

Sbírka úloh k předmětu MB141

přednášející: Mgr. David Kruml, Ph. D.

cvičící: Mgr. Jan Procházka

jaro 2025

Obsah

1	Algebra	2
1.1	Komplexní čísla	2
1.2	Dělitelnost a zbytkové třídy modulo n	8
1.3	Polynomy	15
1.4	Soustavy lineárních rovnic	20
1.5	Maticový počet	27
1.6	Vektorové prostory a podprostory	34
1.7	Deteminant	42
2	Geometrie	48
2.1	Lineární zobrazení	48
2.2	Vlastní čísla a vektory	52
2.3	Afinní geometrie	59
2.4	Eukleidovská geometrie	66
3	Teorie čísel	74
3.1	Počítání v $\mathbb{Z}_m$	74
3.2	Šifrování	77
4	Aplikace	81
4.1	Rekurentní posloupnosti	81
4.2	Markovské procesy	85
4.3	Leslieho populační model	92
4.4	Lineární programování	95

Kapitola 1

Algebra

1.1 Komplexní čísla

Příklad 1.1.1. Číselné množiny, se kterými budeme počítat, jsou přirozená čísla $\mathbb{N}$, celá čísla $\mathbb{Z}$, racionální čísla $\mathbb{Q}$ a reálná čísla $\mathbb{R}$. Stručně si připomeňte vlastnosti sčítání a násobení na jednotlivých množinách.

Řešení. Na všech množinách je sčítání asociativní, tedy

$$x + (y + z) = (x + y) + z;$$

komutativní, tj.

$$x + y = y + x;$$

dále v $\mathbb{Z}$, $\mathbb{Q}$ a $\mathbb{R}$ máme 0 jako neutrální prvek

$$0 + x = x;$$

a ke každému prvku x máme opačný prvek $-x$, tj.

$$x + (-x) = 0.$$

Podobně násobení je na všech množinách asociativní

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z;$$

komutativní

$$x \cdot y = y \cdot x;$$

distributivní vzhledem ke sčítání

$$x \cdot (y + z) = x \cdot y + x \cdot z;$$

máme 1 jako neutrální prvek

$$1 \cdot x = x;$$

a v $\mathbb{Q}$ a v $\mathbb{R}$ máme ke každému nenulovému prvku x inverzní prvek $\frac{1}{x}$, tj.

$$x \cdot \frac{1}{x} = 1. \quad \triangle$$

Příklad 1.1.2. Zaveďte komplexní čísla a popište jejich základní vlastnosti.

Řešení. K reálným číslům přidáme komplexní jednotku i s vlastností $i^2 = -1$; jedná se o jeden z kořenů polynomu $x^2 + 1$. Operace zavádíme induktivně. Sčítání i násobení zachovávají „reálnost“ čísel, takže zde nic neměníme. Pro libovolné $b \in \mathbb{R}$ a i musíme přidat i jejich součin $b \cdot i$ s tím, že $b' \cdot (bi) = (b' b) i$ a $b i := bi$. To zaručí komutativitu a asociativitu násobení. Nakonec pro $a \in \mathbb{R}$ přidáme součty $a + bi$. Obecné komplexní číslo z je tedy tvaru

$$z = a + bi,$$

kde $a, b \in \mathbb{R}$. Číslo a nazýváme *reálnou částí* z , značíme $\Re(z)$ (případně $\text{Re}(z)$), číslo b pak *imaginární částí* z , značíme $\Im(z)$ (případně $\text{Im}(z)$). Všimněme si, že pro komplexní číslo z jsou $\Re(z)$ i $\Im(z) \in \mathbb{R}$. Platí, že dvě komplexní čísla jsou si rovna právě tehdy, jsou-li si rovny jejich reálné i imaginární části. Množinu všech komplexních čísel značíme $\mathbb{C}$.

