}$ *regulární. Označme* $RA =: A' = (\mathbf{a}'_1|\dots\mathbf{a}'_n)$. *Je-li* $(s_1,\dots,s_n) \in \mathbb{F}^n$, *pak* $\sum_{i=1}^n s_i\mathbf{a}_i = \mathbf{o}$, *právě když* $\sum_{i=1}^n s_i\mathbf{a}'_i = \mathbf{o}$.

Důsledek 3. *Nechť* A, A' *jsou dvě matice,* $A \sim A'$. *Pak* $\dim \operatorname{Im} A = \dim \operatorname{Im} A'$.

Důkaz. Z lemmatu 3 plyne, že nějaká podposloupnost $(\mathbf{a}_{i_1}, \mathbf{a}_{i_2}, \dots, \mathbf{a}_{i_k})$ sloupců matice A, kde $i_1 < \dots < i_k$, je lineárně nezávislá, právě když je lineárně nezávislá odpovídající podposloupnost $(\mathbf{a}'_{i_1}, \mathbf{a}'_{i_2}, \dots, \mathbf{a}'_{i_k})$ sloupců A'. Maximální takové lineárně nezávislé podposloupnosti jsou bázemi $\operatorname{Im} A$, resp. $\operatorname{Im} A'$, a počet prvků takových bází je roven $\dim \operatorname{Im} A = \dim \operatorname{Im} A'$. □

Věta 3. *Pro každou matici* $A \in \mathbb{F}^{m\times n}$ *platí* $\dim \operatorname{Im} A = \dim \operatorname{Im} A^T$.

Důkaz. Matici A lze převést posloupností EŘÚ na redukovaný odstupňovaný tvar A'. Posloupnost všech nenulových řádků A' je lineárně nezávislá, a je tedy bází $\operatorname{Im} A'^T$. Množina všech pivotních sloupců A' je lineárně nezávislá a nepivotní sloupce jsou lineárními kombinacemi sloupců pivotních. Tedy posloupnost všech pivotních sloupců je bází $\operatorname{Im} A'$. Pivotních sloupců i nenulových řádků A' je stejně, tedy $\dim \operatorname{Im} A' = \dim \operatorname{Im} A'^T$. Protože řádkové úpravy $A \sim A'$ zachovávají řádkový prostor, platí $\operatorname{Im} A^T = \operatorname{Im} A'^T$. Z důsledku 3 máme $\dim \operatorname{Im} A = \dim \operatorname{Im} A'$, celkově tedy $\dim \operatorname{Im} A = \dim \operatorname{Im} A^T$. □

Na tvrzení je zajímavé, že nám dává rovnost dimenzí dvou podprostorů ve dvou obecně různých aritmetických vektorových prostorech, protože $\operatorname{Im} A \le \mathbb{F}^m$, ale $\operatorname{Im} A^T \le \mathbb{F}^n$. Je to vidět i na příkladu

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix},$$

kde je bází $\operatorname{Im} A$ jednoprvková posloupnost $((1,1))$ a bází $\operatorname{Im} A^T$ posloupnost $((1,0,1))$. Jednoduchý důsledek věty 3 je tedy , že pokud jsou v matici všechny řádky násobkem jednoho z nich, pak jsou i všechny sloupce násobkem jednoho z nich.

Definice 21. Nechť $A \in \mathbb{F}^{m\times n}$. Číslo $\dim \operatorname{Im} A \equiv \dim \operatorname{Im} A^T$ nazýváme *hodnost* matice A, značíme $\operatorname{rank}(A)$.

Tvrzení 22. *Nechť* $A \in \mathbb{F}^{m\times n}$, $R \in \mathbb{F}^{p\times m}$, $Q \in \mathbb{F}^{n\times q}$. *Pak*
(1) $\operatorname{rank}(RA) \le \operatorname{rank}(A)$ *a pokud* $p = m$ *a* R *je regulární,* $\operatorname{rank}(RA) = \operatorname{rank}(A)$
(2) $\operatorname{rank}(AQ) \le \operatorname{rank}(A)$ *a pokud* $n = q$ *a* Q *je regulární,* $\operatorname{rank}(AQ) = \operatorname{rank}(A)$
(3) $\operatorname{rank}(A) = \operatorname{rank}(A^T)$

Důkaz. Protože řádky RA patří do lineárního obalu řádků A, musí být $\operatorname{rank}(RA) \leq \operatorname{rank}(A)$. Protože R je regulární, existuje inverzní matice R^{-1}, která je rovněž regulární. Platí pak $\operatorname{rank}(R^{-1}(RA)) \leq \operatorname{rank}(RA)$, z čehož plyne i opačná nerovnost. Druhý bod se dokáže analogicky, třetí plyne z věty 3. □

Důsledkem tvrzení je nerovnost

$$\operatorname{rank}(AB) \leq \min\{\operatorname{rank}(A), \operatorname{rank}(B)\}$$

a rovnost

$$\operatorname{rank}(ABC) = \operatorname{rank}(B), \text{ pro } A, C \text{ regulární.}$$

Hodnost se tedy dá určovat tak, že kombinací řádkových a sloupcových úprav převedeme matici do tvaru, v němž je možné ji určit snadněji, typicky do odstupňovaného. Hodnost nese o matici a o příslušném zobrazení mnoho informací:

Věta 4. *Nechť $A \in \mathbb{F}^{n\times n}$. Pak jsou následující tvrzení ekvivalentní*

(1) *A je regulární*
(2) $\operatorname{rank}(A) = n$
(3) *množina všech řádků A je lineárně nezávislá*
(4) *množina všech řádků A generuje $\mathbb{F}^n$*
(5) *posloupnost všech řádků A je bází $\mathbb{F}^n$*
(6) *množina všech sloupců A je lineárně nezávislá*
(7) *množina všech sloupců A generuje $\mathbb{F}^n$*
(8) *posloupnost všech sloupců A je bází $\mathbb{F}^n$*
(9) $\operatorname{Im} A = \mathbb{F}^n$
(10) $\operatorname{Ker} A = 0$
(11) *zobrazení F_A je prosté*
(12) *zobrazení F_A je na*
(13) *zobrazení F_A je bijektivní*
(14) *existuje $X \in \mathbb{F}^{n\times n}$, pro kterou $AX = E$.*
(15) *existuje $X \in \mathbb{F}^{n\times n}$, pro kterou $XA = E$.*

Důkaz. Dokážeme řetězec implikací, který propojí všechna tvrzení oběma směry.

$1 \Rightarrow 2$ Je-li A regulární, pak existuje regulární matice A^{-1} splňující $A^{-1}A = E$. Násobení regulární maticí nemění hodnost a $\operatorname{rank}(E) = n$, tedy $\operatorname{rank}(A) = n$.

$2 \Rightarrow 3$ Protože $\dim \operatorname{Im} A^T = \operatorname{rank}(A) = n$, tvoří řádky A n-prvkovou množinu generátorů vektorového prostoru dimenze n. Ta je podle důsledku 1 jeho bází a tudíž je lineárně nezávislá.

$3 \Rightarrow 5$ Množina řádků A je n-prvková lineárně nezávislá podmnožina v $\mathbb{F}^n$, tedy je dle důsledku 1 i jeho bází.

$4 \Rightarrow 5$ Množina řádků A je n-prvková množina generátorů $\mathbb{F}^n$, tedy je dle důsledku 1 i jeho bází.

$2 \Rightarrow 6$ se dokáže podobně jako $2 \Rightarrow 3$. Analogicky máme i $6 \Rightarrow 8$ a $7 \Rightarrow 8$. Implikace $5 \Rightarrow 3$, $5 \Rightarrow 4$, $4 \Rightarrow 2$, $8 \Rightarrow 6$, $8 \Rightarrow 7$, $7 \Rightarrow 2$ plynou z definic. Také je $7 \Leftrightarrow 9 \Leftrightarrow 12$, $6 \Leftrightarrow 10 \Leftrightarrow 11$. Odtud plyne ekvivalence výroků 6 až 12 s výrokem 13.

$13 \Rightarrow 14$ Plyne z tvrzení 12.

$14 \Rightarrow 15$ Je dokázáno v druhé části důkazu 12. Z definice regularity matice pak $14 \Rightarrow 1$.

$15 \Rightarrow 4$ Řádky XA jsou lineárními kombinacemi řádků matice A, lze tedy v lineárním obalu řádků A najít libovolný vektor kanonické báze $\mathbb{F}^n$ a tedy i libovolný vektor $\mathbb{F}^n$.

□

VĚTA 5 (O dimenzi jádra a obrazu). *Nechť* $A \in \mathbb{F}^{m \times n}$. *Pak*

$$\dim \operatorname{Ker} A + \dim \operatorname{Im} A = n$$

DŮKAZ. Pro nulovou matici je tvrzení triviální, předpokládejme tedy $A \neq 0$. Matici A je možné převést pomocí EŘÚ do redukovaného odstupňovaného tvaru, tím se zachovává jak $\operatorname{Ker} A$, tak $\dim \operatorname{Im} A$. Dále vynechejme všechny nulové řádky (ani tím se $\operatorname{Ker} A$ ani $\dim \operatorname{Im} A$ nezmění) a označme výslednou matici A'. Označme $k_1 < k_2 < \ldots < k_r$ sloupcové indexy pivotních sloupců A', tedy $\mathbf{a}'_{k_i} = \mathbf{e}_i \in \mathbb{F}^r$. Označme sloupcové indexy nepivotních sloupců $j_1 < j_2 < \ldots < j_p$, a tyto sloupce samotné $\mathbf{c}_i := \mathbf{a}'_{j_i}$. Uvažujme vektor $\mathbf{x} \in \mathbb{F}^n$, jehož složky s indexy j_1 až j_p jsou zvoleny libovolně. Pokud $A'\mathbf{x} = 0$, pak

$$\sum_{s=1}^{r} x_{k_s} \mathbf{e}_s + \sum_{q=1}^{p} x_{j_q} \mathbf{c}_q = \mathbf{o},$$

neboli

$$\begin{pmatrix} x_{k_1} \\ \vdots \\ x_{k_r} \end{pmatrix} = -\sum_{q=1}^{p} x_{j_q} \mathbf{c}_q$$

Tím jsou určeny všechny zbývající složky vektoru $\mathbf{x}$. Definujme pro každé $i \in \{1, \ldots, p\}$ vektor $\mathbf{u}_i \in \mathbb{F}^n$ tak, že pro každé $q \in \{1, \ldots, p\}$ je jeho j_q-tá složka rovna q-té složce vektoru $\mathbf{e}_i \in \mathbb{F}^p$, a pro každé $s \in \{1, \ldots, r\}$ je jeho k_s-tá složka rovná s-té složce vektoru $-\mathbf{c}_i \in \mathbb{F}^r$. Pak $\mathbf{x} = \sum_{q=1}^{p} x_{j_q} \mathbf{u}_q$, tedy posloupnost $M = (\mathbf{u}_1, \ldots, \mathbf{u}_p)$ generuje $\operatorname{Ker} A'$. Zároveň, pokud by $\sum_{q=1}^{p} y_q \mathbf{u}_q = \mathbf{o}$, musí být každý koeficient y_q roven nule, neboť se rovná j_q-té složce vektoru $\sum_{q=1}^{p} y_q \mathbf{u}_q$. Tedy M je lineárně nezávislá. Musí být tedy bází $\operatorname{Ker} A$, $\dim \operatorname{Ker} A' = p$. Protože $\dim \operatorname{Im} A' = r$ a $p + r = n$, dostáváme odtud tvrzení věty. $\square$

Konstrukce báze M je názornější, pokud $k_s = s$, $j_q = r + q$, tedy pokud jdou v A' nejprve sloupce pivotní a pak nepivotní:

$$A' = \begin{pmatrix} 1 & 0 & \ldots & 0 & c_{11} & c_{12} & \ldots & c_{1p} \\ 0 & 1 & \ldots & 0 & c_{21} & c_{22} & \ldots & c_{2p} \\ \vdots & & \ddots & \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \ldots & 1 & c_{r1} & c_{r2} & \ldots & c_{rp} \end{pmatrix}$$

Báze jádra pak má tvar

$$\begin{aligned} M = \{&(-c_{11}, -c_{21}, \ldots, -c_{r1}, 1, 0, \ldots, 0) \\ &(-c_{12}, -c_{22}, \ldots, -c_{r2}, 0, 1, \ldots, 0) \\ &\vdots \\ &(-c_{1p}, -c_{2p}, \ldots, -c_{rp}, 0, 0, \ldots, 1)\} \end{aligned}$$

Dimenze jádra A se nazývá *nulita* (též *defekt*) matice, značí se $n(A)$. Věta o dimenzi jádra a obrazu je proto známá též pod názvem věta o hodnosti a nulitě:

$$\forall A \in \mathbb{F}^{m \times n} : \operatorname{rank}(A) + n(A) = n$$

Plyne z ní například

TVRZENÍ 23. *Nechť* $A \in \mathbb{R}^{m \times n}$. *Pak* $\operatorname{Ker} A^T A = \operatorname{Ker} A$ *a* $\operatorname{rank} A^T A = \operatorname{rank} A$.

DŮKAZ. Pokud $A\mathbf{x} = \mathbf{o}$, pak jistě $A^T A\mathbf{x} = \mathbf{o}$, tedy $\operatorname{Ker} A \leq \operatorname{Ker} A^T A$. Pokud $A^T A \mathbf{x} = \mathbf{o}$, pak $\mathbf{x}^T A^T A \mathbf{x} = 0$. Označme $\mathbf{y} := A\mathbf{x}$, pak $\mathbf{y}^T = \mathbf{x}^T A^T$ a tedy $0 = \mathbf{y}^T \mathbf{y} = \sum_{i=1}^{m} y_i^2$. Musí tedy být $\mathbf{y} = 0$, neboli $\mathbf{x} \in \operatorname{Ker} A$. Tím je dokázána druhá inkluze. Protože počet sloupců $A^T A$ je stejný jako počet sloupců A, plyne odsud rovnost hodností. $\square$

Tvrzení platí jen pro **reálné** matice. Kde selže důkaz pro $A \in \mathbb{C}^{m\times n}$? Jak by se muselo upravit tvrzení, aby důkaz prošel?

Pomocí hodnosti matice se dá také formulovat kritérium řešitelnosti SLR:

VĚTA 6 (Frobeniova). *Nechť* $A \in \mathbb{F}^{m\times n}$, $\mathbf{b} \in \mathbb{F}^m$. *Soustava* $A\mathbf{x} = \mathbf{b}$ *má řešení, právě když* $\operatorname{rank}(A) = \operatorname{rank}(A|b)$.

DŮKAZ. Soustava má řešení, právě když je $\mathbf{b} \in \operatorname{Im} A$, což nastává právě když $\operatorname{Im}(A|b) = \operatorname{Im}(A)$. Protože $\operatorname{Im} A \leq \operatorname{Im}(A|b)$, nastane toto právě když se rovnají dimenze. $\square$

Pomocí hodnosti se dá formulovat i to, kolik řešení soustava má. Víme, že množina všech řešení soustavy $A\mathbf{x} = \mathbf{b}$ je afinní podprostor $\mathbb{F}^n$ ve tvaru

$$\mathbf{x}_P + \operatorname{Ker} A$$

Z věty o hodnosti a nulitě víme, že dimenze $\operatorname{Ker} A$ je $n - \operatorname{rank}(A)$.

KAPITOLA 7

Reprezentace vektoru a lineárního zobrazení

V definici 18 jsme zavedli pojem báze a reprezentace vektoru vůči bázi. Reprezentaci vzhledem k bázi $B = (v_1, \dots, v_n)$ prostoru V nad $\mathbb{F}$ dimenze n lze chápat jako zobrazení $[\ ]^B : V \to \mathbb{F}^n$, které vektoru $v = \sum_{i=1}^n r_i v_i \in V$ přiřadí aritmetický vektor

$$[v]^B := \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix} \in \mathbb{F}^n$$

Toto zobrazení splňuje důležitou vlastnost:

Tvrzení 24. *Nechť V je vektorový prostor $\mathbb{F}$ konečné dimenze, B jeho báze, $u, v \in V$, $r, s \in \mathbb{F}$. Pak $[ru + sv]^B = r[u]^B + s[v]^B$.*

Důkaz. Nechť $B = (v_1, \dots, v_n)$, $u = \sum_{i=1}^n r_i v_i$, $v = \sum_{i=1}^n s_i v_i$. Pak

$$[ru+sv]^B = \left[r\sum_{i=1}^n r_i v_i + s\sum_{i=1}^n s_i v_i \right]^B = \left[\sum_{i=1}^n (rr_i + ss_i) v_i \right]^B =$$
$$= (rr_1 + ss_1, \dots, rr_n + ss_n)^T = r(r_1, \dots, r_n)^T + s(s_1, \dots, s_n)^T = r[u]^B + s[v]^B$$

□

Stejnou vlastnost jsme viděli poprvé v tvrzení 3 v první kapitole, kde se týkala zobrazení ortogonální projekce $P_{\mathbf{x}}$, a posléze i u dalších zobrazení. Definujme ji nyní obecně:

Definice 22. Nechť V, W jsou dva vektorové prostory nad $\mathbb{F}$ a $f : V \to W$ je zobrazení splňující $\forall r, s \in \mathbb{F}$, $\forall u, v \in V$

$$f(ru + sv) = rf(u) + sf(v)$$

Takové f nazýváme *lineární zobrazení.*

Označme o_V nulový vektor ve V a o_W nulový vektor ve W.

Důsledek 4. *Nechť V, W jsou dva vektorové prostory nad $\mathbb{F}$ a $f : V \to W$ je lineární zobrazení. Pak*

(1) $\forall u, v \in V : f(u + v) = f(u) + f(v)$
(2) $\forall u \in V$, $\forall r \in \mathbb{F}$: $f(ru) = rf(u)$.
(3) $f(o_V) = o_W$
(4) $\forall v \in V$: $f(-v) = -f(v)$

Důkaz. Volíme v definici lineárního zobrazení postupně $r = s = 1$; $s = 0$; $r = s = 0$; $r = 0$, $s = -1$ a využíváme základní vlastnosti vektorového prostoru. □

Příklady 2. Kromě $[\ ]^B$ a příkladů uvedených v první kapitole uveďme ještě několik dalších:

- Pokud $A \in \mathbb{F}^{m \times n}$ je matice, pak zobrazení $F_A : \mathbb{F}^n \to \mathbb{F}^m$ zavedené stejně jako v první kapitole předpisem $F_A(\mathbf{x}) = A\mathbf{x}$, je lineární.

