

Příklad. 1A. [2 body] Uvažujme vektorový prostor \mathbb{R}^4 . Rozhodněte, které z vektorů

$$u_1 = (1, 3, -3, -11), \quad u_2 = (2, 3, -1, 2)$$

patří do podprostoru P generovaného vektory

$$v_1 = (1, 1, -1, -1), \quad v_2 = (3, 1, -5, -1), \quad v_3 = (0, 3, 5, 1).$$

Řešení. Vektory v_1, v_2, v_3 naskládáme jako sloupce nalevo do maticového schématu. Kdybychom testovali jeden vektor, zařadili bychom ho napravo a zjišťovali, zda navyšuje hodnotu matice, či ekvivalentně, zda má odpovídající soustava rovnic řešení. Úpravy na schodový tvar by se ovšem prováděly pro oba vektory u_1, u_2 stejně, můžeme si tedy postup racionalizovat a vyřešit jediným schématem, kde vypíšeme vpravo oba vektory:

$$\left(\begin{array}{ccc|cc} 1 & 3 & 0 & 1 & 2 \\ 1 & 1 & 3 & 3 & 3 \\ -1 & -5 & 5 & -3 & -1 \\ -1 & -1 & 1 & -11 & 2 \end{array} \right) \sim \dots \sim \left(\begin{array}{ccc|cc} 1 & 3 & 0 & 1 & 2 \\ 0 & -2 & 3 & 2 & 1 \\ 0 & 0 & 2 & -4 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array} \right)$$

Sloupec vektoru u_2 vyčnívá za poslední schod určený levou stranou, zvýšil by tak hodnotu matice, a proto v podprostoru P neleží. Naopak u_1 se do tohoto posledního schodu vejde, tj. je nutně lineární kombinací vektorů v_1, v_2, v_3 a patří tedy do P . \square

Příklad. 1B. [2 body] Necht' zobrazení $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ je symetrií (zrcadlením) podle roviny $\rho : x_2 = 0$. Najděte matici M takovou, že v souřadnicích standardní báze je $f(x) = Mx$.

Řešení. Normálovým vektorem roviny ρ je $n = (0, 1, 0)$. Ten se při zrcadlení zobrazí na opačný vektor: $f(n) = -n$. V rovině ρ leží mimo jiné další dva vektory standardní báze $u = (1, 0, 0)$ a $v = (0, 0, 1)$ a ty zůstávají při zrcadlení na místě: $f(u) = u, f(v) = v$. Protože známe obrazy všech vektorů standardní báze, jejich prostým poskládáním do sloupců dostáváme ihned matici M :

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

\square

Příklad. 1C. [2 body] V prostoru \mathbb{R}^3 určete průnik roviny $\rho : x - 2y + 3z = 2$ a přímky $p : x + y = -1, y - z = -1$. Jaká je jejich vzájemná poloha?

Řešení. Body průniku musí současně vyhovovat všem rovnicím, budeme je tedy řešit jako soustavu lineárních rovnic:

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

Soustava má zřejmě nekonečně mnoho řešení (s jedním parametrem), průnikem je tak celá přímka p a platí $p \subseteq \rho$. \square

Příklad. 2A. [2 body] Určete zbytek po dělení čísla $5^{(5^5)}$ jedenácti.

Řešení. Podle malé Fermatovy věty platí $5^{10} \equiv 1 \pmod{11}$, čehož využijeme ke snížení exponentu 5^5 na jeho zbytek po dělení deseti. Platí $5^5 = 5 \cdot (5^2)^2 \equiv 5 \pmod{10}$, proto $5^{5^5} \equiv 5^5 = 5 \cdot (5^2)^2 \equiv 5 \cdot 3^2 \equiv 1 \pmod{11}$. Zbytek po dělení čísla 5^{5^5} jedenácti je 1. \square

Příklad. 2B. [5 bodů] Alice a Bob používají pro šifrovanou komunikaci protokol ElGamal. Veřejnými informacemi jsou modul 13 a primitivní kořen $g = 7$.

a) Ověřte, že g je skutečně primitivní kořen.

b) Útočníci Evě se podařilo vyzvědět společný soukromý klíč $g^{ab} = 6$, z něž díky výpočtům v části a) zvládla určit exponent $ab = ?$, a také Bobův soukromý klíč $b = 5$. Pomozte Evě dokončit rozbití šifry a určete Alicin soukromý klíč a .

