MB141, zkouška 1. 6. 2022

Příklad. **1A.** [6 bodů] V prostoru $\mathbb{R}^4$ jsou dány podprostory

$$P = [(1,1,-1,-1),(2,3,2,-2)], \quad Q = [(2,0,1,1),(4,4,7,-1)].$$

(a) Najděte báze a dimenze jejich průniku a součtu.
(b) Zjistěte pomocí výpočtu, zda vektor $(1,2,3,4)$ leží v podprostoru $P+Q$. Body budou uděleny jen za správné zdůvodnění.

Řešení. **(a)** Označme $u_1 = (1,1,-1,-1), u_2 = (2,3,2,-2) \in P$ a $v_1 = (2,0,1,1), v_2 = (4,4,7.-1) \in Q$. Vektor v průniku je tvaru

$$z = au_1 + bu_2 = cv_1 + dv_2.$$

Najdeme c, d řešením soustavy s maticí

$$\left(\begin{array}{cc|cc} 1 & 2 & 2 & 4 \\ 1 & 3 & 0 & 4 \\ -1 & 2 & 1 & 7 \\ -1 & -2 & 1 & -1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 2 & 2 & 4 \\ 0 & 1 & -2 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

Řešení je $(c,d) = (-p,p)$, kde $p \in \mathbb{R}$ je parametr. Proto

$$P \cap Q = \{-pv_1 + pv_2 \in \mathbb{R}^4\} = [v_2 - v_1] = [(2,4,6,-2)] = [(1,2,3,-1)].$$

Báze $P \cap Q$ je tvořena vektorem $(1,2,3,-1)$.

Z předchozího výpočtu plyne, že

$$P + Q = [u_1, u_2, v_1, v_2] = [u_1, u_2, v_1],$$

kde u_1, u_2, v_1 jsou lineárně nezávislé, tedy tvoří bázi součtu.

(b) Vektor $(1,2,3,4)$ leží v $P+Q$, právě když má řešení rovnice

$$au_1 + bu_2 + cv_1 = (1,2,3,4)$$

o neznámých a, b, c. Matice soustavy je

$$\left(\begin{array}{ccc|c} 1 & 2 & 2 & 1 \\ 1 & 3 & 0 & 2 \\ -1 & 2 & 1 & 3 \\ -1 & -2 & 1 & 4 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 2 & 2 & 1 \\ 0 & 1 & -2 & 1 \\ 0 & 0 & 3 & 5 \\ 0 & 0 & 0 & -\frac{55}{3} \end{array}\right)$$

Soustava nemá řešení, tedy $(1,2,3,4) \notin P+Q$.

(Při troše opatrnosti v interpretaci schodového tvaru bylo možné úkol řešit společným maticovým schématem s částí (a).) □

Bodování. Sestavení soustavy rovnic pro (a) **1 bod**.
Výpočet koeficientů pro průnik **1 bod**.
Báze a dimenze průniku **1 bod**.
Báze a dimenze součtu **1 bod**.
Sestavení soustavy rovnic pro (b) **1 bod**.
Výpočet a správná odpověď, zda vektor leží v součtu **1 bod**. □

Příklad. **1B.** [6 bodů] V prostoru $\mathbb{R}^4$ jsou dány podprostory

$$U = [(1,1,-1,1),(2,1,2,0)], \quad V = [(2,0,-1,3),(5,2,0,4)].$$

(a) Najděte báze a dimenze jejich průniku a součtu.
(b) Zjistěte pomocí výpočtu, zda vektor $(1,2,3,4)$ leží v podprostoru $U+V$. Body budou uděleny jen za správné zdůvodnění.

Řešení. **(a)** Označme $u_1 = (1,1,-1,1), u_2 = (2,1,2,0) \in U$ a $v_1 = (2,0,-1,3), v_2 = (5,2,0,4) \in V$. Vektor v průniku je tvaru

$$z = au_1 + bu_2 = cv_1 + dv_2.$$

Najdeme c, d řešením soustavy s maticí

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

Řešení je $(c,d) = (-p,p)$, kde $p \in \mathbb{R}$ je parametr. Proto

$$U \cap V = \{-pv_1 + pv_2 \in \mathbb{R}^4\} = [v_2 - v_1] = [(3,2,1,1)].$$

Báze $U \cap V$ je tvořena vektorem $(3,2,1,1)$.

Z předchozího výpočtu plyne, že

$$U + V = [u_1, u_2, v_1, v_2] = [u_1, u_2, v_1],$$

kde u_1, u_2, v_1 jsou lineárně nezávislé, tedy tvoří bázi součtu.

