MB141, 30. 5. 2023, zkouška, skupina X

Příklad. 1. [2 body] Doplňte vektory $u = (1, 1, 2, -1)$, $v = (-3, 0, -4, 2)$ dalšími dvěma vektory e_i, e_j tak, aby dohromady tvořily bázi celého prostoru $\mathbb{R}^4$, kde e_1, e_2, e_3, e_4 značí standardní bázi. Jinými slovy vyberte z šestice vektorů u, v, e_1, e_2, e_3, e_4 nějakou maximální lineárně nezávislou podmnožinu (obsahující oba vektory u, v).

Řešení. Do společného maticového schématu s u, v zapíšeme všechny e_1, e_2, e_3, e_4, upravíme na schodový tvar a sledujeme, které sloupce navyšují hodnost matice (jsou nezávislé na předchozích):

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

Nové schody se utváří ve třetím a pátém sloupci, což odpovídá e_1 a e_3. Bází je tedy např. čtveřice (u, v, e_1, e_3). □

Příklad. 2. [2 body] Určete vzdálenost mimoběžek $p : [0, -3, 4]+t(1, 0, -2)$ a $q : [11, 1, 3]+s(3, 0, 1)$ v $\mathbb{R}^3$.

Řešení. Výpočet si lze významně ulehčit, pokud si všimneme, že zaměření každé z přímek p, q leží pouze v rovině xz a osa mimoběžek je tudíž rovnoběžná se souřadnou osou y. Díky tomu je zřejmé, že průsečíky, v nichž se osa mimoběžek realizuje, mají stejné souřadnice x a z a vzdálenost lze spočítat pouze z rozdílu v souřadnicích y. Ovšem tato souřadnice je pro přímku p i přímku q konstantní a můžeme si ji vypůjčit už z bodů $[0, -3, 4], [11, 1, 3]$ parametrického vyjádření. Dostáváme

$$d(p, q) = |-3 - 1| = 4.$$

□

Příklad. 3. [2 body] Určete odchylku přímky $p : [-1, 2, 2] + t(-1, 1, 0)$ a roviny $\rho : 2x - y + z = 1$ v prostoru $\mathbb{R}^3$.

Řešení. Protože známe směrový vektor $v = (-1, 1, 0)$ a normálový vektor $n = (2, -1, 1)$, můžeme snadno určit úhel, který svírají odpovídající přímky:

$$\cos\alpha = \frac{|\langle v, n\rangle|}{\|v\| \cdot \|n\|} = \frac{|-3|}{\sqrt{2} \cdot \sqrt{6}} = \frac{\sqrt{3}}{2}.$$

Odtud $\alpha = \pi/6$ $(= 30°)$ a hledanou odchylku podprostorů dopočítáme jako doplněk do pravého úhlu $\pi/2 - \pi/6 = \pi/3$ $(= 60°)$. □

Příklad. 4. [2 body] Najděte celá čísla x, y, aby platilo

$$23x + 18y = 1.$$

Řešení. Čísla $23, 18$ jsou nesoudělná, tedy podle Bezoutovy věty má rovnice řešení. Toto řešení lze nalézt postupným dělením se zbytkem podle Eukleidova algoritmu a zpětným

dosazováním:

$$\begin{aligned} 23 &= 18 + 5, & 18(x+y) + 5x &= 1, \\ 18 &= 3 \cdot 5 + 3, & 5(4x+3y) + 3(x+y) &= 1, \\ 5 &= 3 + 2, & 3(5x+4y) + 2(4x+3y) &= 1, \\ 3 &= 2 + 1, & 2(9x+7y) + (5x+4y) &= 1. \end{aligned}$$

Soustava

$$9x + 7y = 0, \qquad 5x + 4y = 1$$

má řešení $x = -7, y = 9$ a to je i odpověď na původní úlohu. □

Příklad. 5. [5 bodů] a) Prolomte šifru RSA s veřejným klíčem $n = 247 = 13 \cdot 19, e = 23$, tj. najděte inverzi d k e modulo $\phi(n)$.

b) V daném kryptosystému zašifrujte zprávu $M = 15$ jako $C = M^e \pmod n$. Při výpočtu doporučujeme počítat C nejdřív zvlášť modulo 13 a modulo 19 a využít Eulerovy věty pro zjednodušení (zredukování) exponentu, poté dát tyto výsledky dohromady pomocí Čínské zbytkové věty.