Vezmeme $w = c + di \in \mathbb{C}$, $c, d \in \mathbb{R}$. Prozkoumáme chování součtu a součinu dle pravidel, která jsme použili při vytvoření komplexních čísel. Součet se chová tak, jak bychom čekali, tedy

$$z + w = (a + bi) + (c + di) = (a + c) + (b + d)i.$$

Můžeme tedy říci, že $\Re(z + w) = \Re(z) + \Re(w)$, podobně pro $\Im$. Pro součin použijeme pravidlo pro násobení mnohočlenů, tedy pravidlo „každý s každým“, přičemž následně vyčíslíme výrazy:

$$z \cdot w = (a + bi) \cdot (c + di) = ac + bci + adi + bd \underbrace{i^2}_{-1} = (ac - bd) + (bc + ad)i$$

Pak platí, že

$$\Re(z \cdot w) = \Re(z) \Re(w) - \Im(z) \Im(w), \quad \Im(z \cdot w) = \Re(z) \Im(w) + \Im(z) \Re(w). \quad (1.1)$$

Pro $z = a + bi \in \mathbb{C}$ zavedeme *číslo k němu komplexně sdružené*, značené $\bar{z}$, a definované jako $\bar{z} = a - bi$. Přiřazení komplexně sdruženého čísla má následující vlastnosti:

- $\bar{\bar{z}} = z$;
- $z = \bar{z}$ právě když $z \in \mathbb{R}$;
- aditivita $\overline{z + w} = \bar{z} + \bar{w}$;

- multiplikativita $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$.

První vlastnost je celkem zřejmá, stejně jako třetí. Druhou vlastnost si ukážeme později (jedna implikace je zřejmá), poslední se dá napočítat

$$\bar{z} \cdot \bar{w} = (a - bi) \cdot (c - di) = ac - bci - adi - bd = (ac - bd) - (bc + ad)i = \overline{z \cdot w}.$$

Spočítejme $z + \bar{z}$ a $z \cdot \bar{z}$. Máme

$$z + \bar{z} = (a + bi) + (a - bi) = 2a = 2\Re(z) \in \mathbb{R}$$

odtud bychom mohli definovat $\Re(z)$ jako $\frac{z+\bar{z}}{2}$, obdobně $\Im(z) = \frac{z-\bar{z}}{2i}$. Odtud vidíme, že pokud $z = \bar{z}$, pak $z = \frac{z+\bar{z}}{2} = \Re(z) \in \mathbb{R}$. Dále

$$z \cdot \bar{z} = (a + bi) \cdot (a - bi) = a^2 - b^2 i^2 = a^2 + b^2 \in \mathbb{R}.$$

a navíc je $z \bar{z} \geq 0$ a rovno nule pouze pro $z = 0$.¹ Definujeme *absolutní hodnotu komplexního čísla* z jako

$$|z| = \sqrt{z \cdot \bar{z}}$$

(výraz je korektně definován, neboť pod odmocninou je nezáporné reálné číslo, pro něž máme jednoznačně definovanou reálnou odmocninu). Nejdůležitější vlastností absolutní hodnoty je multiplikativita, $|z \cdot w| = |z| \cdot |w|$, což plyne rovnou z definice a multiplikativity reálné odmocniny.

S použitím komplexně sdruženého čísla můžeme spočítat převrácené číslo pro $z \neq 0$. Máme

$$\frac{1}{z} \cdot \frac{\bar{z}}{\bar{z}} = \frac{\bar{z}}{|z|^2},$$

což pomocí $z = a + bi$ dává

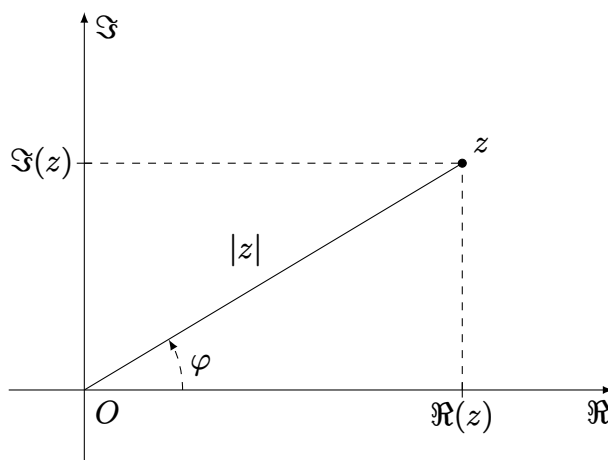
$$\frac{1}{a + bi} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}i.$$