(b) Vektor $(1,2,3,4)$ leží v $U+V$, právě když má řešení rovnice

$$au_1 + bu_2 + cv_1 = (1,2,3,4)$$

o neznámých a, b, c. Matice soustavy je

$$\left(\begin{array}{ccc|c} 1 & 2 & 2 & 1 \\ 1 & 1 & 0 & 2 \\ -1 & 2 & -1 & 3 \\ 1 & 0 & 3 & 4 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 1 & 0 & 2 \\ 0 & 1 & 2 & -1 \\ 0 & 0 & 5 & 1 \\ 0 & 0 & 0 & \frac{47}{5} \end{array}\right)$$

Soustava nemá řešení, tedy $(1,2,3,4) \notin U+V$.

(Při troše opatrnosti v interpretaci schodového tvaru bylo možné úkol řešit společným maticovým schématem s částí (a).) □

Bodování. Sestavení soustavy rovnic pro (a) **1 bod**.
Výpočet koeficientů pro průnik **1 bod**.
Báze a dimenze průniku **1 bod**.
Báze a dimenze součtu **1 bod**.
Sestavení soustavy rovnic pro (b) **1 bod**.
Výpočet a správná odpověď, zda vektor leží v součtu **1 bod**. □

Příklad. **2A.** [6 bodů] Zobrazení $\varphi : \mathbb{R}^3 \to \mathbb{R}^3$ je symetrie podle roviny $x_1 + x_2 + 2x_3 = 0$.

(a) Najděte matici A tak, aby ve standardních souřadnicích bylo

$$\varphi \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = A \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}.$$

(b) Je A ortogonální matice? Zdůvodněte svou odpověď.

(c) Najděte inverzní matici A^{-1}.

Řešení. **(a)** Symetrie podle roviny zobrazuje normálový vektor na opačný vektor a vektory z roviny na sebe. Normálový vektor je $n = (1, 1, 2)$, vektory v rovině jsou např. $u = (1, -1, 0)$ a $v = (0, 2, -1)$. Platí

$$\varphi(n) = -n, \quad \varphi(u) = u, \quad \varphi(v) = v.$$

Odtud již můžeme určit hodnoty zobrazení φ na vektorech e_1, e_2, e_3 standardní báze a tyto hodnoty tvoří sloupce hledané matice. Pro výpočet pišme vektory do řádků

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

Tedy matice

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

(b) Sloupce matice jsou na sebe kolmé a mají jednotkovou velikost. Proto je matice ortogonální.

(c) Protože je A ortogonální je $A^{-1} = A^T = A$. Jiné zdůvodnění spočívá v tom, že se spočítá součin $A \cdot A = E$. □

Bodování. **(a)** Výběr normálového vektoru a úvaha, kam se zobrazuje **1 bod**.
Výběr dvou nezávislých vektorů z roviny a úvaha, kam se zobrazují **1 bod**.
Sestavení schématu/soustavy pro výpočet matice **1 bod**
Výpočet matice **1 bod**

(b) Zdůvodnění ortogonality **1 bod**.

(c) Výpočet inverze **1 bod**. □

Příklad. **2B.** [6 bodů] Zobrazení $\psi : \mathbb{R}^3 \to \mathbb{R}^3$ je symetrie podle roviny $2x_1 - x_2 + x_3 = 0$.

(a) Najděte matici B tak, aby ve standardních souřadnicích bylo

$$\psi \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = B \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}.$$

(b) Je B ortogonální matice? Zdůvodněte svou odpověď.

(c) Najděte inverzní matici B^{-1}.

Řešení. **(a)** Symetrie podle roviny zobrazuje normálový vektor na opačný vektor a vektory z roviny na sebe. Normálový vektor je $n = (2, -1, 1)$, vektory v rovině jsou např. $u = (1, 2, 0)$ a $v = (0, 1, 1)$. Platí

$$\varphi(n) = -n, \quad \varphi(u) = u, \quad \varphi(v) = v.$$

Odtud již můžeme určit hodnoty zobrazení φ na vektorech e_1, e_2, e_3 standardní báze a tyto hodnoty tvoří sloupce hledané matice. Pro výpočet pišme vektory do řádků

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

Tedy matice

$$B = \frac{1}{3} \begin{pmatrix} -1 & 2 & -2 \\ 2 & 2 & 1 \\ -2 & 1 & 2 \end{pmatrix}.$$

(b) Sloupce matice jsou na sebe kolmé a mají jednotkovou velikost. Proto je matice ortogonální.