- Zobrazení výše můžeme snadno zobecnit na zobrazení $f : \mathbb{F}^{n\times k} \to \mathbb{F}^{m\times k}$, $f(X) = AX$ mezi prostory matic.
- Zobrazení $g : P^n(x,\mathbb{R}) \to P^{n-1}(x,\mathbb{R})$, které přiřazuje polynomu $p(x)$ jeho první derivaci $\frac{d}{dx}p(x)$, je také lineární.
- Zobrazení $h : F(\mathbb{R},\mathbb{R}) \to \mathbb{R}$, které přiřazuje funkci $\phi \in F(\mathbb{R},\mathbb{R})$ její hodnotu v nějakém bodě, např $h(\phi) = \phi(7)$, je rovněž lineární.

V úvodní kapitole jsme vyvodili, že lineárnímu zobrazení $f : \mathbb{F}^n \to \mathbb{F}^m$ můžeme přiřadit matici $A = (\mathbf{a}_1|\dots|\mathbf{a}_n)$, jejíž i-tý sloupec je obrazem i-tého vektoru kanonické báze, tedy $f(\mathbf{e}_i) = \mathbf{a}_i$. Tuto úvahu můžeme rozšířit na obecné lineární zobrazení:

Definice 23. Nechť V, W jsou dva vektorové prostory nad $\mathbb{F}$, $f : V \to W$ je lineární zobrazení, $B = (v_1,\dots,v_n)$ je báze V, $C = (w_1,\dots,w_m)$ je báze W. Pak matici

$$[f]_B^C := \big([f(v_1)]^C \big| [f(v_2)]^C \big| \dots \big| [f(v_n)]^C\big)$$

nazýváme *reprezentací lineárního zobrazení f vzhledem k bázím B a C.*

Zvolíme-li za B a C kanonické báze $K_n = (\mathbf{e}_1,\dots,\mathbf{e}_n)$ v $\mathbb{F}^n$, resp. $K_m = (\mathbf{e}_1,\dots,\mathbf{e}_m)$ v $\mathbb{F}^m$, vidíme, že

$$[f]_{K_n}^{K_m} = ([f(\mathbf{e}_1)]^{K_m}|[f(\mathbf{e}_2)]^{K_m}|\dots|[f(\mathbf{e}_n)]^{K_m}) = (f(\mathbf{e}_1)|f(\mathbf{e}_2)|\dots|f(\mathbf{e}_n))$$

Pro zobrazení F_A mezi aritmetickými vektorovými prostory je tedy matice A tohoto zobrazení podle definice v první kapitole rovna reprezentaci $[F_A]_{K_n}^{K_m}$ zobrazení F_A vzhledem ke kanonickým bázím.

Příklad 11. Uvažujme zobrazení $g : P^2(x,\mathbb{R}) \to P^1(x,\mathbb{R})$, $g(p(x)) = \frac{d}{dx}p(x)$, a báze $B = \{1, x, x^2\} \subset P^2(x,\mathbb{R})$, $C = \{1, x\} \subset P^1(x,\mathbb{R})$. Reprezentace obecného prvku prostoru $P^2(x,\mathbb{R})$ vzhledem k bázi B je

$$[ax^2 + bx + c]^B = \begin{pmatrix} c \\ b \\ a \end{pmatrix}$$

Obrazy prvků báze B (čili derivace monomů) jsou

$$g(1) = 0, \qquad g(x) = 1, \qquad g(x^2) = 2x$$

a jejich reprezentace vzhledem k bázi C jsou

$$[g(1)]^C = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \qquad [g(x)]^C = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad [g(x^2)]^C = \begin{pmatrix} 0 \\ 2 \end{pmatrix},$$

tedy reprezentace g vzhledem k B a C je $[g]_B^C = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$.

Příklad 12. Uvažujme lineární zobrazení $F_A : \mathbb{R}^2 \to \mathbb{R}^3$, dané předpisem

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \equiv A\mathbf{x}$$

Pokud K_n označuje kanonickou bázi v $\mathbb{F}^n$, pak $[F_A]_{K_2}^{K_3} = A$. Zvolme jiné báze než kanonické: $B = ((1,2)^T, (1,3)^T)$, $C = ((1,1,0)^T, (1,0,0)^T, (1,0,1)^T)$. Určíme

$$F_A\left(\begin{pmatrix} 1 \\ 2 \end{pmatrix}\right) = \begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix}, F_A\left(\begin{pmatrix} 1 \\ 3 \end{pmatrix}\right) = \begin{pmatrix} 4 \\ 1 \\ 1 \end{pmatrix}$$

Zbývá najít reprezentaci obou vektorů vzhledem k C

$$\left(\begin{array}{ccc|cc} 1 & 1 & 1 & 3 & 4 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 2 & 2 \\ 0 & 0 & 1 & 0 & 1 \end{array}\right) \Rightarrow [F_A]_B^C = \begin{pmatrix} 1 & 1 \\ 2 & 2 \\ 0 & 1 \end{pmatrix}$$

TVRZENÍ 25. *Nechť V, W jsou dva vektorové prostory nad $\mathbb{F}$, $f : V \to W$ lineární zobrazení, B báze V, C báze W, $v \in V$. Pak*

$$[f(v)]^C = [f]_B^C [v]^B$$

.

DŮKAZ. Označme $B = (v_1, \dots, v_n)$ a zapišme $v = \sum_{i=1}^n r_i v_i$, kde $(r_1, \dots, r_n)^T = [v]^B$, pak

$$[f(v)]^C = \left[\sum_{i=1}^n r_i f(v_i)\right]^C = \sum_{i=1}^n r_i [f(v_i)]^C = [f]_B^C [v]^B$$

Nejprve jsme využili linearitu f, pak linearitu $[\ ]^C$ a nakonec definici součinu matice a vektoru. □

Bijektivní lineární zobrazení se nazývá *izomorfismus*. S tímto pojmem jsme se setkali už v kapitole 3, a ve větě 4 jsme ukázali, že F_A je izomorfismus, právě když A je regulární matice. To se dá snadno zobecnit. Nejprve ale potřebujeme dokázat některé vlastnosti izomorfismů:

TVRZENÍ 26. *Nechť V, W jsou vektorové prostory nad $\mathbb{F}$, $f : V \to W$ je izomorfismus a $(v_1, \dots, v_n)$ je posloupnost vektorů ve V. Pak*

1. *$(v_1, \dots, v_n)$ je lineárně nezávislá, právě když $(f(v_1), \dots, f(v_n))$ je lineárně nezávislá.*
2. *$(v_1, \dots, v_n)$ generuje V, právě když $(f(v_1), \dots, f(v_n))$ generuje W.*
3. *$(v_1, \dots, v_n)$ je báze V, právě když $(f(v_1), \dots, f(v_n))$ je báze W.*

DŮKAZ. Označme o_V nulový vektor ve V a o_W nulový vektor ve W. Pokud $\sum_{i=1}^n r_i v_i = o_V$, pak i $\sum_{i=1}^n r_i f(v_i) = o_W$. Je-li tedy $(f(v_1), \dots, f(v_k))$ lineárně nezávislá, musí být všechna $r_i = 0$, tedy $(v_1, \dots, v_k)$ je také lineárně nezávislá. Nechť naopak $\sum_{i=1}^n r_i f(v_i) = o_W$, pak z linearity zobrazení f plyne $f(\sum_{i=1}^n r_i v_i) = o_W$. Protože také $f(o_V) = o_W$ a f je prosté, musí být $\sum_{i=1}^n r_i v_i = o_V$. Je-li $(v_1, \dots, v_n)$ lineárně nezávislá, znamená to, že všechna r_i jsou nulová, tedy i $(f(v_1), \dots, f(v_n))$ je lineárně nezávislá. Tím jsme ukázali opě implikace, které dohromady dávají tvrzení v prvním bodě.

Protože f je na, existuje ke každému $w \in W$ vektor $v \in V$ takový, že $f(v) = w$. Pokud $(v_1, \dots, v_n)$ generuje V, pak existují r_i taková, že $v = \sum_{i=1}^n r_i v_i$. Pak ale z linearity dostáváme, že $w = \sum_{i=1}^n r_i f(v_i)$, tedy $(f(v_1), \dots, f(v_n))$ generuje W. Naopak, je-li $v \in V$, $w = f(v)$ a $w = \sum_{i=1}^n r_i f(v_i)$, pak z linearity $f(v - \sum_{i=1}^n r_i v_i) = o_W$. Protože f je prosté, znamená to, že $v = \sum_{i=1}^n r_i v_i$, tedy $(v_1, \dots, v_n)$ generuje V. Tím je dokázán druhý bod.

Třetí bod plyne z prvního a druhého. □

DŮSLEDEK 5. *Nechť V, W jsou dva vektorové prostory nad $\mathbb{F}$ a $f : V \to W$ je izomorfismus. Pak* $\dim V = \dim W$.

DŮKAZ. Ze třetího bodu tvrzení 26 plyne, že pokud je ve V nebo ve W konečná báze, pak je v druhém z prostorů také konečná báze o stejném počtu prvků. Pokud ani v jednom z prostorů konečná báze není, pak $\dim V = \dim W = \infty$. □

TVRZENÍ 27. *Nechť V, W jsou dva vektorové prostory nad $\mathbb{F}$ konečné dimenze, $f : V \to W$ lineární zobrazení. Pak jsou následující výroky ekvivalentní:*

(1) *f je izomorfismus*
(2) *Pro všechny dvojice bází $B \subset V$, $C \subset W$ je $[f]_B^C$ regulární*
(3) *Pro některou dvojici bází je $B \subset V$, $C \subset W$ je $[f]_B^C$ regulární*

DŮKAZ. Pokud je f izomorfismus, pak je to i prosté zobrazení, platí tedy $f(v) = o_W$ pouze pro $v = o_V$. Zvolme bázi $B \in V$ a $C \in W$, pak z důsledku 5 plyne, že počet prvků B a C je stejný, označme jej n. Platí $f(v) = o_W$ právě když $[f(v)]^C = \mathbf{o} \in \mathbb{F}^m$ a $v = o_V$ právě když $[v]^B = \mathbf{o} \in \mathbb{F}^n$. Tedy $[f(v)]^C \equiv [f]_B^C[v]^B = \mathbf{o}$, právě když $[v]^B = \mathbf{o}$, neboli $\mathrm{Ker}[f]_B^C = 0$. Protože matice $[f]_B^C$ je čtvercová, plyne z toho na základě tvrzení 4, že je i regulární. Tím je dokázána implikace $1 \Rightarrow 2$. Implikace $2 \Rightarrow 3$ je zřejmá, zbývá dokázat $3 \Rightarrow 1$. Pokud $[f]_B^C$ je regulární matice z $\mathbb{F}^{n\times n}$, pak z tvrzení 4 vyplývá $\mathrm{Ker}[f]_B^C = 0$ a $\mathrm{Im}[f]_B^C = \mathbb{F}^n$. Z první vlastnosti plyne, že $[f(v)]^C = \mathbf{o}$, právě když $[v]^B = \mathbf{o}$, tedy $f(v) = o_W$ právě když $v = o_V$, tedy f je prosté. Z druhé víme, že ke každému $\mathbf{y} \in \mathbb{F}^n$ existuje $\mathbf{x} \in \mathbb{F}^n$ takový, že $\mathbf{y} = [f]_B^C\mathbf{x}$. Protože ke každému $\mathbf{x}$ existuje $v \in V$ takový, že $\mathbf{x} = [v]^B$, plyne z toho, že pro každý $\mathbf{y} \in \mathbb{F}^n$ existuje $v \in V$ takové, že $[f(v)]^C = \mathbf{y}$. Pokud $\mathbf{y} = [w]^C$ pro nějaký $w \in W$, pak $[f(v)]^C = [w]^C$ a tedy i $f(v) = w$. Zobrazení f je tudíž nejen prosté, ale také na, je to tedy izomorfismus. □

Aplikujme tvrzení 26 na $[\ ]^B : V \to \mathbb{F}^n$:

DŮSLEDEK 6. *Nechť $(v_1, \ldots, v_k)$ je posloupnost vektorů ve vektorovém prostoru V dimenze n a B je báze V. Pak*
(1) *$(v_1, \ldots, v_k)$ je LN, právě když $([v_1]^B, \ldots, [v_k]^B)$ je LN.*
(2) *$(v_1, \ldots, v_k)$ generuje V, právě když $([v_1]^B, \ldots, [v_k]^B)$ generuje $\mathbb{F}^n$.*
(3) *$(v_1, \ldots, v_k)$ je báze V, právě když $([v_1]^B, \ldots, [v_k]^B)$ báze $\mathbb{F}^n$.*

Tento důsledek nám umožňuje převést mnoho výpočtů na hledání hodnosti nějaké matice. Například

$$\{x^2 + x + 1, x^2 + 2x - 1, 2x^2 - 5x + 3\} \text{ je LN} \Leftrightarrow$$

$$\left\{ \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix}, \begin{pmatrix} 2 \\ -5 \\ 3 \end{pmatrix} \right\} \text{ je LN} \Leftrightarrow \operatorname{rank} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & -1 \\ 2 & -5 & 3 \end{pmatrix} = 3$$

DEFINICE 24. Nechť $f : V \to W$ je lineární zobrazení. Pak množina

$$\mathrm{Ker}\, f = \{v \in V | f(v) = o\}$$

se nazývá *jádro zobrazení f* a množina

$$\mathrm{Im}\, f = \{w \in W | \exists v \in V : f(v) = w\}$$

se nazývá *obraz zobrazení f*.

Definice je stejná, jako jsme měli pro jádro a obraz zobrazení mezi aritmetickými vektorovými prostory. Víme už, že tam je $\mathrm{Ker}\, F_A = \mathrm{Ker}\, A$, tedy množina všech řešení homogenní SLR s maticí A, a $\mathrm{Im}\, F_A = \mathrm{Im}\, A$, tedy sloupcový prostor matice A.

Pokud M je množina vektorů z V, zavedeme označení $f(M)$ pro množinu všech obrazů množiny M v zobrazení f. Speciálně $[M]^B$ je množina reprezentací všech vektorů z M vzhledem k bázi B.

TVRZENÍ 28. *Nechť $f : V \to W$ je lineární zobrazení, $B = (v_1, \ldots, v_n)$ báze V, $C = (w_1, \ldots, w_m)$ báze W. Pak*

$$[\mathrm{Ker}\, f]^B = \mathrm{Ker}[f]_B^C, \qquad [\mathrm{Im}\, f]^C = \mathrm{Im}[f]_B^C$$

DŮKAZ. Platí $\mathbf{x} \in [\operatorname{Ker} f]^B$, právě když $v := \sum_{i=1}^n x_i v_i \in \operatorname{Ker} f$. To zase nastává právě když $f(v) = o_W$, což je ekvivalentní s $[f(v)]^C = \mathbf{o}$ neboli $[f]_B^C [v]^B = \mathbf{o}$. Protože $\mathbf{x} = [v]^B$, je tím dokázána první část tvrzení.

Vektor $\mathbf{y}$ patří do $[\operatorname{Im} f]^C$, právě když existuje $v \in V$ takový, že $[f(v)]^C = \mathbf{y}$. Protože $[f(v)]^C = [f]_B^C [v]^B$, znamená to rovněž, že $\mathbf{y} \in \operatorname{Im} [f]_B^C$. Tím je dokázána druhá část tvrzení. □

Bude-li zobrazení f ve vztahu $[f(v)]^C = [f]_B^C [v]^B$ identita $\mathrm{Id} : V \to V$, dostáváme z něj rovnost

$$[v]^C = [\mathrm{Id}]_B^C [v]^B,$$

která vyjadřuje reprezentaci vektoru v vzhledem k bázi C pomocí reprezentace téhož vektoru vzhledem k bázi B.

DEFINICE 25. Nechť V je vektorový prostor nad $\mathbb{F}$ dimenze n, B, C jsou báze V. Matice $[\mathrm{Id}]_B^C \in \mathbb{F}^{n \times n}$ se nazývá *matice přechodu od báze C k bázi B*.

Protože Id je izomorfismus, je podle tvrzení 27 $[\mathrm{Id}]_B^C$ regulární matice. Ze vztahu $[v]^B = [\mathrm{Id}]_C^B [v]^C$ vzniklého výměnou bází dostáváme, že $\forall v \in V$ platí

$$[v]^B = [\mathrm{Id}]_C^B [\mathrm{Id}]_B^C [v]^B$$

Pokud do první rovnosti dosadíme za vektor v i-tý prvek báze B, máme na levé straně vektor $\mathbf{e}_i$ a na pravé i-tý sloupec matice $[\mathrm{Id}]_C^B [\mathrm{Id}]_B^C$. Ta je tudíž rovna jednotkové matici E. Z posledního bodu tvrzení 4 pak plyne, že $[\mathrm{Id}]_B^C$ je regulární matice a $[\mathrm{Id}]_C^B$ je k ní matice inverzní.

PŘÍKLAD 13. Spočtěme matici přechodu od báze $C = \{(0,1), (-1,1)\}$ k bázi $B = \{(1,2), (1,3)\}$ v $\mathbb{R}^2$. Zobrazíme pomocí Id prvky B a hledáme jejich reprezentaci vzhledem k C, tj. řešíme

$$\left(\begin{array}{rr|rr} 0 & -1 & 1 & 1 \\ 1 & 1 & 2 & 3 \end{array}\right) \sim \left(\begin{array}{rr|rr} 1 & 0 & 3 & 4 \\ 0 & 1 & -1 & -1 \end{array}\right)$$

Hledaná matice přechodu je tedy $[\mathrm{Id}]_B^C = \begin{pmatrix} 3 & 4 \\ -1 & -1 \end{pmatrix}$. Otestujme příkladem: reprezentace vektoru $v = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ jsou

$$[v]^C = \begin{pmatrix} 3 \\ -1 \end{pmatrix}, \quad [v]^B = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

a skutečně platí

$$[\mathrm{Id}]_B^C [v]^B = \begin{pmatrix} 3 & 4 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 \\ -1 \end{pmatrix} = [v]^C$$

KAPITOLA 8

Lineární zobrazení

Nechť V, W jsou vektorové prostory nad $\mathbb{F}$. V předchozí kapitole jsme definovali lineární zobrazení $f : V \to W$ a dva podprostory s ním spojené, jádro $\operatorname{Ker} f \leq V$ a obraz $\operatorname{Im} f \leq W$. Lineární zobrazení mezi dvěma vektorovými prostory konečné dimenze je možné reprezentovat maticí $[f]_B^C$, kde B je nějaká báze V a C je nějaká báze W. Jádro a obraz zobrazení f je možné vyjádřit pomocí jádra a obrazu matice $[f]_B^C$.