Pro $w \in \mathbb{C}$, $w = c + di$ máme podíl

$$\frac{w}{z} = \frac{w \bar{z}}{|z|^2} = \frac{(ac + bd) + (ad - bc)i}{a^2 + b^2}.$$

Zápis $z = a + bi$ nazýváme *algebraickým tvarem* komplexního čísla z . Jelikož je z určeno dvojicí reálných čísel, můžeme si jej zakreslit do tzv. *Gaußovy roviny*, viz obrázek 1.1. S použitím pravoúhlého trojúhelníku $\triangle(O, \Re(z), z)$ vidíme, že:

¹Obecně neexistuje uspořádání komplexních čísel, které by zachovávalo operace. Pokud by bylo například $i > 0$, pak násobení i by nerovnost zachovávalo, tedy bychom dostali $-1 = i^2 > 0 \cdot i = 0$. Obdobně položili-li bychom $i < 0$, pak násobení nerovnosti i by ji otáčelo a opět bychom dostali $-1 > 0$. Píšeme-li tedy pro nějaké $z, w \in \mathbb{C}$ výrazy typu $z \leq w$, implicitně tím uvažujeme tato čísla reálná.



Obrázek 1.1: Zakreslíme si do Gaußovy roviny komplexní číslo $z = \Re(z) + i\Im(z)$ (zde naznačené pro $\Re(z), \Im(z) \geq 0$, pro ostatní případy by byl obrázek „překlopený.“)

$$\cos \varphi = \frac{\Re(z)}{|z|}; \quad \sin \varphi = \frac{\Im(z)}{|z|}; \quad (1.2)$$

a odtud pro $z \neq 0$ máme

$$z = |z| \cdot \frac{\Re(z) + i\Im(z)}{|z|} = |z| \cdot (\cos \varphi + i \sin \varphi).$$

Tento zápis komplexních čísel se nazývá *goniometrický*, a kromě již zavedené absolutní hodnoty je důležitý také úhel φ . Ten se nazývá *argumentem* čísla z a někdy se značí $\varphi = \arg(z)$. Tento úhel je jednoznačně určen rovnicemi (1.2) až na násobek 2π , což je perioda funkcí $\sin$ a $\cos$. Proto klademe $\arg(z) \in [0, 2\pi)$.²

Připomeneme si součtové vzorce pro funkce $\sin$ a $\cos$:

$$\begin{aligned} \sin(\alpha + \beta) &= \sin(\alpha) \cos(\beta) + \cos(\alpha) \sin(\beta) \\ \cos(\alpha + \beta) &= \cos(\alpha) \cos(\beta) - \sin(\alpha) \sin(\beta) \end{aligned} \quad (1.3)$$

(povšimněte si podobnosti s (1.1), což není náhoda). Pomocí nich máme pro $z = |z| (\cos \varphi + i \sin \varphi)$ a $w = |w| (\cos \psi + i \sin \psi)$ součin

$$\begin{aligned} z \cdot w &= |z| \cdot |w| \cdot (\cos \varphi + i \sin \varphi) (\cos \psi + i \sin \psi) \\ &= |z| |w| \cdot \left((\cos(\varphi) \cos(\psi) - \sin(\varphi) \sin(\psi)) + i (\sin(\varphi) \cos(\psi) + \cos(\varphi) \sin(\psi)) \right) \\ &\stackrel{(1.3)}{=} |z| |w| \cdot (\cos(\varphi + \psi) + i \sin(\varphi + \psi)). \end{aligned} \quad (1.4)$$

Odtud vidíme důležitou vlastnost argumentu, tedy že

$$\arg(z \cdot w) = \arg(z) + \arg(w) \text{ modulo } 2k\pi$$

²Argumet je jednoznačně určen v jakémkoli jednostranně otevřeném intervalu o délce 2π , nejčastěji se používá $[0, 2\pi)$ nebo ještě častěji $[-\pi, \pi)$.

pro $k \in \mathbb{Z}$. Důsledkem (1.4) je pak Moivrova věta.