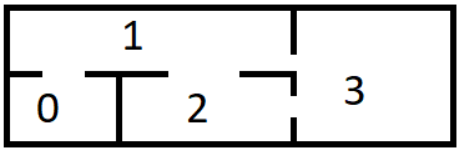
(c) Protože je B ortogonální je $B^{-1} = B^T = B$. Jiné zdůvodnění spočívá v tom, že se spočítá součin $B \cdot B = E$. □

Bodování. **(a)** Výběr normálového vektoru a úvaha, kam se zobrazuje **1 bod**.
Výběr dvou nezávislých vektorů z roviny a úvaha, kam se zobrazují **1 bod**.
Sestavení schématu/soustavy pro výpočet matice **1 bod**
Výpočet matice **1 bod**

(b) Zdůvodnění ortogonality **1 bod**.

(c) Výpočet inverze **1 bod**. □

Příklad. **3A.** [6 bodů]



Myš vložíme do bludiště tvaru na obrázku. Myš si v každém kroku vybere náhodně (se stejnou pravděpodobností) jedny dveře vedoucí z komůrky, v které se aktuálně nachází, a přejde jimi do nové komůrky. Modelujte pohyb myši v bludišti pomocí Markovova procesu.

(a) Napište matici tohoto procesu.
(b) Vysvětlete, jaký je význam koeficientu matice v 2. sloupci a 3. řádku.
(c) Ve které komůrce se myš nachází s největší pravděpodobností po velkém počtu kroků? A s jakou pravděpodobností to je?
(d) S jakou pravděpodobností se myš dostane z komůrky 2 do komůrky 3 právě třemi přechody?

Řešení. **(a)** Matice tohoto procesu je

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

(b) Prvek M_{32} je pravděpodobnost, že myš přejde z komůrky 1 do komůrky 2.
(c) Spočítáme pravděpodobnostní vlastní vektor k vlastnímu číslu 1 matice M.

$$(M - E)x = 0, \quad x_1 + x_2 + x_3 + x_4 = 1.$$

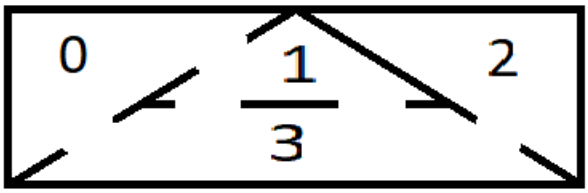
To vede na homogenní soustavu

$$\begin{pmatrix} -1 & 1/3 & 0 & 0 \\ 1 & -1 & 1/2 & 1/2 \\ 0 & 1/3 & -1 & 1/2 \\ 0 & 1/3 & 1/2 & -1 \end{pmatrix} \sim \begin{pmatrix} -3 & 1 & 0 & 0 \\ 0 & 2 & -6 & 3 \\ 0 & 0 & 9 & -9 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Řešení je $x = \frac{1}{8}(1, 3, 2, 2)^T$. Tedy myš bude po velkém počtu kroků nejčastěji v komůrce 1, a to s pravděpodobností $3/8$.
(d) Hledaná pravděpodobnost je čtvrtá složka vektoru $M^3 \cdot (0, 0, 1, 0)^T$ a to je $7/24$. □

Bodování. (a) Matice **2 body**
(b) Význam koeficientu **1 bod**.
(c) Vlastní vektor **1 bod**, komůrka a pravděpodobnost **1 bod**.
(d) Postup a výpočet **1 bod**. □

Příklad. **3B.** [6 bodů]



Myš vložíme do bludiště tvaru na obrázku. Myš si v každém kroku vybere náhodně (se stejnou pravděpodobností) jedny dveře vedoucí z komůrky, v které se aktuálně nachází, a přejde jimi do nové komůrky. Modelujte pohyb myši v bludišti pomocí Markovova procesu.

(a) Napište matici tohoto procesu.
(b) Vysvětlete, jaký je význam koeficientu matice v 2. sloupci a 4. řádku.
(c) Ve které komůrce se myš nachází s největší pravděpodobností po velkém počtu kroků? A s jakou pravděpodobností to je?
(d) S jakou pravděpodobností se myš dostane z komůrky 0 do komůrky 1 právě třemi přechody?

Řešení. **(a)** Matice tohoto procesu je

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

(b) Prvek M_{42} je pravděpodobnost, že myš přejde z komůrky 1 do komůrky 3.
(c) Spočítáme pravděpodobnostní vlastní vektor k vlastnímu číslu 1 matice M.

$$(M - E)x = 0, \quad x_1 + x_2 + x_3 + x_4 = 1.$$

To vede na homogenní soustavu

$$\begin{pmatrix} -1 & 1/3 & 0 & 1/4 \\ 1/2 & -1 & 0 & 1/2 \\ 0 & 0 & -1 & 1/4 \\ 1/2 & 2/3 & 1 & -1 \end{pmatrix} \sim \begin{pmatrix} 1 & -2 & 0 & 1 \\ 0 & 10 & 6 & -9 \\ 0 & 0 & -4 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Řešení je $x = \frac{1}{10}(2, 3, 1, 4)^T$. Tedy myš bude po velkém počtu kroků nejčastěji v komůrce 3, a to s pravděpodobností $4/10 = 2/5$.
(d) Hledaná pravděpodobnost je druhá složka vektoru $M^3 \cdot (1, 0, 0, 0)^T$ a to je $15/48$. □