Uvažujme nyní další lineární zobrazení $g : V \to W$. Součet zobrazení f a g je zobrazení $f + g : V \to W$ definované předpisem

$$\forall v \in V : (f + g)(v) := f(v) + g(v)$$

Pro $r \in \mathbb{F}$ je r-násobek f zobrazení $rf : V \to W$ definované

$$\forall v \in V : (rf)(v) := rf(v)$$

Snadno se ověří, že jak $f + g$, tak rf jsou také lineární zobrazení.

Tvrzení 29. *Nechť V, W jsou vektorové prostory konečné dimenze nad $\mathbb{F}$, B je báze V, C je báze W, $f, g : V \to W$ lineární zobrazení, $r \in \mathbb{F}$. Pak*

$$[f + g]_B^C = [f]_B^C + [g]_B^C, \qquad [rf]_B^C = r[f]_B^C$$

Důkaz. Nechť $B = (v_1, \dots, v_n)$. Pak z definic plyne

$$\begin{aligned}
[f + g]_B^C &= ([(f + g)(v_1)]^C \mid \dots \mid [(f + g)(v_n)]^C) \\
&= ([f(v_1) + g(v_1)]^C \mid \dots \mid [f(v_n) + g(v_n)]^C) \\
&= ([f(v_1)]^C + [g(v_1)]^C \mid \dots \mid [f(v_n)]^C + [g(v_n)]^C) = [f]_B^C + [g]_B^C
\end{aligned}$$

Podobně

$$[rf]_B^C = ([rf(v_1)]^C \mid \dots \mid [rf(v_n)]^C) = r[f]_B^C$$

□

Je-li U další vektorový prostor nad $\mathbb{F}$ a $h : U \to V$ lineární zobrazení, pak lze opět jednoduše ověřit, že složené zobrazení $f \circ h : U \to W$ je také lineární.

Tvrzení 30. *Nechť U, V, W jsou vektorové prostory konečné dimenze nad $\mathbb{F}$, D je báze U, B je báze V, C je báze W, $f : V \to W$, $h : U \to V$ lineární zobrazení. Pak*

$$[f \circ h]_D^C = [f]_B^C \, [h]_D^B$$

Důkaz. Nechť $D = (u_1, \dots, u_p)$, $u \in U$. Pak

$$[(f \circ h)(u)]^C = [f(h(u))]^C = [f]_B^C \, [h(u)]^B = [f]_B^C \, [h]_D^B \, [u]^D$$

Dosadíme-li za vektor u i-tý prvek báze D, dostáváme, že i-tý sloupec matice $[f]_B^C \, [h]_D^B$ je roven $[(f \circ h)(u_i)]^C$, tedy i-tému sloupci matice $[f \circ h]_D^C$. □

Jinými slovy reprezentace složeného zobrazení $f \circ h$ je rovna součinu matic reprezentujících f a h. Speciálně odtud plyne *transformační formule pro reprezentaci lineárního zobrazení*:

Tvrzení 31. *Nechť V, W jsou vektorové prostory konečné dimenze nad $\mathbb{F}$, B, B' jsou báze V, C, C' jsou báze W, $f : V \to W$. Pak*

$$[f]_{B'}^{C'} = [\mathrm{Id}]_C^{C'} \, [f]_B^C \, [\mathrm{Id}]_{B'}^B$$

Důkaz. Stačí použít tvrzení 30 na složení tří lineárních zobrazení $\mathrm{Id} \circ f \circ \mathrm{Id}$:

$$[f]_{B'}^{C'} = [\mathrm{Id} \circ f \circ \mathrm{Id}]_{B'}^{C'} = [\mathrm{Id}]_C^{C'} \, [f]_B^C \, [\mathrm{Id}]_{B'}^B,$$

□

Příklad 14. V minulé kapitole jsme měli zobrazení $F : \mathbb{R}^2 \to \mathbb{R}^3$ s reprezentacemi

$$[F]_{K_2}^{K_3} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ -2 & 1 \end{pmatrix}, \quad [F]_B^C = \begin{pmatrix} 1 & 1 \\ 2 & 2 \\ 0 & 1 \end{pmatrix},$$

kde $B = ((1,2)^T, (1,3)^T)$, $C = ((1,1,0)^T, (1,0,0)^T, (1,0,1)^T)$. Protože

$$[\mathrm{Id}]_C^{K_3} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad [\mathrm{Id}]_{K_2}^B = \left([\mathrm{Id}]_B^{K_2}\right)^{-1} = \begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix},$$

můžeme ověřit $[\mathrm{Id}]_C^{K_3} \, [F]_B^C \, [\mathrm{Id}]_{K_2}^B = [F]_{K_2}^{K_3}$ dosazením:

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

Lineárnímu zobrazení $f : V \to W$ se říká také *homomorfismus vektorových prostorů V a W*. Zobrazení, pro které $V = W$, tedy se stejným zdrojovým a cílovým prostorem, se nazývá *endomorfismus vektorového prostoru V*. Pokud B, B' jsou dvě báze V, označme

- $R := [\mathrm{Id}]_{B'}^B$ matici přechodu od B k B'
- $A := [f]_B^B$ *matici endomorfismu vzhledem k bázi B.*
- $A' := [f]_{B'}^{B'}$ matici endomorfismu vzhledem k bázi B'.

Pak dostáváme *transformační formuli pro matici endomorfismu*:

$$A' = [f]_{B'}^{B'} = [\mathrm{Id}]_B^{B'} [f]_B^B [\mathrm{Id}]_{B'}^B = R^{-1} A R$$

Dvě matice A', A, pro něž existuje regulární matice R taková, že $A' = R^{-1}AR$, se nazývají *podobné*. Podobnost je relace ekvivalence. Charakterizovat třídy této ekvivalence, a tedy umět poznat, zda jsou dvě matice podobné, se naučíme v kapitole o Jordanově tvaru.

Připomeňme z minula, že izomorfismus je bijektivní lineární zobrazení. Složením dvou izomorfismů je opět izomorfismus. Inverzní zobrazení k izomorfismu $f : V \to W$ díky bijektivitě existuje a je také bijektivní. Abychom ukázali jeho linearitu, definujme pro nějaké $w_1, w_2 \in W$ vektory $v_1 = f^{-1}(w_1)$ a $v_2 = f^{-1}(w_2)$. Pak pro $r, s \in \mathbb{F}$

$$f(rv_1 + sv_2) = rf(v_1) + sf(v_2) = rw_1 + sw_2, \text{ tedy}$$
$$f^{-1}(rw_1 + sw_2) = rv_1 + sv_2 = rf^{-1}(w_1) + sf^{-1}(w_2).$$

Dva vektorové prostory, mezi nimiž existuje izomorfismus, se nazývají *izomorfní*. Izomorfnost je relace ekvivalence vektorových prostorů. Už v důsledku 5 jsme ukázali, že izomorfní vektorové prostory mají stejnou dimenzi. V následující větě ukážeme, že pro vektorové prostory konečné dimenze platí i opačná implikace.

Věta 7. *Dva vektorové prostory V, W nad $\mathbb{F}$ konečné dimenze jsou izomorfní, právě když mají stejnou dimenzi.*

Důkaz. Pokud $\dim V = \dim W =: n$, pak zvolme bázi B ve V, bázi C ve W a označme

$$g := [\ ]^B : V \to \mathbb{F}^n$$
$$h := [\ ]^C : W \to \mathbb{F}^n$$

Protože g i h jsou izomorfismy, jsou izomorfismem i zobrazení

$$h^{-1} : \mathbb{F}^n \to W$$
$$h^{-1} \circ g : V \to W$$

Tedy V a W jsou izomorfní. □

Nechť V, W jsou dva vektorové prostory nad $\mathbb{F}$. Množina všech homomorfismů z V do W je vektorový prostor s operacemi součtu homomorfismů a násobení homomorfismu skalárem z $\mathbb{F}$, značí se $\mathrm{Hom}(V, W)$. Ověření, že je splněna definice 11 necháváme na čtenáři.

Věta 8. *Pokud* $\dim V = n$ *a* $\dim W = m$, *pak* $\dim \mathrm{Hom}(V, W) = mn$.

Důkaz. Zvolme ve V bázi B a v W bázi C. Zobrazení

$$[\ ]_B^C : \mathrm{Hom}(V, W) \to \mathbb{F}^{m \times n},$$

které přiřazuje homomorfismu f jeho reprezentaci $[f]_B^C$, je lineární a bijektivní, tedy izomorfismus. Protože prostor $\mathbb{F}^{m\times n}$ má bázi například $\{E_{ij} | i \in \{1, \dots, m\}, j \in \{1, \dots, n\}$ o mn prvcích, je $\dim \mathbb{F}^{m\times n} = mn$ a tedy také $\dim \mathrm{Hom}(V, W) = mn$. □

Vektorový prostor všech endomorfismů prostoru V se místo $\mathrm{Hom}(V, V)$ častěji značí symbolem $\mathrm{End}(V)$, $\dim \mathrm{End}(V) = n^2$. Prostý homomorfismus se označuje slovem *monomorfismus*, pokud je na, pak mu říkáme *epimorfismus*.

Věta 9 (O zadání homomorfismu hodnotami na bázi). *Nechť V, W jsou vektorové prostory nad $\mathbb{F}$, $B = (v_1, \dots, v_n)$ je báze V a $M = (w_1, \dots, w_n)$ posloupnost vektorů ve W. Pak existuje právě jeden $f \in \mathrm{Hom}(V, W)$ takový, že*

$$f(v_1) = w_1, \quad f(v_2) = w_2, \quad \dots, \quad f(v_n) = w_n$$

Navíc f je monomorfismus, právě když M je lineárně nezávislá a f je epimorfismus, právě když M generuje W.

Důkaz. Je-li $v \in V$, $\mathbf{x} := [v]^B$, pak definujme $f(v) := \sum_{i=1}^n x_i w_i$. Důkaz, že f je homomorfismus ♣, stejně tak důkaz jednoznačnosti a ekvivalentní podmínky mono-/epimorfismu. □

V následující větě nemusíme předpokládat, že vektorové prostory mají konečnou dimenzi.

Věta 10. *Nechť U, V, W jsou vektorové prostory nad $\mathbb{F}$, $f \in \mathrm{Hom}(V, W)$, $g \in \mathrm{Hom}(U, V)$. Platí*

(1) *f je monomorfismus, právě když* $\mathrm{Ker}\, f = 0$
(2) *f je epimorfismus, právě když* $\mathrm{Im}\, f = W$
(3) *Jsou-li f, g monomorfismy, pak je $f \circ g$ monomorfismus.*
(4) *Jsou-li f, g epimorfismy, pak je $f \circ g$ epimorfismus.*
(5) *Je-li $f \circ g$ monomorfismus, je g monomorfismus.*
(6) *Je-li $f \circ g$ epimorfismus, je f epimorfismus.*

Důkaz. Pokud pro $v_1, v_2 \in V$ platí $f(v_1) = f(v_2)$, je $f(v_1 - v_2) = o_W$ a tedy $v_1 - v_2 \in \mathrm{Ker}\, f$. Tedy $\mathrm{Ker}\, f = 0$ znamená, že $v_1 = v_2$, čili f je monomorfismus. Naopak pokud f je monomorfismus, nemůže být vzorem o_W jiný vektor než o_V, tedy $\mathrm{Ker}\, f = 0$. Tím jsme ověřili první bod, druhý plyne z definic.

Pokud f je monomorfismus a $f(g(v)) = o_W$, pak $g(v) = o_V$, a je-li i g monomorfismus, musí být $v = o_U$. S využitím prvního bodu odtud plyne třetí bod. Podobně, je-li $w \in W$ a f je epimorfismus, pak existuje $v \in V$ takový, že $f(v) = w$. Je-li g epimorfismus, pak existuje $u \in U$ takový, že $g(u) = v$. Celkově tedy pro každý $w \in W$ existuje $u \in U$ takový, že $(f \circ g)(u) = w$, čímž je dokázán čtvrtý bod.

Pro pátý bod si stačí uvědomit, že pokud g není monomorfismus, tedy dle prvního bodu existuje nenulový $u \in U$ takový, že $g(u) = o_V$, pak i $(f \circ g)(u) = o_W$, tedy i $f \circ g$ má nenulové jádro. Podobně šestý bod vyplývá z toho, že vektor, který není v obrazu f, nemůže být ani v obrazu $f \circ g$. □

VĚTA 11 (O dimenzi jádra a obrazu). *Nechť V, W jsou vektorové prostory nad $\mathbb{F}$, $\dim V = n$, $f \in \operatorname{Hom}(V, W)$. Pak*

$$\dim \operatorname{Ker} f + \dim \operatorname{Im} f = n$$

DŮKAZ. Argumentace je jednodušší, pokud předpokládáme, že $\dim W < \infty$. Zvolíme-li bázi B ve V a bázi C ve W, pak

$$\dim \operatorname{Ker} f = \dim[\operatorname{Ker} f]^B = \dim \operatorname{Ker}[f]_B^C$$
$$\dim \operatorname{Im} f = \dim[\operatorname{Im} f]^C = \dim \operatorname{Im}[f]_B^C$$

Protože n je rovno počtu sloupců matice $[f]_B^C$, plyne tvrzení z věty o hodnosti a nulitě pro tuto matici. □

Dimenzi $\operatorname{Ker} f$ nazýváme *nulitou homomorfismu* f, značíme $n(f)$. Dimenzi $\operatorname{Im} f$ nazýváme *hodností homomorfismu* f, značíme $\operatorname{rank}(f)$. Předchozí věta se tedy dá nazývat i větou o hodnosti a nulitě homomorfismu. Plyne z ní

TVRZENÍ 32. *Nechť V je vektorový prostor nad $\mathbb{F}$ konečné dimenze, $f \in \operatorname{End}(V)$. Je-li f mono- nebo epimorfismus, pak už musí být i izomorfismem.*

DŮKAZ. Pokud f je monomorfismus, je $\operatorname{Ker} f = 0$, tedy $n(f) = 0$. Pak ale $\operatorname{rank}(f) = n$, tedy $\dim \operatorname{Im} f = \dim V$. Musí být proto $\operatorname{Im} f = V$, neboli f je epimorfismus a tudíž i izomorfismus. Pokud f je epimorfismus, má důkaz tytéž kroky, jen v opačném pořadí. □

Izomorfismus $f \in \operatorname{End}(V)$ se nazývá *automorfismem* prostoru V.

KAPITOLA 9

Determinant

V první kapitole jsme se dotkli souvislosti vektorového spučinu a určení objemu rovnoběžníka a rovnoběžnostěnu. Ve cvičení 1 jsme zavedli veličinu

$$V(\mathbf{x},\mathbf{y},\mathbf{z}) := (\mathbf{x}\times\mathbf{y}).\mathbf{z} \equiv \sum_{i=1}^{3}\sum_{j=1}^{3}\sum_{k=1}^{3}\varepsilon_{ijk}x_i y_j z_k,$$

určenou trojicí vektorů $\mathbf{x},\mathbf{y},\mathbf{z}\in\mathbb{R}^3$. Ukázali jsme, že její absolutní hodnota udává objem rovnoběžnostěnu určeného vektory $\mathbf{x},\mathbf{y},\mathbf{z}\in\mathbb{R}^3$. Důkaz byl založen na tom, že zobrazení $V:\mathbb{R}^3\times\mathbb{R}^3\times\mathbb{R}^3\to\mathbb{R}$ má následující vlastnosti:

(1) $V(r\mathbf{x}_1+s\mathbf{x}_2,\mathbf{y},\mathbf{z}) = rV(\mathbf{x}_1,\mathbf{y},\mathbf{z})+sV(\mathbf{x}_2,\mathbf{y},\mathbf{z})$
(2) $V(\mathbf{x},\mathbf{y},\mathbf{z}) = -V(\mathbf{y},\mathbf{x},\mathbf{z}) = V(\mathbf{y},\mathbf{z},\mathbf{x})$
(3) $V(\mathbf{e}_1,\mathbf{e}_2,\mathbf{e}_3)=1$

První vlastnost, linearita, je hned vidět z definice V. Druhá vyplývá z toho, že $\varepsilon_{ijk}=-\varepsilon_{jik}=\varepsilon_{jki}$ pro všechny možné trojice indexů $i,j,k\in\{1,2,3\}$. Pokud zobrazení při výměně proměnných v nějaké dvojici argumentů změní znaménko, říkáme, že je v této dvojici argumentů *antisymetrické*. Je-li antisymetrické v každé dvojici argumentů, říkáme, že je *úplně antisymetrické*. Poslední vlastnost platí, protože $\varepsilon_{123}=1$. Z druhé vlastnosti plyne linearita i ve 2. a 3. argumentu a také, že $V(\mathbf{x},\mathbf{y},\mathbf{z})=0$, kdykoli se některé dva vektory z $\mathbf{x},\mathbf{y},\mathbf{z}$ rovnají.

Není těžké si rozmyslet, že zobrazení V je těmito třemi vlastnostmi určeno jednoznačně. Chvíli předstírejme, že definici V neznáme, a používejme jen vlastnosti a jejich důsledky. Pak

$$\begin{aligned}
V(\mathbf{x},\mathbf{y},\mathbf{z}) &= V(x_1\mathbf{e}_1+x_2\mathbf{e}_2+x_3\mathbf{e}_3, y_1\mathbf{e}_1+y_2\mathbf{e}_2+y_3\mathbf{e}_3, z_1\mathbf{e}_1+z_2\mathbf{e}_2+z_3\mathbf{e}_3)\\
&= \sum_{i=1}^{3}\sum_{j=1}^{3}\sum_{k=1}^{3} x_i y_j z_k V(\mathbf{e}_i,\mathbf{e}_j,\mathbf{e}_k)\\
&= x_1y_2z_3V(\mathbf{e}_1,\mathbf{e}_2,\mathbf{e}_3)+x_1y_3z_2V(\mathbf{e}_1,\mathbf{e}_3,\mathbf{e}_2)+x_2y_1z_3V(\mathbf{e}_2,\mathbf{e}_1,\mathbf{e}_3)\\
&\quad + x_2y_3z_1V(\mathbf{e}_2,\mathbf{e}_3,\mathbf{e}_1)+x_3y_1z_2V(\mathbf{e}_3,\mathbf{e}_1,\mathbf{e}_2)+x_3y_2z_1V(\mathbf{e}_3,\mathbf{e}_2,\mathbf{e}_1)\\
&= x_1y_2z_3-x_1y_3z_2-x_2y_1z_3+x_2y_3z_1+x_3y_1z_2-x_3y_2z_1
\end{aligned}$$

Druhá rovnost je důsledkem linearity ve všech třech argumentech, ve třetí jsme z $3.3.3=27$ sčítanců vynechali 21, které jsou nulové, protože se do nějaké dvojice argumentů dosazují dva stejné vektory. Nakonec využíváme druhé a třetí vlastnosti. Výsledné vyjádření $V(\mathbf{x},\mathbf{y},\mathbf{z})$ se shoduje s jeho definicí pomocí vektorového a skalárního součinu.