Věta (Moivre). Pro $z \in \mathbb{C} \setminus \{0\}$, $\arg(z) = \varphi$, $a, n \in \mathbb{N}$ platí

$$z^n = |z|^n (\cos(n\varphi) + i \sin(n\varphi)).$$

Důsledek. Pro $z = |z| (\cos(\varphi + 2k\pi) + i \sin(\varphi + 2k\pi)) \in \mathbb{C} \setminus \{0\}$, $k \in \mathbb{Z}$, $a, n \in \mathbb{N}$ platí

$$\sqrt[n]{z} = \sqrt[n]{|z|} \left(\cos \frac{\varphi + 2k\pi}{n} + i \sin \frac{\varphi + 2k\pi}{n} \right)$$

pro $k \in \mathbb{Z}$, přičemž pro různá k existuje právě n různých hodnot.

Moivrovu větu a její důsledek pak použijeme při počítání komplexních odmocnin. $\triangle$

Příklad 1.1.3. Najděte řešení kvadratické rovnice $z^2 = a$ pro $a \in \mathbb{R}$. Najděte řešení kvadratické rovnice $z^2 = a + bi$ v algebraickém a goniometrickém tvaru.

Řešení. Je-li $a \geq 0$, má rovnice $z^2 = a$ dvě řešení, $z = \pm\sqrt{a}$. Je-li $a < 0$, pak je $-a > 0$ a rovnici lze psát jako

$$z^2 = (-a)i^2$$

a odtud vidíme rovnou $z = \pm i\sqrt{-a}$.

Uvažujme rovnici $z^2 = a + bi$. Můžeme psát $z = c + di$, odtud

$$z^2 = c^2 - d^2 + 2cdi = a + bi.$$

Porovnáním reálných a imaginárních částí přejdeme k soustavě

$$\begin{aligned} c^2 - d^2 &= a \\ 2cd &= b \end{aligned}$$

dvou rovnic se dvěma *reálnými* neznámými, kterou vyřešíme. Podrobněji viz Úlohu 1.10 sbírce příkladů z předmětu M6170 Analýza v komplexním oboru.³

Řešíme-li rovnici $z^2 = r (\cos \varphi + i \sin \varphi)$, máme podle důsledku Moivrovovy věty

$$\begin{aligned} z &= \sqrt{r} \left(\cos \frac{\varphi + 2k\pi}{2} + i \sin \frac{\varphi + 2k\pi}{2} \right) \\ &= \sqrt{r} \left(\cos \left(\frac{\varphi}{2} + k\pi \right) + i \sin \left(\frac{\varphi}{2} + k\pi \right) \right), \end{aligned}$$

odkud s použitím (1.3) a vlastností goniometrických funkcí následně dostáváme

$$= \pm \sqrt{r} \left(\cos \frac{\varphi}{2} + i \sin \frac{\varphi}{2} \right) \quad \triangle$$

³https://www.math.muni.cz/~zemanekp/files/M6170/sbirka_M6170_Prochazka.pdf

Příklad 1.1.4. Určete všechna z taková, že

a) $z^3 = 1 + i$,

b) $z^6 = 64$.

Řešení. V obou případech použijeme důsledek Moivroy věty. Začneme a). Nejprve si převedeme číslo $1 + i$ do goniometrického tvaru. Vidíme, že

$$|1 + i| = \sqrt{1 + 1} = \sqrt{2}.$$

Zbývá najít argument. Hledáme φ takové, že

$$\cos \varphi = \frac{1}{\sqrt{2}}, \quad \sin \varphi = \frac{1}{\sqrt{2}}.$$

Sinus i kosinus φ musejí být stejné, to nastane pro $\varphi = \frac{\pi}{4} + 2k\pi = \frac{8k+1}{4}\pi$, $k \in \mathbb{Z}$. Řešíme tedy rovnici

$$z^3 = \sqrt{2} \left(\cos \left(\frac{8k+1}{4}\pi \right) + i \sin \left(\frac{8k+1}{4}\pi \right) \right)$$

odkud dostaneme

$$z = \sqrt[3]{2} \left(\cos \left(\frac{8k+1}{12}\pi \right) + i \sin \left(\frac{8k+1}{12}\pi \right) \right)$$

pro $k \in \{0, 1, 2\}$. Pro $k = 1$ dostaneme argument $\frac{3}{4}\pi$ se snadno vyčíslitelnými hodnotami sinu a kosinu. Máme

$$\cos \frac{3\pi}{4} = -\frac{1}{\sqrt{2}} \quad \sin \frac{3\pi}{4} = \frac{1}{\sqrt{2}},$$

odtud

$$\sqrt[3]{2} \left(\cos \frac{3\pi}{4} + i \sin \frac{3\pi}{4} \right) = \sqrt[3]{2} \left(-\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}} \right) = -\frac{1}{\sqrt[3]{2}} + \frac{i}{\sqrt[3]{2}}.$$