Řešení. a) Protože $247 = 13 \cdot 19$, snadno určíme $\phi(n) = 12 \cdot 18 = 216$. Kongruence $23d \equiv 1 \pmod{216}$ má řešení $d \equiv 47$.

b) Dostáváme $15^{23} \equiv 2^{11} \equiv 2 \cdot 4^5 \equiv 8 \cdot 3^2 \equiv 7 \pmod{13}$ a $15^{23} \equiv (-4)^5 \equiv -4 \cdot (-3)^2 \equiv 2 \pmod{19}$. Z druhé kongruence $15^{23} = 19t + 2$, dosazením do první a vyřešením dostaneme $t \equiv 3 \pmod{13}$, takže $C \equiv 15^{23} \equiv 59 \pmod{247}$. □

Příklad. 6. [2 body] Najděte nějakou matici L Leslieho procesu, v němž rozlišujeme 3 věkové kategorie, populace je stabilní, kategorie zaujímají poměr $4 : 2 : 1$ v pořadí od nejmladší po nejstarší, nejmladší kategorie nemá žádné potomstvo a nejstarší kategorie na konci cyklu celá umírá.

Řešení. Ze zadání ihned vyplývá, že matice L bude mít na 2. a 3. řádku jediné dvě nenulové hodnoty a ty odpovádají naději přežití z 1. do 2. a z 2. do 3. kategorie. Z poměru plyne, že v obou případech je naděje $1/2$. Vektor $v = (4, 2, 1)$ má být řešením homogenní soustavy $(L - E)v = 0$. Průzkum 2. a 3. řádku soustavy potvrzuje již provedenou úvahu, zbývá určit 1. řádek matice. Podle zadání je buňka v levém horním rohu nulová, buňky ve 2. a 3. sloupci označme b a c. Musí platit $-4+2b+c = 0$, čehož dosáhneme například volbou $b = 1, c = 2$. Dostáváme matici

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

□

Příklad. 7. [5 bodů] a) Najděte vlastní čísla a vlastní vektory lineárního zobrazení $f : \mathbb{R}^3 \to \mathbb{R}^3, f(v) = Av$ daného maticí

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

b) Na základě těchto výsledků určete, o jaké zobrazení se jedná (symetrie podle podprostoru ..., projekce na podprostor ..., atp.).

Řešení. a) Vlastní čísla jsou kořeny charakteristického polynomu:

$$|A-\lambda E| = \begin{vmatrix} -\lambda & -1 & 0 \\ -1 & -\lambda & 0 \\ 0 & 0 & 1-\lambda \end{vmatrix} = (\lambda^2-1)(1-\lambda) = -(\lambda+1)(\lambda-1)^2,$$

tj. jednoduchý $\lambda_1 = -1$ a dvojnásobný $\lambda_2 = 1$. Řešením odpovídajících homogenních soustav $(A-\lambda_i E)v = 0$ dojdeme např. k vlastnímu vektoru $u = (1,1,0)$ pro $\lambda_1 = -1$ a vektorům $v = (0,0,1), w = (1,-1,0)$ pro $\lambda_2 = 1$. (Stačí nám najít vektory tvořící bázi příslušného podprostoru.)

b) Vlastní čísla znamenají, že zobrazení f obrací vektor u, zatímco v, w zůstávají na místě. Jedná se tedy o symetrii (zrcadlení) podle roviny. Tu popíšeme buď to pomocí směrových vektorů v, w, nebo pomocí normálového vektoru u:

$$\rho : t(0,0,1) + s(1,-1,0), \qquad \rho : x + y = 0.$$

□