V této kapitole zobecníme V do libovolné dimenze n, tedy na zobrazení

$$V:\underbrace{\mathbb{R}^n\times\ldots\times\mathbb{R}^n}_{n}\to\mathbb{R}$$

Jednou z cest by bylo požadovat opět linearitu v každém argumentu, antisymetrii v každé dvojici argumentů a $V(\mathbf{e}_1,\ldots,\mathbf{e}_n)=1$. Tím bychom získali jednoznačné vyjádření $V(\mathbf{x}_1,\ldots,\mathbf{x}_n)$ pomocí složek vektorů $\mathbf{x}_i$, a znaménka v tomto vyjádření by definovala hodnoty $\varepsilon_{i_1\ldots i_n}$. Zobecněné vlastnosti (1),(2) a (3) pak zaručují, že je V

rozumným vyjádřením objemu rovnoběžnostěnu definovaného vektory $\mathbf{x}_1, \dots, \mathbf{x}_n$. My se vydáme opačnou cestou: nejprve zobecníme veličinu ε_{ijk} a vlastnosti (1),(2) a (3) a s nimi i souvislost s objemem získáme jako důsledky.

1. Permutace

Uvažujme nějakou konečnou množinu, například $M = \{1, 2, \dots, n\}$, a množinu všech bijektivních zobrazení z M do M. Pak tato množina s operací skládání zobrazení splňuje definici 9 a je to tedy grupa. Neutrální prvek této grupy, tedy zobrazení identita na M, značíme id.

Definice 26. Grupa všech bijektivních zobrazení množiny $\{1, 2, \dots, n\}$ do sebe s operací skládání se nazývá *symetrická grupa* a značí se S_n. Její prvky se nazývají *permutace*.

Dva základní způsoby zápisu permutace si můžeme ukázat na příkladu

$$\begin{tikzcd}[column sep=small] \pi := 1 \arrow[rr, bend left] & 2 \arrow[rrr, bend left] & 3 \arrow[rrrr, bend left] & 4 \arrow[lll, bend left] & 5 \arrow[lll, bend left] & 6 \arrow[loop above] & 7 \arrow[lll, bend left] \equiv \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 7 & 1 & 2 & 6 & 4 \end{pmatrix} \end{tikzcd}$$

V tabulkovém zápisu je každý sloupec tvořen dvojicí vzor, obraz, tedy například $\pi(4) = 1$. Šipkový zápis můžeme přepsat jako

$$\begin{tikzcd} 1 \arrow[r] & 3 \arrow[d] & 2 \arrow[d, bend left] & 6 \arrow[loop below] \\ 4 \arrow[u] & 7 \arrow[l] & 5 \arrow[u, bend left] & \end{tikzcd}$$

Definice 27. Nechť $\pi \in S_n$. Prvek $i \in \{1, \dots, n\}$ nazýváme *samodružný*, pakliže $\pi(i) = i$. Permutaci π nazýváme *cyklus délky* k, pokud existuje posloupnost $(i_1, \dots, i_k)$ z $\{1, \dots, n\}$ taková, že pro všechna $j \in \{1, \dots, k-1\}$ je $\pi(i_j) = i_{j+1}$ a $\pi(i_k) = i_1$, a že všechny prvky $\{1, \dots, n\}$ mimo tuto posloupnost jsou samodružné. Cyklus délky 2 nazýváme *transpozice*.

V pojmosloví i v zápise bývá běžné ztotožňovat cyklus délky alespoň 2 s příslušnou posloupností nesamodružných prvků. Cykly jsou *nezávislé*, pokud tyto posloupnosti neobsahují žádný společný prvek. Permutaci π z příkladu pak můžeme zapsat jako (1374)(25), tedy jako rozklad na nezávislé cykly délky alespoň 2, nebo jako (1374)(25)(6), pokud vypíšeme i samodružné prvky coby cykly délky 1. Je snadné si rozmyslet, že takový rozklad má každá permutace a že je určen jednoznačně. Můžeme ho chápat buď jako množinu cyklů v permutaci se vyskytujících, nebo jako složení příslušných permutací, v příkladu $(1374) \circ (25)$.

Permutace obecně nekomutují, to je vidět třeba na příkladu transpozic z S_3

$$(12) \circ (13) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132)$$

$$(13) \circ (12) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)$$

Pokud ale skládáme nezávislé cykly, na pořadí nezáleží, permutaci π tedy lze zapsat i jako $(25) \circ (1374)$.

Podobně jako jsme zapsali cyklus (i_1, i_2, i_3) délky 3 jako složení dvou transpozic $(i_1, i_3) \circ (i_1, i_2)$, můžeme obecný cyklus délky k zapsat jako

$$(i_1, i_2, \dots, i_k) = (i_1, i_k) \circ (i_1, i_2, \dots, i_{k-1}) = \ldots = (i_1, i_k) \circ (i_1, i_{k-1}) \circ \ldots \circ (i_1, i_2),$$

tedy jako složení $k-1$ transpozic. Takových rozkladů je mnoho, například

$$(1374) = (14) \circ (17) \circ (13) = (13) \circ (37) \circ (74) = (47) \circ (43) \circ (41) = \ldots$$

Každou permutaci tedy umíme zapsat jako složení transpozic, např $\pi = (14)\circ(17)\circ(13)\circ(25)$. Budeme chtít na základě takového rozkladu přiřadit permutaci hodnotu $+1$ nebo -1, které bude odpovídat hodnotě ϵ_{ijk} z úvodu kapitoly.

LEMMA 4. *Je-li $\pi \in S_n$ permutace a $(ij) \in S_n$ transpozice, pak označme p, resp. q počet cyklů sudé délky v rozkladu permutace π, resp. $\pi \circ (ij)$ na nezávislé cykly. Pak $|p-q| = 1$.*

DŮKAZ. Rozebereme dva případy. Pokud jsou i, j součástí dvou různých nezávislých cyklů v rozkladu π, zapišme tyto cykly jako $(i, i_2, \dots, i_r)$ a $(j, j_2, \dots, j_s)$, $r, s \in \mathbb{N}$. Pak

$$(i, i_2, \dots, i_r) \circ (j, j_2, \dots, j_s) \circ (ij) = (i, j_2, \dots, j_s, j, i_2, \dots, i_r)$$

Tedy ze dvou cyklů délek r, s vznikl jeden cyklus délky $r+s$. Ostatní cykly v rozkladu π se složením s (ij) nemění. Jsou-li r, s obě sudá, je i $r+s$ sudé. Je-li právě jedno z r, s liché, je $r+s$ liché. V obou případech počet cyklů sudé délky klesl o 1. Jsou-li r, s obě lichá, je $r+s$ sudé a počet cyklů sudé délky vzrostl o 1. Tedy p a q se liší vždy o 1.

Jsou-li naopak i, j součástí téhož cyklu v π, pak pro tento cyklus platí

$$(i, j_2, \dots, j_s, j, i_2, \dots, i_r) \circ (ij) = (i, i_2, \dots, i_r) \circ (j, j_2, \dots, j_s)$$

a můžeme použít tytéž úvahy jako v předchozím případě. □

DEFINICE 28. Nechť $\pi \in S_n$ je permutace a $\pi_1, \dots, \pi_k \in S_n$ jsou transpozice takové, že $\pi = \pi_1 \circ \pi_2 \circ \dots \circ \pi_k$. Pak definujeme *znaménko permutace* π jako $\operatorname{sgn}\pi := (-1)^k$. Pokud $\operatorname{sgn}\pi = +1$, mluvíme o *sudé permutaci*, pokud $\operatorname{sgn}\pi = -1$, je π *lichá permutace*.

Permutaci π lze zapsat jako složení transpozic mnoha způsoby. To, že všechny vedou ke stejné hodnotě znaménka, a tedy že je definice korektní, lze ukázat s pomocí lemmatu 4. Protože π_1 obsahuje právě jeden cyklus sudé délky a složení s transpozicí podle lemmatu mění počet cyklů sudé délky právě o 1, nahoru, či dolů, je parita (sudost či lichost) počtu cyklů sudé délky π stejná jako parita čísla k. To ale bude platit pro jakýkoli jiný zápis π jako složení transpozic $\pi'_1 \circ \dots \circ \pi'_l$, tedy parita čísla l je stejná jako parita k.

DŮSLEDEK 7. *Nechť $\pi, \rho \in S_n$ a p je počet cyklů sudé délky v rozkladu permutace π na nezávislé cykly.*

(1) $\operatorname{sgn}\pi = (-1)^p$.
(2) $\operatorname{sgn}(\pi \circ \rho) = \operatorname{sgn}\pi \operatorname{sgn}\rho$
(3) $\operatorname{sgn}\pi^{-1} = \operatorname{sgn}\pi$

PŘÍKLAD 15. Grupa S_3 obsahuje $3! = 6$ prvků: identitu, tři transpozice a dva cykly délky 3. Jejich znaménka jsou

$$\begin{array}{ccc} \operatorname{sgn}\mathrm{id} = +1 & \operatorname{sgn}(12) = -1 & \operatorname{sgn}(123) = 1 \\ \operatorname{sgn}(13) = -1 & \operatorname{sgn}(23) = -1 & \operatorname{sgn}(132) = 1 \end{array}$$

Pokud definujeme $\varepsilon_{\pi(1)\pi(2)\pi(3)} := \operatorname{sgn}\pi$ a $\varepsilon_{ijk} = 0$ jindy, dostáváme přesně veličinu ε z definice zobrazení V.

2. Determinant a jeho výpočet

DEFINICE 29. Nechť $A \in \mathbb{F}^{n\times n}$. *Determinantem* matice A rozumíme číslo

$$\det A := \sum_{\pi \in S_n} \operatorname{sgn}\pi \; a_{1\pi(1)} a_{2\pi(2)} \dots a_{n\pi(n)}$$

Determinant $n \times n$ matice je tedy součet $n!$ sčítanců, z nichž každý je až na znaménko součinem n-tice elementů matice, z nichž žádné dva neleží ve stejném řádku ani sloupci. Pro 2×2 a 3×3 matice lze definici použít přímo k výpočtu:

$$\begin{aligned}
\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} &= \operatorname{sgn} \mathrm{id}\, a_{11}a_{22} + \operatorname{sgn}(12) a_{12}a_{21} \\
&= a_{11}a_{22} - a_{12}a_{21} \\
\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} &= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} \\
&\quad - a_{11}a_{23}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33}
\end{aligned}$$

Pro $n > 3$ je už počet potřebných operací neprakticky vysoký. Důležitý speciální případ je dolní trojúhelníková matice, v níž $a_{ij} = 0$ pro $i < j$. Pro každou permutaci $\pi \neq \mathrm{id}$ platí, že $\pi(i) > i$ pro nejmenší prvek $\{1, \dots, n\}$, který není vůči π samodružný. Pak ale ze sčítanců v definici determinantu zbyde jen ten první $a_{11}a_{22} \dots a_{nn}$, ostatní obsahují vždy alespoň jeden činitel $a_{i\pi(i)}$ rovný nule. Stejně tak i determinant horní trojúhelníkové matice je roven součinu jejích diagonálních prvků. Plyne to i z následující věty:

Věta 12. *Nechť $A \in \mathbb{F}^{n \times n}$. Pak $\det A = \det A^T$.*

Důkaz. Každá permutace π má k sobě jednoznačně přiřazenou permutaci inverzní $\rho := \pi^{-1}$, v definici determinantu tedy můžeme sčítat i přes ni:

$$\begin{aligned}
\det A &= \sum_{\pi \in S_n} \operatorname{sgn}(\pi) a_{1\pi(1)} a_{2\pi(2)} \dots a_{n\pi(n)} \\
&= \sum_{\rho \in S_n} \operatorname{sgn}(\rho^{-1}) a_{1\rho^{-1}(1)} a_{2\rho^{-1}(2)} \dots a_{n\rho^{-1}(n)}
\end{aligned}$$

Z důsledku 7 víme, že $\operatorname{sgn} \rho = \operatorname{sgn} \rho^{-1}$. Množina uspořádaných dvojic $\{(1, \rho^{-1}(1)), (2, \rho^{-1}(2)), \dots, (n, \rho^{-1}(n))\}$ obsahuje tytéž prvky jako množina $\{(\rho(1), 1), (\rho(2), 2), \dots, (\rho(n), n)\}$, jen v jiném pořadí. Tedy

$$\det A = \sum_{\rho \in S_n} \operatorname{sgn}(\rho) a_{\rho(1)1} a_{\rho(2)2} \dots a_{\rho(n)n} = \sum_{\rho \in S_n} \operatorname{sgn}(\rho) a^T_{1\rho(1)} a^T_{2\rho(2)} \dots a^T_{n\rho(n)},$$

což je z definice rovno $\det A^T$. □

Ukažme nyní souvislost determinantu se zobrazením V z úvodu kapitoly. Pro $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{R}^3$ definujme $A := (\mathbf{x}|\mathbf{y}|\mathbf{z})$. Pak z věty plyne, že

$$\begin{aligned}
\det A = \det A^T &= \sum_{\rho \in S_3} \operatorname{sgn}(\rho) a_{\rho(1)1} a_{\rho(2)2} a_{\rho(3)3} = \sum_{\rho \in S_3} \operatorname{sgn}(\rho) x_{\rho(1)} y_{\rho(2)} z_{\rho(3)} \\
&= \sum_{i=1}^{3} \sum_{j=1}^{3} \sum_{k=1}^{3} \varepsilon_{ijk} x_i y_j z_k = V(\mathbf{x}, \mathbf{y}, \mathbf{z})
\end{aligned}$$

Determinant je tedy skutečně zobecněním zobrazení V a vyplatí se na něj nahlížet jako na funkci, která přiřazuje n-prvkové posloupnosti vektorů $\mathbf{a}_1, \dots, \mathbf{a}_n$ z $\mathbb{F}^n$ číslo $\det(\mathbf{a}_1| \dots |\mathbf{a}_n)$. Ze tří vlastností úplně charakterizujících zobrazení V i jeho zobecnění do vyšší dimenze vidíme tu třetí ihned:

$$V(e_1, \dots, e_n) = \det(\mathbf{e}_1| \dots |\mathbf{e}_n) = 1$$

Úplnou antisymetrii a linearitu v každém argumentu ukážeme v následujícím tvrzení:

Tvrzení 33. *Nechť $i \in \{1, \dots, n\}$, $\mathbf{a}_1, \dots, \mathbf{a}_n, \mathbf{a}'_i \in \mathbb{F}^n$, $r, r' \in \mathbb{F}$, $\rho \in S_n$. Pak*

(1) $\det(\mathbf{a}_1|\dots|r\mathbf{a}_i+r'\mathbf{a}_i'|\dots|\mathbf{a}_n) = r\det(\mathbf{a}_1|\dots|\mathbf{a}_i|\dots|\mathbf{a}_n)+r'\det(\mathbf{a}_1|\dots|\mathbf{a}_i'|\dots|\mathbf{a}_n)$
(2) $\det(\mathbf{a}_{\rho(1)}|\dots|\mathbf{a}_{\rho(n)}) = \operatorname{sgn}(\rho)\det(\mathbf{a}_1|\dots|\mathbf{a}_n)$

DŮKAZ. Pro první tvrzení stačí jen roznásobit každý člen sumy

$$\sum_{\rho\in S_n}\operatorname{sgn}(\rho)a_{\rho(1)1}\dots(ra_{\rho(i)i}+r'a'_{\rho(i)i})\dots a_{\rho(n)n}$$

Druhé plyne z úprav využívajících důsledek 7 a skutečnost, že množiny $\{\pi|\pi\in S_n\}$ a $\{\rho\circ\pi|\pi\in S_n\}$ jsou totožné:

$$\begin{aligned}\det(\mathbf{a}_{\rho(1)}|\dots|\mathbf{a}_{\rho(n)}) &= \sum_{\pi\in S_n}\operatorname{sgn}\pi\ a_{1,\rho(\pi(1))}a_{2,\rho(\pi(2))}\dots a_{n,\rho(\pi(n))}\\ &= \operatorname{sgn}\rho^{-1}\sum_{\pi\in S_n}\operatorname{sgn}(\rho\circ\pi)\ a_{1,(\rho\circ\pi)(1)}a_{2,(\rho\circ\pi)(2)}\dots a_{n,(\rho\circ\pi)(n)}\\ &= \operatorname{sgn}\rho\sum_{\tau\in S_n}\operatorname{sgn}\tau\ a_{1,\tau(1)}a_{2,\tau(2)}\dots a_{n,\tau(n)}\end{aligned}$$

□

DŮSLEDEK 8. *Nechť* $A\in\mathbb{F}^{n\times n}$, $r\in\mathbb{F}$. *Pak*

(1) *Má-li A dva sloupce stejné nebo jeden ze sloupců nulový, pak* $\det A = 0$.
(2) *ESÚ typu přičtení r-násobku sloupce do jiného sloupce nemění determinant.*
(3) *ESÚ typu násobení sloupce číslem r násobí celý determinant číslem r.*
(4) *ESÚ typu prohození dvou sloupců obrací znaménko determinantu.*
(5) *Platí i analogická tvrzení pro řádky a EŘÚ.*

DŮKAZ. První a čtvrté tvrzení plynou z druhé části tvrzení 33, třetí z jeho první části. Druhé dostaneme z rovnosti

$$\det(\mathbf{a}_1|\dots|\mathbf{a}_i+r\mathbf{a}_j|\dots|\mathbf{a}_n) = \det(\mathbf{a}_1|\dots|\mathbf{a}_i|\dots|\mathbf{a}_n)+r\det(\mathbf{a}_1|\dots|\mathbf{a}_j|\dots|\mathbf{a}_n),$$

v níž je druhý člen na pravé straně nula z první části tohoto tvrzení. Pátý bod plyne z věty 12. □

Determinant matice můžeme tedy efektivně vypočítat pomocí posloupnosti EŘÚ a ESÚ, které matici převedou na jednodušší, nejlépe horní či dolní trojúhelníkovou matici. Zkusme si výpočet determinantu na příkladě, v rámci nějž rovněž začneme používat obvyklé značení determinantu matice nahrazením závorky svislou čárou.

$$\begin{vmatrix}7&2&1&4\\3&6&-9&3\\2&4&0&3\\5&-2&3&0\end{vmatrix} = 3\begin{vmatrix}7&2&1&4\\1&2&-3&1\\2&4&0&3\\5&-2&3&0\end{vmatrix} = 6\begin{vmatrix}7&1&1&4\\1&1&-3&1\\2&2&0&3\\5&-1&3&0\end{vmatrix} =$$

$$= -6\begin{vmatrix}1&7&1&4\\1&1&-3&1\\2&2&0&3\\-1&5&3&0\end{vmatrix} = -6\begin{vmatrix}1&7&1&4\\0&-6&-4&-3\\0&-12&-2&-5\\0&12&4&4\end{vmatrix} = 24\begin{vmatrix}1&1&7&4\\0&4&6&3\\0&2&12&5\\0&1&3&1\end{vmatrix} =$$

$$= -24\begin{vmatrix}1&1&7&4\\0&1&3&1\\0&0&6&3\\0&0&-6&-1\end{vmatrix} = -72\begin{vmatrix}1&1&7&4\\0&1&3&1\\0&0&2&1\\0&0&0&2\end{vmatrix} = -288$$

VĚTA 13. *Matice* $A\in\mathbb{F}^{n\times n}$ *je regulární, právě když* $\det(A)\neq 0$.