Bodování. (a) Matice **2 body**.
(b) Význam koeficientu **1 bod**.
(c) Vlastní vektor **1 bod**, komůrka a pravděpodobnost **1 bod**.
(d) Postup a výočet **1 bod**. □

Příklad. **4A.** [6 bodů] Šifrou RSA s veřejným klíčem $n = 115$ a šifrovacím exponentem $e = 31$ bylo posláno číslo $Z = 52$. Šifru prolomte a určete zaslanou zprávu $M \in \{1, 2, \ldots, 114\}$. [Návod: využívejte rozklad modulu na součin mocnin prvočísel.]

Řešení. K prolomení šifry potřebujeme najít inverzi d exponentu e modulo $\varphi(115) = 88$, což umíme provést několika způsoby. Např. rozložením $88 = 8 \cdot 11$ dostaneme soustavu kongruencí

$$31d \equiv 1 \mod 8, \qquad 31d \equiv 1 \mod 11,$$

které nejprve vyřešíme odděleně

$$\begin{aligned} -d &\equiv 1 \mod 8, & -2d &\equiv 1 \mod 11, \\ d &\equiv -1 \mod 8, & d &\equiv 5 \mod 11, \end{aligned}$$

a poté najdeme společný výsledek pro původní modul $d \equiv 71 \mod 88$.

Dešifrování zprávy provedeme umocněním $Z^d \mod 115$. Opět se vyplatí využít rozklad modulu $115 = 5 \cdot 23$. S využitím malé Fermatovy věty v prvním kroku dostáváme

$$52^{71} \equiv 2^3 \equiv 3 \mod 5$$

a

$$52^{71} \equiv 6^5 = 6 \cdot 36^2 \equiv 6 \cdot (-10)^2 \equiv 6 \cdot 8 \equiv 2 \mod 23,$$

odkud již určíme $52^{71} \equiv 48 \mod 115$. □

Bodování. Úvaha, že dešifrovaná zpráva je tvaru $Z^d \mod n$, kde $ed \equiv 1 \mod \varphi(n)$ **1 bod**
Výpočet $\varphi(n)$ **1 bod**
Výpočet inverze $d = e^{-1}$ **2 body**
Dešifrování zprávy **2 body** □

Příklad. 4B. [6 bodů] Šifrou RSA s veřejným klíčem $n = 133$ a šifrovacím exponentem $e = 53$ bylo posláno číslo $Z = 109$. Šifru prolomte a určete zaslanou zprávu $M \in \{1, 2, \ldots, 132\}$. [Návod: využívejte rozklad modulu na součin mocnin prvočísel.]

Řešení. K prolomení šifry potřebujeme najít inverzi d exponentu e modulo $\varphi(133) = 108$, což umíme provést několika způsoby. Např. rozložením $108 = 4 \cdot 27$ dostaneme soustavu kongruencí

$$53d \equiv 1 \mod 4, \qquad 53d \equiv 1 \mod 27,$$

které nejprve vyřešíme odděleně

$$d \equiv 1 \mod 4, \qquad -d \equiv 1 \mod 27,$$
$$d \equiv -1 \mod 27,$$

a poté najdeme společný výsledek pro původní modul $d \equiv 53 \mod 108$.

Dešifrování zprávy provedeme umocněním $Z^d \mod 133$. Opět se vyplatí využít rozklad modulu $133 = 7 \cdot 19$. S využitím malé Fermatovy věty v prvním kroku dostáváme

$$109^{53} \equiv 4^5 = 4 \cdot 16^2 \equiv 4 \cdot 2^2 \equiv 2 \mod 7$$

a

$$109^{53} \equiv (-5)^{17} = -5 \cdot 25^8 \equiv -5 \cdot 6^8 = -5 \cdot 36^4 \equiv -5 \cdot (-2)^4 \equiv -5 \cdot (-3) \equiv 15 \mod 19,$$

odkud již určíme $109^{53} \equiv 72 \mod 133$. □

Bodování. Úvaha, že dešifrovaná zpráva je tvaru $Z^d \mod n$, kde $ed \equiv 1 \mod \varphi(n)$ **1 bod**
Výpočet $\varphi(n)$ **1 bod**
Výpočet inverze $d = e^{-1}$ **2 body**
Dešifrování zprávy **2 body** □