

Příklad 1. [2 body] Doplníte vektory $u = (1, 1, 4, -2)$, $v = (0, 3, -2, 1)$ 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 , upra- víme na schodový tvar a sledujeme, které sloupce navyšují hodnotu matice (jsou nezávislé na předchozích):

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

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

Příklad 2. [2 body] Určete vzdálenost mimoběžek $p : [1, -3, 3] + t(1, 0, 2)$ a $q : [9, 2, 3] + s(-3, 0, 1)$ 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 $[1, -3, 3]$, $[9, 2, 3]$ parametrického vyjádření. Dostáváme

$$d(p, q) = |-3 - 2| = 5.$$

\square

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

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

$$\cos \alpha = \frac{|\langle v, n \rangle|}{\|v\| \cdot \|n\|} = \frac{|-3|}{\sqrt{6} \cdot \sqrt{6}} = \frac{1}{2}.$$

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

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

$$27x + 19y = 1.$$

Řešení. Čísla 27, 19 jsou nesoudělná, tedy podle Bezoutovy věty má rovnice řešení. Toto řešení lze nalézt postupným dělením se zbytkem podle Eukleidova algoritmu a zpětným

dosazováním:

$$\begin{aligned} 27 &= 19 + 8, & 19(x + y) + 8x &= 1, \\ 19 &= 2 \cdot 8 + 3, & 8(3x + 2y) + 3(x + y) &= 1, \\ 8 &= 2 \cdot 3 + 2, & 3(7x + 5y) + 2(3x + 2y) &= 1, \\ 3 &= 2 + 1, & 2(10x + 7y) + (7x + 5y) &= 1. \end{aligned}$$

Soustava

$$10x + 7y = 0, \quad 7x + 5y = 1$$

má řešení $x = -7, y = 10$ a to je i odpověď na původní úlohu. \square

Příklad 5. [5 bodů] a) Prolomte šifru RSA s veřejným klíčem $n = 247 = 13 \cdot 19, e = 29$, tj. najděte inverzi d k e modulo $\phi(n)$.

b) V daném kryptosystému zašifrujte zprávu $M = 17$ jako $C = M^e \pmod{n}$. Při výpočtu doporučujeme počítat C nejdříve 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 $29d \equiv 1 \pmod{216}$ má řešení $d \equiv 149$.

b) Dostáváme $17^{29} \equiv 4^5 \equiv 4 \cdot 3^2 \equiv -3 \pmod{13}$ a $17^{29} \equiv (-2)^{11} \equiv -2 \cdot 4^5 \equiv -8 \cdot (-3)^2 \equiv 4 \pmod{19}$. Z druhé kongruence $17^{29} = 19t + 4$, dosazením do první a vyřešením dostaneme $t \equiv 1 \pmod{13}$, takže $C \equiv 17^{29} \equiv 23 \pmod{247}$. \square

Příklad 6. [2 body] Najděte nějakou matici L Leslieho procesu, v němž rozlišujeme 3 věkové kategorie, populace je stabilní, kategorie zaujímají poměr 3 : 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 odpovídají naději přežití z 1. do 2. a z 2. do 3. kategorie. Z poměrů plyne, že v jednotlivých případech je naděje $2/3$, resp. $1/2$. Vektor $v = (3, 2, 1)$ 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 $-3 + 2b + c = 0$, čehož dosáhneme například volbou $b = 1, c = 1$. Dostáváme matici

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

\square

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

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

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:

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

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 $u = (0, 1, 1)$ pro $\lambda_1 = -1$ a vektorům $v = (1, 0, 0)$, $w = (0, 1, -1)$ 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 :

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

□