DŮKAZ. Regularita i nenulovost determinantu se zachovávají pomocí EŘÚ a ESÚ, stačí se tedy dívat jen na matici v odstupňovaném tvaru. Ta je regulární, právě když má všechny prvky na hlavní diagonále nenulové, což nastává právě když je nenulový determinant. □

Minorem nebo též *subdeterminantem* rozumíme determinant nějaké čtvercové podmatice, tj. matice vzniklé vynecháním některých řádků a sloupců.

TVRZENÍ 34. *Nechť* $A \in \mathbb{F}^{m\times n}$. *Pak* $\operatorname{rank}(A) = k$, *právě když největší řád nenulového minoru* A *je* k.

DŮKAZ. Je-li $\operatorname{rank}(A) = k$, pak lze ze sloupců A vybrat nějakou bázi $(\mathbf{a}_{i_1}, \dots, \mathbf{a}_{i_k})$ prostoru $\operatorname{Im} A$. Protože $A' = (\mathbf{a}_{i_1}|\dots|\mathbf{a}_{i_k})$ má hodnost k, lze vybrat k-prvkovou bázi jejího řádkového prostoru. Výsledná $k\times k$ podmatice je regulární a má tedy nenulový determinant. Kdyby v A existoval nenulový minor vyššího řádu, pak by jeho sloupce byly lineárně nezávislé a tudíž by musely být lineárně nezávislé i příslušné sloupce matice A. To je ale v rozporu s tím, že každá lineárně nezávislá posloupnost $\operatorname{Im} A$ má nejvýše k prvků. □

Označme A_{ij} podmatici matice A vzniklou vyškrtnutím i-tého řádku a j-tého sloupce.

VĚTA 14 (Laplaceův rozvoj podle sloupce). *Nechť* $A \in \mathbb{F}^{n\times n}$, $j \in \{1,\dots,n\}$. *Pak*

$$\det A = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij})$$

DŮKAZ. Protože $\mathbf{a}_j = \sum_{i=1} a_{ij}\mathbf{e}_i$, dostáváme z linearity v j-tém sloupci

$$\det A = \sum_{i=1}^{n} a_{ij} \det(\mathbf{a}_1|\dots|\mathbf{a}_{j-1}|\mathbf{e}_i|\mathbf{a}_{j+1}|\dots|\mathbf{a}_n)$$

U determinantu v i-tém sčítanci je třeba $n-j$ transpozic na přesunutí j-tého sloupce na poslední pozici a $n-i$ transpozic na přesunutí i-tého řádku na poslední pozici, determinant se tím vynásobí faktorem $(-1)^{n-j+n-i} = (-1)^{i+j}$. Matice A', která takto vznikne, má podmatici A'_{nn} rovnu A_{ij}, a poslední sloupec $\mathbf{e}_n$. Její determinant je s využitím věty 12 roven

$$\det A' = \sum_{\pi\in S_n} \operatorname{sgn}\pi\ a'_{\pi(1),1}\dots a'_{\pi(n),n} \quad = \sum_{\substack{\pi\in S_n\\ \pi(n)=n}} \operatorname{sgn}\pi\ a'_{\pi(1),1}\dots a'_{\pi(n-1),n-1}a'_{n,n},$$

kde jsme se v posledním výrazu mohli omezit jen na permutace splňující $\pi(n) = n$, protože pro ostatní je $a'_{\pi(n),n} = 0$. Ale $a'_{n,n} = 1$ a $\operatorname{sgn}\pi = \operatorname{sgn}\pi'$ pro $\pi' \in S_{n-1}$ vzniklou zúžením π na množinu $\{1,\dots,n-1\}$. Tedy

$$\det A' = \sum_{\pi'\in S_{n-1}} \operatorname{sgn}\pi'\ a'_{\pi'(1),1}\dots a'_{\pi'(n-1),n-1} = \det(A'_{nn}) = \det(A_{ij})$$

Tedy determinant v i-tém sčítanci je roven $(-1)^{i+j}\det(A_{ij})$. □

Laplaceův rozvoj je vlastně rekurentní předpis pro determinant. Z věty 12 plyne, že jej lze provést i podle kteréhokoli řádku. Kombinace úprav a rozvoje podle řádku či sloupce s velkým počtem nul je obvykle nejrychlejší cesta k výpočtu determinantu:

$$\begin{vmatrix} 0 & 0 & 2 & 0 & 3 \\ 2 & 0 & 0 & 3 & 0 \\ 3 & 2 & 0 & 1 & 0 \\ 7 & 1 & 5 & 3 & 0 \\ 4 & 2 & 0 & 2 & 1 \end{vmatrix} = 2\begin{vmatrix} 2 & 0 & 3 & 0 \\ 3 & 2 & 1 & 0 \\ 7 & 1 & 3 & 0 \\ 4 & 2 & 2 & 1 \end{vmatrix} - 5\begin{vmatrix} 0 & 0 & 0 & 3 \\ 2 & 0 & 3 & 0 \\ 3 & 2 & 1 & 0 \\ 4 & 2 & 2 & 1 \end{vmatrix} =$$

$$2\begin{vmatrix} 2 & 0 & 3 \\ 3 & 2 & 1 \\ 7 & 1 & 3 \end{vmatrix} + 15\begin{vmatrix} 2 & 0 & 3 \\ 3 & 2 & 1 \\ 4 & 2 & 2 \end{vmatrix} = 2\begin{vmatrix} 2 & 0 & 3 \\ -11 & 0 & -5 \\ 7 & 1 & 3 \end{vmatrix} + 15\begin{vmatrix} 2 & 0 & 3 \\ -1 & 0 & -1 \\ 4 & 2 & 2 \end{vmatrix}$$

$$= -2\begin{vmatrix} 2 & 3 \\ -11 & -5 \end{vmatrix} - 30\begin{vmatrix} 2 & 3 \\ -1 & -1 \end{vmatrix} = -2(-10+33) - 30(-2+3) = -76$$

KAPITOLA 10

Aplikace determinantu

Jednou z nejstarších aplikací determinantu je explicitní určení řešení soustavy lineárních rovnic, tzv. Cramerovo pravidlo:

VĚTA 15. *Nechť $A \in \mathbb{F}^{n\times n}$ je regulární matice, $\mathbf{b} \in \mathbb{F}^n$. Označme $A_{i,\mathbf{b}}$ matici, která vznikne nahrazením i-tého sloupce A vektorem $\mathbf{b}$. Pak i-tá složka vektoru $\mathbf{x}$, který je jediným řešením soustavy rovnic $A\mathbf{x} = \mathbf{b}$, je rovna*

$$x_i = \frac{\det A_{i,\mathbf{b}}}{\det A}$$

DŮKAZ. Pro řešení SLR $A\mathbf{x} = \mathbf{b}$ platí $\sum_{j=1}^n x_j \mathbf{a}_j = \mathbf{b}$. Pak

$$\begin{aligned}
\det A_{i,\mathbf{b}} &= \det(\mathbf{a}_1|\ldots|\mathbf{a}_{i-1}|\sum_{j=1}^n x_j\mathbf{a}_j|\mathbf{a}_{i+1}|\ldots|\mathbf{a}_n) \\
&= \sum_{j=1}^n x_j \det(\mathbf{a}_1|\ldots|\mathbf{a}_{i-1}|\mathbf{a}_j|\mathbf{a}_{i+1}|\ldots|\mathbf{a}_n) \\
&= x_i \det(\mathbf{a}_1|\ldots|\mathbf{a}_{i-1}|\mathbf{a}_i|\mathbf{a}_{i+1}|\ldots|\mathbf{a}_n) = x_i \det A
\end{aligned}$$

Využili jsme linearitu v i-tém sloupci a fakt, že determinant matice se dvěma stejnými sloupci je roven 0. Je-li A regulární, pak $\det A \neq 0$, po vydělení $\det A$ dostáváme vyjádření x_i. □

Jednoduchým příkladem užití Cramerova pravidla je

$$\begin{pmatrix} 7 & 8 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 4 \\ 1 \end{pmatrix} \Rightarrow x_1 = \frac{\begin{vmatrix} 4 & 8 \\ 1 & 3 \end{vmatrix}}{\begin{vmatrix} 7 & 8 \\ 2 & 3 \end{vmatrix}} = \frac{4}{5}, \quad x_2 = \frac{\begin{vmatrix} 7 & 4 \\ 2 & 1 \end{vmatrix}}{\begin{vmatrix} 7 & 8 \\ 2 & 3 \end{vmatrix}} = -\frac{1}{5}$$

Pro větší soustavy je Gaussova eliminace rychlejší, ale i tak Cramerovo pravidlo nalézá využití v teorii, případně pro výpočet konkrétní i-té složky řešení, která nás zajímá.

Ve větě o Laplaceově rozvoji se vyskytly výrazy tvaru $(-1)^{i+j}\det(A_{ij})$, jimž se říká *algebraický doplněk prvku* a_{ij}. Matice, která má na pozici ij algebraický doplněk prvku a_{ji} (**pozor, indexy jsou obráceně!**) matice A, se nazývá *matice adjungovaná k* A a značí $\mathrm{adj}(A)$. Má jednoduchý vztah k matici inverzní:

VĚTA 16. *Nechť $A \in \mathbb{F}^{n\times n}$ je regulární. Pak $A^{-1} = \frac{1}{\det A}\mathrm{adj}(A)$.*

DŮKAZ. Jediným řešením soustavy rovnic $A\mathbf{x} = \mathbf{e}_j$ je j-tý sloupec matice A^{-1}. Podle Cramerova pravidla má x_i, tedy element A^{-1} na pozici ij, hodnotu $\frac{1}{\det A}\det A_{i,\mathbf{e}_j}$. Rozvojem podle i-tého sloupce dostáváme, že $\det A_{i,\mathbf{e}_j}$ je roven

$$\det(\mathbf{a}_1|\ldots|\mathbf{a}_{i-1}|\mathbf{e}_j|\mathbf{a}_{i+1}|\ldots|\mathbf{a}_n) = (-1)^{j+i}\det A_{ji} = \mathrm{adj}(A)_{ij}$$

□

Příklady 3.

$$A = \begin{pmatrix} 7 & 8 \\ 2 & 3 \end{pmatrix} \Rightarrow \operatorname{adj}(A) = \begin{pmatrix} 3 & -8 \\ -2 & 7 \end{pmatrix} \Rightarrow A^{-1} = \frac{1}{5}\begin{pmatrix} 3 & -8 \\ -2 & 7 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 0 & 5 \\ 1 & 0 & 1 \end{pmatrix}^{-1} = \frac{1}{2}\begin{pmatrix} \begin{vmatrix} 0 & 5 \\ 0 & 1 \end{vmatrix} & -\begin{vmatrix} 2 & 3 \\ 0 & 1 \end{vmatrix} & \begin{vmatrix} 2 & 3 \\ 0 & 5 \end{vmatrix} \\ -\begin{vmatrix} 4 & 5 \\ 1 & 1 \end{vmatrix} & \begin{vmatrix} 1 & 3 \\ 1 & 1 \end{vmatrix} & -\begin{vmatrix} 1 & 3 \\ 4 & 5 \end{vmatrix} \\ \begin{vmatrix} 4 & 0 \\ 1 & 0 \end{vmatrix} & -\begin{vmatrix} 1 & 2 \\ 1 & 0 \end{vmatrix} & \begin{vmatrix} 1 & 2 \\ 4 & 0 \end{vmatrix} \end{pmatrix},$$

což je po vyčíslení $\frac{1}{2}\left(\begin{smallmatrix} 0 & -2 & 10 \\ 1 & -2 & 7 \\ 0 & 2 & -8 \end{smallmatrix}\right)$. Pro větší matice než 3×3 se už vzorec nevyplatí, ale opět je užitečný pro teorii a pro získání konkrétního elementu inverzní matice bez nutnosti spočítat inverzní matici celou.

Je-li A regulární matice, existuje posloupnost elementárních matic $E_1, \dots, E_k$, která převede A na matici jednotkovou:

$$E_k \dots E_2 E_1 A = E$$

Pak ale $A^{-1} = E_k \dots E_2 E_1$ a $A = E_1^{-1} E_2^{-1} \dots E_k^{-1}$, a protože inverzní matice k elementární matici je elementární, plyne z toho, že každou regulární matici lze zapsat jako součin elementárních matic. Determinant elementární matice umíme snadno určit:

- matice přičtení násobku řádku do jiného řádku má determinant 1
- matice vynásobení řádku číslem r má determinant r
- matice prohození dvojice řádků má determinant -1.

Uvažujme nyní součin AB dvou čtvercových matic, přičemž $A = E_1 E_2 \dots E_k$, kde E_i jsou elementární matice. Pak jistě

$$\det(AB) = \det(E_1(E_2 \dots E_k B)) = \det(E_1)\det(E_2 \dots E_k B),$$

protože násobení maticí E_1 je řádková úprava matice $E_2 \dots E_k B$, která změní její determinant přesně stejně, jako kdyby se vynásobil číslem $\det E_1$. Opakováním stejné úvahy zjistíme, že

$$\det(AB) = \det(E_1)\det(E_2)\dots\det(E_k)\det(B)$$
$$\det(A) = \det(E_1)\det(E_2)\dots\det(E_k)$$

Odtud plyne

Věta 17. *Nechť $A, B \in \mathbb{F}^{n\times n}$. Pak $\det AB = \det A \det B$.*

Důkaz. Je-li A regulární, plyne věta z úvah výše. Je-li A singulární, pak je singulární i AB a obě mají determinant 0. □

Důsledek 9. *Nechť $A, R \in \mathbb{F}^{n\times n}$, R regulární. Pak*

(1) $\det(R^{-1}) = \frac{1}{\det R}$
(2) $\det(R^{-1}AR) = \det A$

Důkaz. První bod plyne z

$$\det(R^{-1})\det(R) = \det(R^{-1}R) = \det E = 1,$$

druhý z

$$\det(R^{-1}AR) = \det(R^{-1})\det A \det R = \frac{1}{\det R}\det A \det R = \det A$$

□

Podobné matice mají tedy stejný determinant. Pokud A je matice $[f]_B^B$ nějakého endomorfismu $f \in \mathrm{End}(V)$ vzhledem k bázi B a $A' = [f]_{B'}^{B'}$ je matice téhož endomorfismu vzhledem k bázi B', plyne z transformační formule, že $\det A = \det A'$. Následující definice je tedy korektní:

Definice 30. Nechť V je vektorový prostor konečné dimenze nad $\mathbb{F}$, B jeho báze a $f \in \mathrm{End}(V)$. Pak *determinant endomorfismu* f je determinant jeho matice $[f]_B^B$.

Uvažujme bázi $B = (v_1, \dots, v_n)$ reálného vektorového prostoru V a posloupnost $C = (w_1, \dots, w_n)$ vzniklou z posloupnosti B jednou z elementárních úprav definovaných nad tvrzením 19. Podle věty 9 existuje právě jeden endomorfismus $f_1 \in \mathrm{End}(V)$ takový, že $f_1(B) = C$, tedy že pro všechna $i \in \{1, \dots, n\}$ je $f_1(v_i) = w_i$. Nazývejme jej *elementární endomorfismus*. Snadno si rozmyslíme, že matice $E_1 := [f_1]_B^B$ je elementární matice, a že $\det E_1$ je až na znaménko roven poměru objemů rovnoběžnostěnů definovaných posloupnostmi $f_1(B)$ a B. Stačí si uvědomit, že při elementární úpravě prvního i druhého typu se zachovává $n-1$ vektorů, které můžeme vzít jako základnu rovnoběžnostěnu, a změna zbývajícího vektoru výšku měřenou od této základny buď nemění (úprava prvního typu), nebo násobí číslem r (úprava druhého typu). Úprava třetího typu rovnoběžnostěn nemění, jen ho zadává posloupností vektorů v jiném pořadí.

Obecný regulární endomorfismus f s maticí $A = [f]_B^B$ můžeme s pomocí rozkladu A na součin $E_1 E_2 \dots E_k$ elementárních matic chápat jako složení elementárních endomorfismů $f = f_1 \circ \dots \circ f_k$. Protože $\det A = \det E_1 \dots \det E_k$ je roven součinu koeficientů, jimiž endomorfismy f_i mění objem rovnoběžnostěnu určeného posloupností B, můžeme $\det A$ interpretovat jako podíl objemů $f(B)$ a B. Protože $\det f = \det A$ nezávisí na volbě báze B, můžeme determinant endomorfismu chápat jako koeficient, jímž se mění při zobrazení f objem libovolného rovnoběžnostěnu, nebo dokonce jakéhokoli útvaru ve V, který lze rovnoběžnostěny (infinitezimálně) pokrýt. Toto pozorování je základem teorie vícerozměrné integrace.

Definice 31. Nechť $B = (\mathbf{b}_1, \dots, \mathbf{b}_n)$ je báze $\mathbb{R}^n$. Pokud $\det(\mathbf{b}_1 | \dots | \mathbf{b}_n)$ je kladný, nazveme bázi B *pravotočivou*, pokud je záporný, pak *levotočivou*. Levotočivost nebo pravotočivost báze nazýváme souhrnně její *orientací*.