Celkem tedy máme

$$z = \begin{cases} \sqrt[3]{2} \left(\cos \frac{\pi}{12} + i \sin \frac{\pi}{12} \right) \\ -\frac{1}{\sqrt[3]{2}} + \frac{i}{\sqrt[3]{2}} \\ \sqrt[3]{2} \left(\cos \frac{17\pi}{12} + i \sin \frac{17\pi}{12} \right) \end{cases}$$

Nyní řešíme část b). Je jasné, že $|64| = 64 = 2^6$, podobně je zřejmě argument 64 roven 0 (reálná čísla mají kladná argument 0 a záporná argument $\pm\pi$ podle potřeby). Řešíme rovnici

$$z^6 = 64 \left(\cos(2k\pi) + i \sin(2k\pi) \right),$$

pomocí důsledku Moivrovovy věty dostaneme

$$z = 2 \left(\cos \frac{k\pi}{3} + i \sin \frac{k\pi}{3} \right)$$

pro $k \in \{0, 1, 2, 3, 4, 5\}$. Zde umíme snadno vyčíslit hodnoty sinů a kosinů pro všechna k . Máme

$$z = \begin{cases} 2 (\cos 0 + i \sin 0) & = & 2 \\ 2 \left(\cos \frac{\pi}{3} + i \sin \frac{\pi}{3} \right) & = & 1 + i\sqrt{3} \\ 2 \left(\cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3} \right) & = & -1 + i\sqrt{3} \\ 2 (\cos \pi + i \sin \pi) & = & -2 \\ 2 \left(\cos \frac{4\pi}{3} + i \sin \frac{4\pi}{3} \right) & = & -1 - i\sqrt{3} \\ 2 \left(\cos \frac{5\pi}{3} + i \sin \frac{5\pi}{3} \right) & = & 1 - i\sqrt{3} \end{cases}$$

Podobné úlohy jsou například Úlohy 1.17 – 1.19 ve sbírce úloh z Analýzy v komplexním oboru M6170.⁴ $\triangle$

1.2 Dělitelnost a zbytkové třídy modulo n

Příklad 1.2.1. Zaveďte kongruence a zbytkové třídy modulo n pro $2 \leq n \in \mathbb{N}$.

Řešení. Zafixujme $2 \leq n \in \mathbb{N}$. Řekneme, že n dělí $m \in \mathbb{Z}$, jestliže existuje $q \in \mathbb{Z}$ takové, že $m = q \cdot n$. Pak píšeme

$$n \mid m$$

Pro $m \in \mathbb{Z}$ existují jednoznačná $q, r \in \mathbb{Z}$, $0 \leq r < n$ taková, že

$$m = q \cdot n + r$$

(věta o dělení se zbytkem). Řekneme, že a a b jsou *kongruentní* modulo n , psáno

$$a \equiv b \pmod{n},$$

jestliže dávají stejný zbytek po dělení n , neboli lze li obě psát ve tvaru $a = qn + r$ a $b = q'n + r$. To je zřejmě právě tehdy, když

$$b - a = n(q' - q)$$

tedy právě tehdy, když $n \mid b - a$. Je-li $a_1 \equiv b_1$ a $a_2 \equiv b_2 \pmod{n}$, pak

$$a_1 + a_2 \equiv b_1 + b_2 \pmod{n}, \quad a_1 a_2 \equiv b_1 b_2 \pmod{n}. \quad (1.5)$$

Podle předpokladů můžeme psát $b_1 - a_1 = n \cdot q_1$ a $b_2 - a_2 = n \cdot q_2$ pro nějaká $q_1, q_2 \in \mathbb{Z}$. Pro důkaz první kongruence chceme, aby n dělilo $b_1 + b_2 - (a_1 + a_2)$, což ovšem můžeme