Řešení. a) Číslo g je primitivním kořenem, pokud $\phi(13) = 12$ je nejmenší přirozený exponent x , pro nějž je $g^x \equiv 1 \pmod{13}$. Protože $12 = 2^2 \cdot 3$, stačí prověřit mocniny g pro maximální dělitele 12, což jsou 4 a 6. (Pokud $g^4 \not\equiv 1$ a $g^6 \not\equiv 1$, pak $g^x \equiv 1$ až pro $x = 12$.) Dostáváme (vše v modulu 13):

$$7^2 = 49 \equiv -3,$$

$$7^4 \equiv (-3)^2 \equiv -4 \not\equiv 1,$$

$$7^6 \equiv (-3)^3 \equiv -4 \cdot (-3) \equiv -1 \not\equiv 1,$$

tedy $g = 7$ je primitivní.

b) Potřebujeme s co nejmenší námahou zjistit exponent ab ze znalosti společného klíče $g^{ab} \equiv 6$, odkud se znalostí b už snadno určíme a . Ve výpočtech z a) jsme zjistili, že $7^1 \equiv 7$ a $7^6 \equiv -1$, z čehož plyne $7^7 \equiv 7^{1+6} \equiv 7 \cdot (-1) \equiv -7 \equiv 6$. To znamená, že $ab \equiv 5a \equiv 7 \pmod{12}$ a tedy $a \equiv 11 \pmod{12}$. \square

Příklad. 3A. [2 body] Určete vzdálenost bodu $A = [3, 2]$ od přímky $p : 2x - y = -1$ v rovině \mathbb{R}^2 .

Řešení. Vzdálenost se bude realizovat ve směru kolmém na přímku, tedy ve směru normálového vektoru $n = (2, -1)$. Pata kolmice B na přímce p je tedy tvaru $A + tn$ pro vhodné t a současně splňuje rovnici přímky. Dosazením tohoto parametrického vyjádření dostaneme rovnici

$$2(3 + 2t) - (2 - t) = -1,$$

jejímž řešením je $t = -1$. Vzdálenost určíme jako velikost vektoru tn :

$$d(A, p) = \|tn\| = |t| \cdot \|n\| = |-1| \cdot \sqrt{2^2 + (-1)^2} = \sqrt{5}.$$

\square

Příklad. 3B. [5 bodů] Uvažujeme třístavový Markovův řetězec se stavy A, B, C a pravděpodobnostmi přechodů

$$\begin{array}{lll} P(A \rightarrow A) = 0, & P(A \rightarrow B) = 1/2, & P(B \rightarrow A) = 1/3, \\ P(B \rightarrow B) = 1/3, & P(A \rightarrow C) = 1/2, & P(C \rightarrow A) = 0, \\ P(B \rightarrow C) = 1/3, & P(C \rightarrow B) = 1/2, & P(C \rightarrow C) = 1/2, \end{array}$$

a) Sestavte přechodovou pravděpodobnostní matici M a ověřte, že je primitivní, tj. že nějaká mocnina M^k má všechny členy kladné.

b) Určete pravděpodobnost, s jakou se bude po dostatečně dlouhé době systém dostávat do stavu A .

Řešení. a) Matici sestavujeme tak, aby vstupní stavy odpovídaly sloupcům a výstupní stavy řádkům. Při dodržení abecedního pořadí stavů dostaneme matici

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

Primitivnost můžeme prověřit symbolickým umocňováním matice $\begin{pmatrix} 0 & + & 0 \\ + & + & + \\ + & + & + \end{pmatrix}$, přičemž zjistíme, že již M^2 je pozitivní.

b) Hledáme vlastní vektor pro vlastní číslo 1, tj. řešíme homogenní soustavu $(M - E)x = 0$. Netriviálním řešením je například vektor $x = (1, 3, 3)$. Jeho vydělením číslem $1 + 3 + 3 = 7$ dostaneme pravděpodobnostní vektor $(1/7, 3/7, 3/7)$. Stav A tedy bude navštěvován s pravděpodobností $1/7$. \square