Z úvah výše vyplývá, že elementární úprava nemění orientaci báze, právě když je determinant příslušné elementární matice kladný. Tedy znaménko $\det f$ vyjadřuje, zda mají báze B a $f(B)$ stejnou orientaci. I v případě bází v reálném vektorovém prostoru V, který není aritmetický, můžeme zavést orientaci jako rozdělení množiny všech bází na dvě třídy ekvivalence vzhledem k relaci „existuje endomorfismus $f \in \mathrm{End}(V)$ s kladným determinantem, který zobrazuje jednu na druhou“ nebo ekvivalentně „matice přechodu mezi těmito bázemi má kladný determinant“.

Další veličinou, která se zachovává při podobnosti je *stopa matice* $A \in \mathbb{F}^{n \times n}$, definovaná jako $\mathrm{Tr}\, A = \sum_{i=1}^n a_{ii}$, tedy součet prvků na diagonále. Pro $A \in \mathbb{F}^{n \times p}$, $B \in \mathbb{F}^{p \times q}$, $C \in \mathbb{F}^{q \times n}$ platí

$$\mathrm{Tr}\, ABC = \sum_{i=1}^{n} \sum_{j=1}^{p} \sum_{k=1}^{q} a_{ij} b_{jk} c_{ki} = \sum_{j=1}^{p} \sum_{k=1}^{q} \sum_{i=1}^{n} b_{jk} c_{ki} a_{ij} = \mathrm{Tr}\, BCA,$$

tzv. *cykličnost stopy*. Odtud pak

$$\mathrm{Tr}\, R^{-1} A R = \mathrm{Tr}\, R R^{-1} A = \mathrm{Tr}\, A$$

Proto i stopu lze definovat pro libovolný endomorfismus $f \in \mathrm{End}(V)$ jako stopu $\mathrm{Tr}[f]_B^B$ jeho libovolné matice. Další maticové veličiny, které lze takto vztáhnout na příslušné endomorfismy (tzv. *invarianty*, protože nezávisí na zvolené reprezentaci) potkáme v kapitole o diagonalizaci.

KAPITOLA 11

Diagonalizace

Diagonalizace $n \times n$ matice A je hledání diagonální matice

$$D = \begin{pmatrix} \lambda_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \lambda_n \end{pmatrix} =: \operatorname{diag}(\lambda_1, \dots, \lambda_n),$$

splňující pro nějakou regulární matici R vztah

$$A = RDR^{-1}$$

Protože $D^k = \operatorname{diag}(\lambda_1^k, \dots, \lambda_n^k)$ a

$$A^k = \underbrace{RDR^{-1}RDR^{-1}\dots RDR^{-1}}_{k} = RD^kR^{-1},$$

stačí nám znalost D a R k nalezení libovolné mocniny matice A. Protože $A = [F_A]_K^K$, lze vztah $D = R^{-1}AR$ chápat jako transformační formuli

$$[F_A]_B^B = [\mathrm{Id}]_K^B \; [F_A]_K^K \; [\mathrm{Id}]_B^K,$$

pro nějakou vhodnou bázi B, zvanou *báze z vlastních vektorů*. Budeme se tedy nejprve zabývat tím, jak se taková báze dá nalézt.

1. Vlastní čísla a vlastní vektory

DEFINICE 32. Nechť V je vektorový prostor nad $\mathbb{F}$. Číslo $\lambda \in \mathbb{F}$ je *vlastním číslem* endomorfismu $f \in \operatorname{End}(V)$, pakliže pro nějaký nenulový vektor $v \in V$ platí $f(v) = \lambda v$. Každý vektor, který toto splňuje, se nazývá *vlastním vektorem* f příslušným vlastnímu číslu λ.

Podmínku $f(v) = \lambda v$ lze přepsat jako $(f - \lambda \mathrm{Id})(v) = 0$. Vlastní vektory jsou tedy prvky $V_\lambda := \operatorname{Ker}(f - \lambda \mathrm{Id})$ neboli *vlastního podprostoru endomorfismu f příslušného vlastnímu číslu λ.*

Dle definice je λ vlastní číslo f, pakliže $\operatorname{Ker}(f - \lambda \mathrm{Id}) \neq 0$. Je-li $\dim V = n$ a C báze V, nastává to právě když $[f - \lambda \mathrm{Id}]_C^C$ je singulární matice. V označení $[f]_C^C = A$ to znamená, že

$$\det(A - \lambda E) \equiv \begin{vmatrix} a_{11} - \lambda & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} - \lambda & & \vdots \\ \vdots & & \ddots & \\ a_{n1} & \dots & & a_{nn} - \lambda \end{vmatrix} = 0$$

PŘÍKLAD 16. Pro $n = 2$ a $n = 3$ můžeme přímým výpočtem ověřit, že

$$\begin{vmatrix} a_{11} - \lambda & a_{12} \\ a_{21} & a_{22} - \lambda \end{vmatrix} = (-\lambda)^2 + (a_{11} + a_{22})(-\lambda) + (a_{11}a_{22} - a_{21}a_{12})$$
$$= \lambda^2 - \operatorname{Tr} A \; \lambda + \det A$$

$$\det(A - \lambda E) = (-\lambda)^3 + (\operatorname{Tr} A)(-\lambda)^2 + (\operatorname{Tr}(\operatorname{adj}(A)))(-\lambda) + \det A$$

DEFINICE 33. *Charakteristickým polynomem matice* $A \in \mathbb{F}^{n\times n}$ nazýváme polynom $p_A(\lambda) := \det(A - \lambda E)$. *Charakteristický polynom endomorfismu* f je $\det(f - \lambda\,\mathrm{Id})$, čili charakteristický polynom jeho libovolné matice $[f]_C^C$.

Charakteristický polynom $n \times n$ matice má stupeň n a koeficient $(-1)^n$ u λ^n, protože jediný sčítanec v definici determinantu $\det(A - \lambda E)$, který k λ^n přispívá, je ten odpovídající identické permutaci. Protože každý sčítanec odpovídající neidentické permutaci obsahuje alespoň jeden činitel nad diagonálou a alespoň jeden činitel pod ní, pochází i koeficient λ^{n-1} pouze ze součinu diagonálních elementů $(a_{11} - \lambda)\dots(a_{nn} - \lambda)$ a je tedy roven $(-1)^{n-1}\operatorname{Tr} A$ u λ^{n-1}. Absolutní člen $p_A(\lambda)$ je roven $p_A(0)$, tedy $\det A$.

Obecný koeficient u λ^{n-k} roven

$$(-1)^{n-k} \sum_{\substack{I\subset\{1,\dots,n\}\\ |I|=k}} \det(A_{II}),$$

kde A_{II} je $k \times k$ podmatice A vzniklá vynecháním všech řádků a sloupců, jejichž indexy nejsou v množině I. Speciálně koeficient u λ je roven $-\sum_{i=1}^n \det(A_{ii}) \equiv -\operatorname{Tr}(\operatorname{adj}(A))$, kde A_{ii} je $n-1 \times n-1$ podmatice vzniklá vynecháním i-tého řádku i sloupce. Nejlépe je to vidět, když si představíme každé λ na diagonále $\det(A - \lambda E)$ obarvené jinou barvou a nahlédneme, že koeficient u i-tého barevného λ je právě $\det(A_{ii})$.

PŘÍKLADY 4.

(1) Zobrazení $f : P^n(x,\mathbb{R}) \to P^n(x,\mathbb{R})$ definované jako derivace polynomu $[f(p)](x) := \frac{d}{dx}p(x)$ má jediné vlastní číslo 0, vlastní podprostor je tvořen konstantními polynomy.
(2) Vlastními čísly $D = \operatorname{diag}(d_1,\dots,d_n)$ jsou $d_1,\dots,d_n$ a příslušné vlastní podprostory jsou (pro případ vzájemně různých d_i) lineární obaly prvků kanonické báze $\langle \mathbf{e}_1\rangle,\dots,\langle \mathbf{e}_n\rangle \in \mathbb{C}^n$.
(3) Pokud $Ax = \lambda x$ a A je regulární, pak $A^{-1}x = \lambda^{-1}x$, čili inverzní matice má stejné vlastní podprostory, ale převrácená vlastní čísla.
(4) Pokud $A = Q^{-1}BQ$, pak $Ax = \lambda x$ znamená $BQx = \lambda Qx$, tedy λ je vlastním číslem B s vlastním vektorem Qx. Podobné matice mají tedy stejná vlastní čísla.
(5) $\det(A^T - \lambda E) = \det(A - \lambda E)^T = \det(A - \lambda E)$, tedy A^T má stejná vlastní čísla jako A.

2. Diagonalizace matice

Vlastní čísla lze tedy nalézt jako kořeny charakteristického polynomu. Teorie se zjednoduší, když budeme moci předpokládat, že A je komplexní matice a vlastní čísla také hledáme v $\mathbb{C}$. Opíráme se přitom o tzv. Základní větu algebry:

VĚTA 18. *Každý nekonstantní polynom s komplexními koeficienty má alespoň jeden kořen v* $\mathbb{C}$.

Důkaz je nad rámec kurzu. Můžeme ale odvodit jednoduchý důsledek:

DŮSLEDEK 10. *Nechť* $p(x)$ *je polynom stupně* $n > 0$ *s komplexními koeficienty. Pak má* n *komplexních kořenů včetně násobností.*

Důkaz indukcí. Pro $n = 1$ zjevně platí. Nechť $x_0 \in \mathbb{C}$ je kořen $p(x) = \sum_{i=0}^n a_i x^i$. Pak $p(x) = p(x) - p(x_0) = \sum_{i=0}^n a_i(x^i - x_0^i)$, což lze zapsat jako$(x - x_0)q(x)$, kde $q(x)$ je polynom stupně $n-1$. Ten má z indukčního předpokladu $n-1$ kořenů včetně násobností. Tedy $p(x)$ má n kořenů včetně násobností.

DEFINICE 34. Množina všech vlastních čísel matice A se nazývá její *spektrum*, značí se $\sigma(A)$. Pro $\lambda_i \in \sigma(A)$ je jeho *algebraická násobnost* definována jako násobnost λ_i coby kořenu $p_A(\lambda)$, a jeho *geometrická násobnost* jako dimenze prostoru $\operatorname{Ker}(A - \lambda_i E)$. Analogicky jsou definovány tytéž pojmy pro endomorfismus.

LEMMA 5. *Nechť V je vektorový prostor nad $\mathbb{F}$ dimenze n, $f \in \operatorname{End}(V)$ a pro všechny prvky množiny $M = \{\lambda_1, \ldots, \lambda_k\}$ je zvolena nějaká báze B_i vlastního prostoru V_{λ_i}. Pak je množina $B = B_1 \cup \ldots \cup B_k$ lineárně nezávislá.*

DŮKAZ. Uvažujme množinu $N \subset V$ nenulových vektorů, v níž každý prvek patří jinému vlastnímu prostoru V_{λ_i}. Je-li N lineárně závislá, lze z ní vybrat bázi $N' = \{v_{i_1}, \ldots, v_{i_q}\}$ jejího lineárního obalu, kde $v_{i_j} \in V_{\lambda_{i_j}}$, a vyjádřit nějaký $v_j \in N \setminus N'$ jako $v_j = \sum_{p=1}^q r_p v_{i_p}$. Je-li $v_j \in V_{\lambda_j}$, pak $f(v_j) = \lambda_j v_j = \sum_{p=1}^q r_p \lambda_j v_{i_p}$, ale zároveň

$$f(v_j) = \sum_{p=1}^{q} r_p f(v_{i_p}) = \sum_{p=1}^{q} r_p \lambda_{i_p} v_{i_p}$$

Tedy $\sum_{p=1}^q r_p(\lambda_{i_p} - \lambda_j)v_{i_p} = 0$. Protože žádný rozdíl $\lambda_{i_p} - \lambda_j$ není 0 a i některé r_p musí být nenulové, je to ve sporu s lineární nezávislostí N'. Tedy N nemůže být lineárně závislá.

Označme nyní $B_i = (w_{i1}, \ldots, w_{in_i})$ a uvažujme lineární kombinaci ve tvaru

$$\sum_{i_1=1}^{n_1} r_{1i_1} w_{1i_1} + \ldots + \sum_{i_k=1}^{n_k} r_{ki_k} w_{ki_k} = o$$

Označme jednotlivé sumy jako $v_1, \ldots, v_k$, pak $v_j \in V_{\lambda_j}$. Kdyby byly některé z vektorů $v_1, \ldots, v_k$ nenulové, pak bychom měli jejich lineární kombinaci rovnou nulovému vektoru, což podle úvahy z prvního odstavce nemůže nastat. Tedy musí být všechny v_j nulové, a protože posloupnosti B_j jsou lineárně nezávislé, musí být pak nulové i všechny koeficienty r_{ji_j}. Tedy B je lineárně nezávislá. $\square$

Je-li V nad $\mathbb{C}$, $M = \sigma(f)$ a každé vlastní číslo f má stejnou algebraickou i geometrickou násobnost, pak $|B| = n$ a je to tedy na základě lemmatu báze V. Speciálně to musí nastat v případě, že jsou všechny algebraické násobnosti všech $\lambda_i \in \sigma(f)$ rovny jedné. Protože $\dim \operatorname{Ker}(f - \lambda_i \operatorname{Id})$ je vždy alespoň 1, má B alespoň n prvků, a protože je lineárně nezávislá, musí jich mít právě n.

Předpokládejme nyní, že pro $f \in \operatorname{End}(V)$ v prostoru V máme bázi $B = (v_1, \ldots, v_n)$ složenou z vlastních vektorů f. Pokud $v_i \in V_\lambda$ pro nějaké $\lambda_i \in \sigma(f)$, pak $f(v_i) = \lambda_i v_i$, neboli $[f(v_i)]^B = \lambda_i \mathbf{e}_i$. Pak ale

$$[f]_B^B = \big([f(v_1)]^B \big| \ldots \big| [f(v_n)]^B\big) = \begin{pmatrix} \lambda_1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & \lambda_n \end{pmatrix}$$

V tomto vztahu na rozdíl od lemmatu 5 nepředpokládáme všechna λ_i vzájemně různá. Speciálně pro $f = F_A$ s bází z vlastních vektorů $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ máme

$$\begin{aligned} A \equiv [F_A]_K^K &= [\operatorname{Id}]_B^K \; [F_A]_B^B \; [\operatorname{Id}]_K^B = \\ &= (\mathbf{v}_1|\ldots|\mathbf{v}_n) \begin{pmatrix} \lambda_1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & \lambda_n \end{pmatrix} (\mathbf{v}_1|\ldots|\mathbf{v}_n)^{-1} \end{aligned}$$

PŘÍKLAD 17. Diagonalizujme matici $A = \begin{pmatrix} 1 & 1 \\ -3 & 5 \end{pmatrix}$. Char. polynom je

$$p_A(\lambda) = \lambda^2 - \operatorname{Tr} A \; \lambda + \det A = \lambda^2 - 6\lambda + 8 = (\lambda - 2)(\lambda - 4)$$

Tedy $\sigma(A) = \{2, 4\}$. Vlastní podprostory pak jsou

$$V_4 = \operatorname{Ker}\begin{pmatrix}-3 & 1\\ -3 & 1\end{pmatrix} = \left\langle \begin{pmatrix}1\\3\end{pmatrix}\right\rangle, \; V_2 = \operatorname{Ker}\begin{pmatrix}-1 & 1\\ -3 & 3\end{pmatrix} = \left\langle \begin{pmatrix}1\\1\end{pmatrix}\right\rangle$$

Tedy

$$A = \begin{pmatrix}1 & 1\\ -3 & 5\end{pmatrix} = \begin{pmatrix}1 & 1\\ 3 & 1\end{pmatrix}\begin{pmatrix}4 & 0\\ 0 & 2\end{pmatrix}\frac{1}{(-2)}\begin{pmatrix}1 & -1\\ -3 & 1\end{pmatrix}$$

Má-li A včetně násobností n vlastních čísel, pak je její charakteristický polynom rozložitelný, tj.

$$\begin{aligned} p_A(\lambda) &\equiv (-\lambda)^n + \operatorname{Tr} A(-\lambda)^{n-1} + \ldots + \det(A)\\ &= (\lambda_1 - \lambda)(\lambda_2 - \lambda)\ldots(\lambda_n - \lambda)\\ &= (-\lambda)^n + (\lambda_1 + \ldots + \lambda_n)(-\lambda)^{n-1} + \ldots + \lambda_1\lambda_2\ldots\lambda_n \end{aligned}$$

Z porovnání absolutních členů vidíme, že $\det A$ je roven součinu všech n vlastních čísel a $\operatorname{Tr} A$ je rovna součtu všech vlastních čísel. Charakteristický polynom, vlastní čísla a jejich algebraické i geometrické násobnosti, stopa, determinant i ostatní koeficienty charakteristického polynomu se nemění při podobnostní transformaci $A \to R^{-1}AR$. Jsou to tedy invarianty, lze je zavést i pro endomorfismy, se zachováním vztahů mezi nimi. Jeden takový, který platí pro 2×2 matice a lze jej snadno ověřit přímým výpočtem, je

$$\det A = \frac{1}{2}(\operatorname{Tr}(A)^2 - \operatorname{Tr}(A^2))$$

Obecně platí, že koeficienty $p_A(\lambda)$ lze vždy vyjádřit pomocí $\operatorname{Tr}(A^k)$, $k \leq n$.

Některé endomorfismy a matice diagonalizovatelné nejsou, protože lineárně nezávislá množina $B = B_1 \cup \ldots \cup B_k$ neobsahuje dost vektorů, aby to byla báze. Příkladem je třeba matice

$$A = \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix} \;\Rightarrow\; \sigma(A) = \{0\}, \text{ tedy } \; V_0 = \left\langle \begin{pmatrix}1\\0\end{pmatrix}\right\rangle,$$

nebo endomorfismus D prostoru $V = P^n(x, \mathbb{C})$, který přiřazuje polynomu $p(x)$ jeho první derivaci podle x. Pokud definujeme ve V bázi $C = (1, x, \frac{x^2}{2}, \ldots, \frac{x^n}{n!})$, spojuje ji D do řetízku

$$0 \xleftarrow{D} 1 \xleftarrow{D} x \xleftarrow{D} \tfrac{x^2}{2} \xleftarrow{D} \ldots \xleftarrow{D} \tfrac{x^{n-1}}{(n-1)!} \xleftarrow{D} \tfrac{x^n}{n!} \;,$$

z něhož lze vyčíst, že

$$[D]_C^C = \begin{pmatrix}0 & 1 & 0 & \ldots & 0 & 0\\ 0 & 0 & 1 & \ldots & 0 & 0\\ \vdots & & & \ddots & 0 & 0\\ 0 & 0 & 0 & \ldots & 1 & 0\\ 0 & 0 & 0 & \ldots & 0 & 1\\ 0 & 0 & 0 & \ldots & 0 & 0\end{pmatrix}$$

Matice tohoto typu se objevují v teorii Jordanova tvaru, která řeší otázku matic, které diagonalizovatelné nejsou.

Příklad 18. Rotace v rovině $\mathbb{R}^2$ o pravý úhel má matici vzhledem ke K

$$[F_A]_K^K \equiv A = \begin{pmatrix}\cos\frac{\pi}{2} & -\sin\frac{\pi}{2}\\ \sin\frac{\pi}{2} & \cos\frac{\pi}{2}\end{pmatrix} = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} \in \mathbb{R}^{2\times 2}$$

Ta má charakteristický polynom $\lambda^2 + 1$, tedy nemá reálná vlastní čísla, ani nemá v $\mathbb{R}^2$ žádné vlastní vektory. Chápeme-li ale F_A jako endomorfismus prostoru $\mathbb{C}^2$, pak $\sigma(A) = \{i, -i\}$ a příslušné vlastní podprostory jsou $\langle(1,-i)\rangle$, resp. $\langle(1,i)\rangle$. Diagonalizace pak má tvar

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

Pro obecnou matici rotace se dá analogicky spočítat, že

$$\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix} \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{-i\alpha} \end{pmatrix} \frac{1}{2i} \begin{pmatrix} i & -1 \\ i & 1 \end{pmatrix}$$

3. Diagonalizace symetrické matice

Nechť $A \in \mathbb{C}^{m\times n}$, pak $\bar{A}$ označuje matici stejného typu, jejíž každý element $\bar{a}_{ij}$ je komplexně sdružený k odpovídajícímu elementu a_{ij} matice A. Matice $A^+ := \bar{A}^T$ se nazývá matice *hermitovsky sdružená* k matici A.

Tvrzení 35. *Nechť $A \in \mathbb{C}^{m\times n}$, $B \in \mathbb{C}^{n\times p}$. Pak*

$$(AB)^+ = B^+A^+$$

Pokud $m = n$ a A je regulární, pak $(A^+)^{-1} = (A^{-1})^+$.

Důkaz. Z vlastností operací na $\mathbb{C}$ plyne, že $\overline{AB} = \bar{A}\bar{B}$. Vztah $(AB)^+ = B^+A^+$ pak plyne z tvrzení 6. Druhá část věty vyplývá z $(A^{-1})^+A^+ = (AA^{-1})^+ = E^+ = E$ a jednoznačnosti inverzní matice. □

Pokud $A^+ = A$, říkáme, že A je *hermitovská matice.*

Věta 19. *Nechť $A \in \mathbb{C}^{n\times n}$ je hermitovská matice. Pak každé její vlastní číslo je reálné.*

Důkaz. Pokud $\lambda \in \mathbb{C}$, $\mathbf{v} \in \mathbb{C}^n$ splňují $A\mathbf{v} = \lambda\mathbf{v}$, máme z tvrzení 35 i $\mathbf{v}^+A^+ = \bar{\lambda}\mathbf{v}^+$. Pak s využitím $A = A^+$

$$\lambda\mathbf{v}^+\mathbf{v} = \mathbf{v}^+A\mathbf{v} = \mathbf{v}^+A^+\mathbf{v} = \bar{\lambda}\mathbf{v}^+\mathbf{v}$$

Protože $\mathbf{v}^+\mathbf{v} = \sum_{i=1}^n |v_i|^2 \neq 0$ pro $\mathbf{v} \neq 0$, musí být $\lambda = \bar{\lambda}$. □

Speciálním případem hermitovské matice je reálná symetrická matice, tedy $A = A^T$. Pokud $\lambda \in \mathbb{R}$ je její vlastní číslo, pak i $A - \lambda E$ je reálná matice a báze jejího jádra sestává z vektorů z $\mathbb{R}^n$.

Tvrzení 36. *Nechť $A \in \mathbb{R}^{n\times n}$ je symetrická matice, λ, μ dvě různá vlastní čísla matice A, $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$ příslušné vlastní vektory, tj. $\mathbf{v} \in V_\lambda$, $\mathbf{w} \in V_\mu$. Pak $\mathbf{v} \perp \mathbf{w}$.*

Důkaz. Z $A\mathbf{v} = \lambda\mathbf{v}$ a $A\mathbf{w} = \mu\mathbf{w}$ plyne, že

$$\mu\mathbf{v}^T\mathbf{w} = \mathbf{v}^TA\mathbf{w} = \mathbf{v}^TA^T\mathbf{w} = (A\mathbf{v})^T\mathbf{w} = \lambda\mathbf{v}^T\mathbf{w}$$

Protože $\lambda \neq \mu$, musí být $\mathbf{v}^T\mathbf{w} = 0$, neboli $\mathbf{v} \perp \mathbf{w}$. □

Má-li matice A všech n vlastních čísel vzájemně různých, je v bázi z vlastních vektorů každý vektor kolmý na každý jiný. Takové bázi se říká *ortogonální.* Později ukážeme, že ortogonální bázi z vlastních vektorů lze najít pro každou symetrickou matici.

Z každé ortogonální báze $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ v $\mathbb{R}^n$ lze vytvořit bázi $\left(\frac{\mathbf{v}_1}{\|\mathbf{v}_1\|}, \ldots, \frac{\mathbf{v}_n}{\|\mathbf{v}_n\|}\right)$, která je stále ortogonální a navíc má každý vektor normu 1. Taková báze se nazývá *ortonormální.* Protože $\|\mathbf{v}\|^2 = \mathbf{v}^T\mathbf{v}$, plyne odtud

Tvrzení 37. *Nechť $B = (\mathbf{u}_1, \ldots, \mathbf{u}_n)$ je ortonormální báze $\mathbb{R}^n$, $U = [\mathrm{Id}]^K_B$. Pak $U^T = U^{-1}$.*

Důkaz. Platí $U^TU = (\mathbf{u}_1|\ldots|\mathbf{u}_n)^T(\mathbf{u}_1|\ldots|\mathbf{u}_n) = E$. □

Reálná čtvercová matice U s vlastností $U^T U = E$ se nazývá *ortogonální matice*. Pokud tedy A je reálná $n \times n$ symetrická matice, která má n vzájemně různých vlastních čísel, víme, že musí existovat ortogonální matice U taková, že $U^T A U$ je diagonální.

Několik pozorování k ortogonálním maticím:

(1) Endomorfismus $F_R \in \mathrm{End}(\mathbb{R}^n)$, kde R je ortogonální, zachovává normu, neboť $\|R\mathbf{v}\|^2 = \mathbf{v}^T R^T R \mathbf{v} = \|\mathbf{v}\|^2$.

(2) Zachovává i skalární součin, protože ten lze vyjádřit pomocí norem
$$\mathbf{v}^T \mathbf{w} = \frac{1}{4}(\|\mathbf{v} + \mathbf{w}\|^2 - \|\mathbf{v} - \mathbf{w}\|^2)$$
Stačí ověřit, že $\|\mathbf{v} \pm \mathbf{w}\|^2 = \mathbf{v}^T \mathbf{v} \pm 2\mathbf{v}^T \mathbf{w} + \mathbf{w}^T \mathbf{w}$.

(3) Naopak každá čtvercová matice U, která zachovává skalární součin, tedy $(U\mathbf{v})^T U\mathbf{w} = \mathbf{v}^T \mathbf{w}$ pro libovolné $\mathbf{v}, \mathbf{w}$, je ortogonální, protože $(U\mathbf{e_i})^T U\mathbf{e_j} = \mathbf{e_i}^T U^T U \mathbf{e}_j$ se rovná ij-tému elementu matice $U^T U$ a $\mathbf{e_i}^T \mathbf{e}_j$ je 1 právě když $i = j$, jinak 0. Tedy například matice rotace vzhledem ke kanonické bázi je také ortogonální matice.

(4) Snadno se ověří, že množina všech $n \times n$ ortogonálních matic tvoří grupu, tedy součin dvou ortogonálních matic je ortogonální matice a $U^{-1} = U^T$ je ortogonální matice, pokud U je ortogonální matice. Pak i matice $U^T R U$, kde U, R jsou ortogonální, je ortogonální. Pokud tedy B je ortonormální báze a $U = [\mathrm{Id}]^K_B$, pak $[F_R]^B_B$ je ortogonální matice, neboli zobrazení určené ortogonální maticí vzhledem ke kanonické bázi je reprezentované ortogonální maticí i ke všem ostatním ortonormálním bázím.

(5) Chápeme-li F_R, kde R je reálná ortogonální matice, jako endomorfismus prostoru $\mathbb{C}^n$ a $\mathbf{v} \in \mathbb{C}$ je jeho nenulový vlastní vektor příslušný vlastnímu číslu $\lambda \in \mathbb{C}$, pak
$$\bar{\lambda}\lambda \mathbf{v}^+ \mathbf{v} = (R\mathbf{v})^+ (R\mathbf{v}) = \mathbf{v}^+ R^+ R \mathbf{v} = \mathbf{v}^+ R^T R \mathbf{v} = \mathbf{v}^+ \mathbf{v},$$
tedy musí být $\bar{\lambda}\lambda = |\lambda|^2 = 1$, neboli vlastní čísla F_R musí ležet na jednotkové kružnici v $\mathbb{C}$.

Podrobněji se těmito vlastnostmi budeme zabývat v kapitole o obecném skalárním součinu v letním semestru.

KAPITOLA 12

Direktní součet

Připomeňme z první kapitoly ortogonální projekci $P_{\mathbf{x}} \in \mathrm{End}(\mathbb{R}^n)$ do směru nenulového vektoru $\mathbf{x} \in \mathbb{R}^n$:

$$P_{\mathbf{x}}(\mathbf{y}) = \frac{\mathbf{x}.\mathbf{y}}{\|\mathbf{x}\|^2}\mathbf{x}$$

Zvolme $B_1 = (r\mathbf{x})$ bázi prostoru $\langle \mathbf{x} \rangle$ a $B_2 = (\mathbf{u}_1, \ldots, \mathbf{u}_{n-1})$ nějakou bázi ortogonálního doplňku $\mathbf{x}^\perp$. Pro bázi $\mathbb{R}^n$ ve tvaru $B = (r\mathbf{x}, \mathbf{u}_1, \ldots, \mathbf{u}_{n-1})$ má reprezentace $P_{\mathbf{x}}$ jednoduchý tvar

$$[P_{\mathbf{x}}]_B^B = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \ldots & 0 \end{pmatrix}$$

Máme tedy dvojici podprostorů $W_1 := \langle \mathbf{x} \rangle$, $W_2 := \mathbf{x}^\perp$ takových, že sjednocením jejich bází B_1, B_2 vznikne báze celého prostoru. Právě taková konfigurace se popisuje pomocí direktního součtu.

1. Součet a direktní součet

Definice 35. Nechť V je vektorový prostor nad $\mathbb{F}$ a W_1, W_2 jeho dva podprostory. Pak jejich ***součtem*** $W_1 + W_2$ je množina všech vektorů, které lze zapsat jako součet $w_1 + w_2$, kde $w_i \in W_i$. Pokud navíc $W_1 \cap W_2 = 0$, nazýváme $W_1 + W_2$ ***direktní součet podprostorů*** a označujeme jej $W_1 \oplus W_2$. Pokud $W_1 \oplus W_2 = V$, pak W_2 je ***doplňkem podprostoru*** W_1 ve V.

Příklady 5. V $\mathbb{R}^3$ jsou co do možných dimenzí tři netriviální příklady součtu podprostorů:

- Dvě různé přímky, např. $\left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right\rangle \oplus \left\langle \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\rangle$
- Dvě různé roviny, např. $\left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\rangle + \left\langle \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle = \mathbb{R}^3$, ale součet není direktní, protože průnikem rovin je jejich průsečnice.
- Rovina a přímka v ní neležící, např. $\left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\rangle \oplus \left\langle \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle = \mathbb{R}^3$.

Zbylé možnosti by zahrnovaly buď triviální podprostory 0 a $\mathbb{R}^3$, nebo situaci, kdy je jeden podprostor rovný druhému podprostoru nebo je jeho podprostorem.

Tvrzení 38. *Každý prvek $W_1 \oplus W_2$ lze zapsat jako součet vektoru z $w_1 \in W_1$ a vektoru $w_2 \in W_2$ právě jedním způsobem.*

Důkaz. Stačí ukázat jednoznačnost. Pokud by existovaly $w_1, w_1' \in W_1$, $w_2, w_2' \in W_2$ takové, že $w_1 + w_2 = w_1' + w_2'$, pak $w_1 - w_1' = w_2' - w_2$. Levá strana rovnosti patří do W_1, pravá do W_2, musí tedy být obě nula. $\square$

TVRZENÍ 39. *Pokud W_1, W_2 jsou podprostory ve V, pak $W_1 + W_2 = \langle W_1 \cup W_2 \rangle$, tedy součet podprostorů je také podprostor. Pokud M_1 je množina generátorů W_1 a M_2 je množina generátorů W_2, pak jejich sjednocení $M_1 \cup M_2$ generuje $W_1 + W_2$.*

DŮKAZ. Každý součet vektorů $w_1 + w_2$ je lineární kombinací prvků z $W_1 \cup W_2$ a lze jej zapsat jako lineární kombinaci prvků z $M_1 \cup M_2$. Naopak každou lineární kombinaci prvků z $W_1 \cup W_2$ lze zapsat jako součet vektoru z W_1 a z W_2, stejně tak pro lineární kombinaci prvků z $M_1 \cup M_2$. □

Tuto charakterizaci součtu můžeme rozšířit na součet libovolného množství podprostorů:

DEFINICE 36. Nechť $\mathcal{W}$ je množina podprostorů ve vektorovém prostoru V. Pak definujeme jejich *součet* jako

$$\sum_{W \in \mathcal{W}} W := \left\langle \bigcup_{W \in \mathcal{W}} W \right\rangle$$

I zde je zřejmé, že sjednocení množin generátorů jednotlivých podprostorů generuje jejich součet. Je třeba si uvědomit, že ačkoli množina $\mathcal{W}$ může být nekonečná, v $\sum_{W \in \mathcal{W}} W$ se vyskytují jen součty konečně mnoha vektorů.

VĚTA 20 (O dimenzi spojení a průniku). *Nechť $W_1, W_2 \leq V$, oba konečné dimenze. Pak*

$$\dim W_1 + W_2 = \dim W_1 + \dim W_2 - \dim W_1 \cap W_2$$

DŮKAZ. Nechť $(u_1, \dots, u_p)$ je báze $W_1 \cap W_2$. Doplňme ji podle důsledku 2 na bázi $(u_1, \dots, u_p, v_1, \dots, v_q)$ prostoru W_1 a na bázi $(u_1, \dots, u_p, w_1, \dots, w_r)$ prostoru W_2. Posloupnost $(u_1, \dots, u_p, v_1, \dots, v_q, w_1, \dots, w_r)$ generuje $W_1 + W_2$, ukážeme, že je lineárně nezávislá. Pokud

$$\sum_{i=1}^{p} a_i u_i + \sum_{i=1}^{q} b_i v_i + \sum_{i=1}^{r} c_i w_i = o$$

pro nějaké skaláry a_i, b_i, c_i, pak $\sum a_i u_i + \sum b_i v_i = -\sum c_i w_i$ je vektor, který je díky tvaru levé strany ve W_1 a zároveň díky tvaru pravé strany ve W_2. Je tedy ve $W_1 \cap W_2$ a lze jej zapsat jako $\sum_{i=1}^{p} d_i u_i$. Pak ale

$$\sum_{i=1}^{p} d_i u_i + \sum_{i=1}^{r} c_i w_i = o,$$

což z lineární nezávislosti posloupnosti $(u_1, \dots, u_p, w_1, \dots, w_r)$ znamená, že všechny koeficienty d_i, c_i jsou rovny nule. Pak ale

$$\sum_{i=1}^{p} a_i u_i + \sum_{i=1}^{q} b_i v_i = o,$$

takže z lineární nezávislosti $(u_1, \dots, u_p, v_1, \dots, v_q)$ dovodíme, že i všechny a_i, b_i jsou rovny nule. Tedy $(u_1, \dots, u_p, v_1, \dots, v_q, w_1, \dots, w_r)$ je báze $W_1 + W_2$ a stačí jen ověřit, že dimenze splňují

$$p + q + r = (p + q) + (p + r) - p$$

□

Pro direktní součet tedy platí $\dim W_1 \oplus W_2 = \dim W_1 + \dim W_2$. Navíc posloupnost (B_1, B_2), kde B_i je báze W_i, je bází $W_1 \oplus W_2$. Chceme definovat direktní součet více než dvou podprostorů tak, aby pro něj platily analogické vlastnosti. Mohli bychom zkusit požadovat, že součet tří podprostorů W_1, W_2, W_3 je direktní, pokud všechny průniky dvojic i celé trojice jsou nulové, ale to nefunguje: stačí uvažovat tři různé přímky v $\mathbb{R}^3$, z jejich průniků není poznat, zda jejich sjednocení generuje celý prostor nebo jen rovinu. Založíme tedy definici na tvrzení 38.

DEFINICE 37. Nechť $W_1, \dots, W_k \leq V$. Pak součet $W = W_1 + \dots + W_k$ označíme za *direktní*, pokud lze každý vektor $w \in W$ zapsat jako součet $w_1 + \dots + w_k$, kde $w_i \in W_i$, právě jedním způsobem. Označujeme jej pak

$$W = W_1 \oplus \dots \oplus W_k \equiv \bigoplus_{i=1}^{k} W_i$$

VĚTA 21. *Nechť $W_1, \dots, W_k \leq V$ jsou konečné dimenze. Pak*

$$\dim W_1 \oplus \dots \oplus W_k = \dim W_1 + \dots + \dim W_k$$

DŮKAZ. Nechť B_i je báze W_i, pak ukážeme, že $(B_1, \dots, B_k)$ je báze $W_1 \oplus \dots \oplus W_k$. Libovolný vektor $w \in W_1 + \dots + W_k$ lze zapsat jako součet $w_1 + \dots + w_k$, kde $w_i \in W_i$, a každý w_i lze zapsat jako lineární kombinaci prvků posloupnosti B_i. Tedy w lze zapsat jako lineární kombinaci prvků posloupnosti $(B_1, \dots, B_k)$. Kdyby existoval druhý takový zápis, pak jej zapišme jako $w'_1 + \dots w'_k$, kde w'_i je lineární kombinace prvků B_i. Protože součet $W_1 \oplus \dots \oplus W_k$ je direktní, musí být $w_i = w'_i$ pro všechna i, a protože B_i jsou báze, jsou koeficienty lineární kombinace tvořící w'_i určeny jednoznačně. Tedy koeficienty v zápisu w jako lineární kombinace prvků posloupnosti $(B_1, \dots, B_k)$ jsou určeny jednoznačně, a tedy dle tvrzení 17 (nebo dle definice 18) je to báze $W_1 \oplus \dots \oplus W_k$. □

Bázi direktního součtu, která vznikne z bází jednotlivých sčítanců, budeme říkat *báze podřízená direktnímu součtu*, popřípadě *rozkladu*. Direktní součet jakožto podprostor má samozřejmě mnoho dalších bází, například $B = ((1,1),(1,-1))$ je báze prostoru $\langle(1,0)\rangle \oplus \langle(0,1)\rangle = \mathbb{R}^2$, jejíž prvky neleží v žádném z direktních sčítanců. Pokud bychom $\mathbb{R}^2$ zapsali jako direktní součet $\langle(1,1)\rangle \oplus \langle(1,-1)\rangle$, pak by B tomuto rozkladu podřízená byla.

2. Blokový zápis

Uvažujme dva vektorové prostory a jejich rozklady na direktní součet $V = V_1 \oplus V_2$ a $W = W_1 \oplus W_2$ a jejich dimenze $n = n_1 + n_2$ a $m = m_1 + m_2$. Pokud B_j je báze V_j, $B = (B_1, B_2)$ báze V, $v = v_1 + v_2$, kde $v_i \in V_i$ a $\mathbf{x}_i := [v_i]^{B_i}$, můžeme reprezentaci vektoru v zapsat *blokovým zápisem*

$$[v]^B \equiv \mathbf{x} = \begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{pmatrix} \equiv \begin{pmatrix} [v_1]^{B_1} \\ [v_2]^{B_2} \end{pmatrix}$$

Aritmetický vektor o n složkách je zde zapsán jako vektor složený ze dvou bloků, jimiž jsou aritmetické vektory o n_1, resp. n_2 složkách.

Označme $\iota_1 : V_1 \to V$ lineární zobrazení *vložení* definované předpisem $\iota_1(v_1) = v_1 \in V$. Jeho reprezentace pak splňuje

$$[\iota_1]^B_{B_1} \mathbf{x}_1 = [\iota_1]^B_{B_1} [v_1]^{B_1} = [v_1]^B = \begin{pmatrix} \mathbf{x}_1 \\ \mathbf{o} \end{pmatrix}$$

Tedy

$$[\iota_1]^B_{B_1} = \left(\begin{array}{c|c|c|c} \mathbf{e}_1 & \mathbf{e}_2 & \multirow{2}{*}{\dots} & \mathbf{e}_{n_1} \\ \mathbf{o} & \mathbf{o} & & \mathbf{o} \end{array}\right) =: \begin{pmatrix} E_{n_1} \\ 0 \end{pmatrix},$$

kde $0 \in \mathbb{F}^{n_2 \times n_1}$. Podobně lze definovat $\iota_2 : V_2 \to V$.

Dále zaveďme lineární zobrazení *projekce* $\pi_i : W \to W_i$ tak, že pro libovolný $w \in W$, $w = w_1 + w_2$, kde $w_i \in W_i$, je $\pi_i(w) = w_i$. Pokud $C = (C_1, C_2)$ je báze W složená z bází W_1, W_2 a $[w_i]^{C_i} =: \mathbf{y}_i$, pak

$$[\pi_1]_C^{C_1} \begin{pmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \end{pmatrix} = [\pi_1]_C^{C_1} [w]^C = [w_1]^{C_1} = \mathbf{y}_1$$

Tedy $[\pi_1]_C^{C_1} = (\mathbf{e}_1 | \dots | \mathbf{e}_{m_1} | \mathbf{o} | \dots | \mathbf{o}) =: (E_{m_1}\ 0)$, kde $0 \in \mathbb{F}^{m_1 \times m_2}$.

Uvažujme nyní $f \in \mathrm{Hom}(V, W)$ s reprezentací $[f]_B^C = A \in \mathbb{F}^{m \times n}$ a čtyři zobrazení $f_{ij} \in \mathrm{Hom}(V_i, W_j)$, $f_{ij} = \pi_i \circ f \circ \iota_j$. Pro f_{11} máme reprezentaci

$$[f_{11}]_{B_1}^{C_1} = [\pi_1]_C^{C_1} [f]_B^C [\iota_1]_{B_1}^B = \begin{pmatrix} E_{m_1} & 0 \end{pmatrix} A \begin{pmatrix} E_{n_1} \\ 0 \end{pmatrix} =: A_{11} \in \mathbb{F}^{m_1 \times n_1},$$

kde A_{11} je matice vzniklá vyškrtnutím posledních n_2 sloupců a posledních m_2 řádků z matice A. Analogicky lze zavést matice

$$[f_{12}]_{B_2}^{C_1} = [\pi_1]_C^{C_1} [f]_B^C [\iota_2]_{B_2}^B = \begin{pmatrix} E_{m_1} & 0 \end{pmatrix} A \begin{pmatrix} 0 \\ E_{n_2} \end{pmatrix} =: A_{12} \in \mathbb{F}^{m_1 \times n_2}$$

$$[f_{21}]_{B_1}^{C_2} = [\pi_2]_C^{C_2} [f]_B^C [\iota_1]_{B_1}^B = \begin{pmatrix} 0 & E_{m_2} \end{pmatrix} A \begin{pmatrix} E_{n_1} \\ 0 \end{pmatrix} =: A_{21} \in \mathbb{F}^{m_2 \times n_1}$$

$$[f_{22}]_{B_2}^{C_2} = [\pi_2]_C^{C_2} [f]_B^C [\iota_2]_{B_2}^B = \begin{pmatrix} 0 & E_{m_2} \end{pmatrix} A \begin{pmatrix} 0 \\ E_{n_2} \end{pmatrix} =: A_{22} \in \mathbb{F}^{m_2 \times n_2}$$

Ty dávají dohromady *blokový zápis matice* $A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$.

TVRZENÍ 40. *Nechť* $n = n_1 + n_2$, $m = m_1 + m_2$, $p = p_1 + p_2$, $A \in \mathbb{F}^{m \times n}$, $B \in \mathbb{F}^{n \times p}$ *s bloky* $A_{ij} \in \mathbb{F}^{m_i \times n_j}$, $B_{ij} \in \mathbb{F}^{n_i \times p_j}$. *Pak součin* $C := AB$ *má blokový zápis*

$$\begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix} = \begin{pmatrix} A_{11}B_{11} + A_{12}B_{21} & A_{11}B_{12} + A_{12}B_{22} \\ A_{21}B_{11} + A_{22}B_{21} & A_{21}B_{12} + A_{22}B_{22} \end{pmatrix}$$

Důkaz lze provést rozepsáním

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} = \sum_{k=1}^{n_1} a_{ik} b_{kj} + \sum_{k=n_1+1}^{n} a_{ik} b_{kj}$$

a interpretací obou sum jako elementů součinu nějakých bloků matic A, B. Nebo můžeme zavést $g \in \mathrm{Hom}(U, V)$, $U = U_1 \oplus U_2$, $D = (D_1, D_2)$ podřízenou bázi, ι'_i, vložení U_i do U a π'_i, projekci V na V_i, rozmyslet si, že

$$\iota_1 \circ \pi'_1 + \iota_2 \circ \pi'_2 = \mathrm{Id} \in \mathrm{End}(V)$$

a poté odvodit, že pro $q, r \in \{1, 2\}$

$$\begin{aligned}
(f \circ g)_{pr} &= \pi_q \circ f \circ g \circ \iota'_r \\
&= \pi_q \circ f \circ (\iota_1 \circ \pi'_1 + \iota_2 \circ \pi'_2) \circ g \circ \iota'_r \\
&= (\pi_q \circ f \circ \iota_1) \circ (\pi'_1 \circ g \circ \iota'_r) + (\pi_q \circ f \circ \iota_2) \circ (\pi'_2 \circ g \circ \iota'_r) \\
&= f_{q1} \circ g_{1r} + f_{q2} \circ g_{2r},
\end{aligned}$$

odkud dostáváme

$$[(f \circ g)_{pr}]_{D_r}^{C_p} = [f_{q1}]_{B_1}^{C_p} [g_{1r}]_{D_r}^{B_1} + [f_{q2}]_{B_2}^{C_p} [g_{2r}]_{D_r}^{B_2} = A_{p1} B_{1r} + A_{p2} B_{2r}$$

Protože direktní sčítanec v rozkladu $V = V_1 \oplus V_2$ může být sám direktním součtem nějakých svých podprostorů, mohou mít i jednotlivé bloky matice samy blokovou strukturu. Tvrzení se pak snadno zobecní pro matice s libovolným blokovým členěním, pouze musí pro každý vyskytující se součin bloků $A_{ik} B_{kj}$ mít blok A_{ik} stejně sloupců, jako má blok B_{kj} řádků.

Pro $f \in \mathrm{End}(V)$, $V = V_1 \oplus \ldots \oplus V_k$ s bází $B = (B_1, \ldots, B_k)$, kde B_i je báze V_i, jsou diagonální bloky $[f]_B^B$ čtvercové matice $[f_{ii}]_{B_i}^{B_i}$, a pokud jsou zároveň mimodiagonální bloky nulové, mluvíme o *blokově diagonální matici*, jsou-li nulové jen na jedné straně diagonály, o *blokově horní/dolní trojúhelníkové matici.*

TVRZENÍ 41. *Nechť $A = \mathrm{diag}(A_{11}, A_{22}, \ldots, A_{kk})$ je blokově diagonální matice. Pak*

(1) $\forall p \in \mathbb{N} : A^p = \mathrm{diag}(A_{11}^p, \ldots, A_{kk}^p)$ *a jsou-li všechny A_{ii} regulární, pak i* $A^{-p} = \mathrm{diag}(A_{11}^{-p}, \ldots, A_{kk}^{-p})$
(2) $\mathrm{rank}(A) = \mathrm{rank}(A_{11}) + \mathrm{rank}(A_{22}) + \ldots + \mathrm{rank}(A_{kk})$
(3) $\mathrm{Tr}(A) = \mathrm{Tr}(A_{11}) + \mathrm{Tr}(A_{22}) + \ldots + \mathrm{Tr}(A_{kk})$
(4) $\det(A) = \det(A_{11}) \det(A_{22}) \ldots \det(A_{kk})$
(5) $\sigma(A) = \sigma(A_{11}) \cup \ldots \cup \sigma(A_{kk})$ *včetně algebraických násobností.*

Navíc části 3,4 a 5 platí i pro horní/dolní trojúhelníkovou matici s týmiž diagonálními bloky.

DŮKAZ. Stačí uvažovat $k = 2$ a $A = \mathrm{diag}(A', A'')$, kde $A' \in \mathbb{F}^{p \times p}$, $A'' \in \mathbb{F}^{q \times q}$, $p + q = n$. Body 1 a 3 jsou jasné, v bodě 4 lze v definici determinantu uvažovat pouze permutace $\pi \in S_n$, pro něž $\pi(i) \leq p$ pro všechna $i \in \{1, \ldots, p\}$. Rozložme π na nezávislé cykly, pak $\pi = \pi'\pi''$, kde π' je složení cyklů na množině $\{1, \ldots, p\}$ a π'' složení cyklů na množině $\{p+1, \ldots, n\}$. Označme $\rho' \in S_p$ permutaci, která vznikne zúžením π' na množinu $\{1, \ldots, p\}$ a $\rho'' \in S_q$ permutaci definovanou $\rho''(i) = \pi''(i) - p$. Pak je $\det(A) = \sum_{\pi \in S_n} \mathrm{sgn}\, \pi a_{1\pi(1)} \ldots a_{n\pi(n)}$

$$= \sum_{\rho' \in S_p} \sum_{\rho'' \in S_q} \mathrm{sgn}(\pi'\pi'') a_{1\rho'(1)} \ldots a_{p\rho'(p)} a_{p+1,p+\rho''(1)} \ldots a_{p+q,p+\rho''(q)}$$
$$= \sum_{\rho' \in S_p} \mathrm{sgn}(\rho') a'_{1\rho'(1)} \ldots a'_{p\rho'(p)} \sum_{\rho'' \in S_q} \mathrm{sgn}(\rho'') a''_{1\rho''(1)} \ldots a''_{q\rho''(q)}$$

Z bodu 4 plyne 5, protože vlastní čísla jsou kořeny polynomu $\det(A - \lambda E_n) = \det(A' - \lambda E_p) \det(A'' - \lambda E_q)$. Bod 2 plyne z Gaussovy eliminace provedené zvlášť na prvních p řádků a zvlášť na zbylých q řádků, kterou se A', A'' převedou do odstupňovaného tvaru, takže jejich hodnost je rovna počtu nenulových řádků z prvních p, resp ze zbylých q. Celá matice A se tím rovněž dostala do odstupňovaného tvaru, takže její hodnost je rovna počtu nenulových řádků v celé upravené matici. Zobecnění 3 horní/dolní trojúhelníkovou matici je zřejmé, pro zobecnění 4 a 5 si stačí uvědomit, že každá permutace, kterou nelze napsat jako $\pi'\pi''$ dle prvního odstavce, zobrazuje alespoň jeden index z množiny $\{1, \ldots, p\}$ do množiny $\{p+1, \ldots, n\}$ a alespoň jeden index naopak. Tedy sčítanec v definici determinantu příslušný této permutaci bude obsahovat alespoň jeden činitel z bloku nad diagonálou a alespoň jeden činitel z bloku pod diagonálou, přičemž alespoň jeden z těchto činitelů je nulový. □

PŘÍKLAD 19. Nechť $\mathbf{x} \in \mathbb{R}^n$, $\|\mathbf{x}\| = 1$, $P_{\mathbf{x}}(\mathbf{y}) = (\mathbf{x}.\mathbf{y})\mathbf{x}$ a $B = (B_1, B_2)$ je báze složená z bází $\langle \mathbf{x} \rangle$ a $\mathbf{x}^\perp$. Označme 0_{n-1} nulovou matici z $\mathbb{F}^{n-1 \times n-1}$ a $\mathbf{o}_{n-1}$ nulový vektor z $\mathbb{F}^{n-1}$. Pak

$$[P_{\mathbf{x}}]_B^B = \begin{pmatrix} 1 & \mathbf{o}_{n-1}^T \\ \mathbf{o}_{n-1} & 0_{n-1} \end{pmatrix}, \quad [P_{\mathbf{x}^\perp}]_B^B = \begin{pmatrix} 0 & \mathbf{o}_{n-1}^T \\ \mathbf{o}_{n-1} & E_{n-1} \end{pmatrix}$$

a matice zrcadlení $Z_{\mathbf{x}^\perp} = \mathrm{Id} - 2P_{\mathbf{x}}$ má blokový tvar

$$[Z_{\mathbf{x}^\perp}]_B^B = \begin{pmatrix} -1 & \mathbf{o}_{n-1}^T \\ \mathbf{o}_{n-1} & E_{n-1} \end{pmatrix}$$

Pokud $n = 3$ a B_2 je ortonormální báze $\mathbf{x}^\perp$, pak matice rotace okolo osy $\langle \mathbf{x} \rangle$ o úhel ϕ vzhledem k bázi B je

$$[R_{\mathbf{x},\phi}]_B^B = \begin{pmatrix} 1 & \mathbf{o}_2^T \\ \mathbf{o}_2 & [R_\phi]_{B_2}^{B_2} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\phi & -\sin\phi \\ 0 & \sin\phi & \cos\phi \end{pmatrix}$$

PŘÍKLAD 20. Uvažujme blokově horní trojúhelníkovou matici $D := \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$, kde $A \in \mathbb{F}^{p\times p}$, $C \in \mathbb{F}^{q\times q}$ jsou regulární. Pak platí

$$\begin{pmatrix} A^{-1} & -A^{-1}BC^{-1} \\ 0 & C^{-1} \end{pmatrix} \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} = \begin{pmatrix} A^{-1}A & A^{-1}B - A^{-1}B \\ 0 & C^{-1}C \end{pmatrix}$$

Matice napravo je jednotková, tedy D je regulární a první matice nalevo je rovna D^{-1}. Jak jsme mohli inverzní matici uhodnout? Stačí se podívat na výpočet inverzní matice k 2×2 matici s elementy a, b, c z $\mathbb{F}$, $a, c \neq 0$:

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1} = \frac{1}{ac} \begin{pmatrix} c & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} \frac{1}{a} & -\frac{b}{ac} \\ 0 & \frac{1}{c} \end{pmatrix}$$

Mezi tvary blokového a neblokového inverzu je zřejmá analogie, až na to, že matice A^{-1}, B, C^{-1} na rozdíl od prvků a^{-1}, b, c^{-1} nekomutují a nemusí jít ani v jiném pořadí vynásobit.

Jako ilustraci použití blokových matic v důkazech uveďme

TVRZENÍ 42. *Nechť $A, B \in \mathbb{F}^{n\times n}$. Pak $\sigma(AB) = \sigma(BA)$ včetně násobností.*

DŮKAZ. Výpočtem ověříme, že

$$\begin{pmatrix} E_n & -A \\ 0_n & E_n \end{pmatrix} \begin{pmatrix} AB & 0_n \\ B & 0_n \end{pmatrix} \begin{pmatrix} E_n & A \\ 0_n & E_n \end{pmatrix} = \begin{pmatrix} 0_n & 0_n \\ B & BA \end{pmatrix}$$

Levá strana má tvar RCR^{-1}, tedy matice C a matice C' na pravé straně jsou podobné a mají stejná vlastní čísla včetně násobností. Protože C i C' jsou obě blokově dolní trojúhelníkové, platí pro ně $\sigma(C) = \sigma(AB) \cup \sigma(0_n)$, $\sigma(C') = \sigma(BA) \cup \sigma(0_n)$ včetně násobností. $\square$

Tvrzení i důkaz se snadno zobecní na obdélníkové matice $A \in \mathbb{C}^{m\times n}$, $B \in \mathbb{C}^{n\times m}$, pouze se bude u AB a BA lišit algebraická násobnost vlastního čísla nula.