⁴https://www.math.muni.cz/~zemanekp/files/M6170/sbirka_M6170_Prochazka.pdf

psát jako $b_1 - a_1 + b_2 - a_2 = (q_1 + q_2)n$, což je dělitelné n . Pro důkaz druhé kongruence chceme, aby výraz $b_1 b_2 - a_1 a_2$ byl dělitelný n . K němu si přičteme a odečteme výraz $a_1 b_2$, čímž máme

$$b_1 b_2 - a_1 a_2 + a_1 b_2 - a_1 b_2 = (b_1 - a_1) b_2 + a_1 (b_2 - a_2) = (q_1 b_2 + a_1 q_2) n,$$

přičemž výraz napravo je dělitelný n . Kongruence tedy zachovávají sčítání i násobení.

Kongruence modulo n je relace *ekvivalence*, neboť

- $a \equiv a \pmod{n}$, jelikož $n \mid 0 = a - a$,
- $a \equiv b \Rightarrow b \equiv a \pmod{n}$, protože $a - b = -(b - a)$ a dělitelnost je zachována bez ohledu na znaménko,
- $a \equiv b \ \& \ b \equiv c \Rightarrow a \equiv c \pmod{n}$ díky tomu, že $c - a = (c - b) + (b - a)$ a kongruence zachovávají součet (to, že $n \mid m$ je ekvivalentní tvrzení $m \equiv 0 \pmod{n}$).

Máme tedy třídy rozkladu množiny $\mathbb{Z}$ pomocí této relace ekvivalence. Přesněji řešeno, množina $\mathbb{Z}$ je rozdělena na n podmnožin tvaru

$$[r]_n := \{nq + r \in \mathbb{Z} \mid q \in \mathbb{Z}\}.$$

To, že každé celé číslo patří (pro dané n) právě do jedné z množin $[r]_n$ vyplývá z věty o dělení se zbytkem. Můžeme definovat součet a součin tříd kongruence $[r]_n$ a $[r']_n$ tak, že vezmeme libovolná dvě čísla z těchto množin (reprezentanty) a podíváme se, do které třídy padne jejich součet respektive součin. Právě (1.5) zaručí, že součet i součin reprezentantů padne vždy do jedné třídy bez ohledu na jejich výběr. Takto definované sčítání a násobení dědí díky své definici některé důležité vlastnosti sčítání a násobení celých čísel – zejména se jedná o komutativitu a asociativitu obou operací, stejně jako o distributivitu násobení vůči sčítání. Třída $[0]_n$ se chová jako neutrální prvek vůči sčítání, třída $[1]_n$ jako neutrální prvek vzhledem k násobení. Dále třída $[n - r]_n$ je opačným prvkem k $[r]_n$ vůči sčítání. Množinu tříd kongruence značíme⁵ $\mathbb{Z}_n$.

Na množině $\mathbb{Z}_n$ máme definované sčítání i násobení pomocí reprezentantů. Lze zvolit libovolné, v praxi se však často volí reprezentanti *co nejmenší*, tedy $0, 1, \dots, r, \dots, n - 1$, případně také doplněné o $-1, -2, \dots, -n + 1$. Kladní reprezentanti z tohoto seznamu jsou právě povolené zbytky po dělení n z naší formulace věty o dělení se zbytkem ze začátku cvičení. Lze tak říci, že na množině zbytků definujeme součet jako zbytek součtu po dělení n , součin podobně jako zbytek součinu po dělení n . $\triangle$

Příklad 1.2.2. Pomocí kongruencí dokažte, že pro libovolná celá čísla a platí:

- a) a^2 má po dělení 4 zbytek 0 nebo 1, c) a^4 má po dělení 16 zbytek 0 nebo 1.
b) a^2 má po dělení 8 zbytek 0, 1 nebo 4,

⁵V tomto předmětu ji budeme značit tak, jinde se lze také setkat s označením $\mathbb{Z}/(n)$, $\mathbb{Z}/n\mathbb{Z}$ nebo $\mathbb{Z}/n$,

Řešení. Připomeneme si vzorečky pro počítání s mocninami

$$x^{a+b} = x^a x^b \qquad x^{a \cdot b} = (x^a)^b = (x^b)^a \quad (1.6)$$

a binomickou větou.

$$(x + y)^m = \sum_{k=0}^m \binom{m}{k} x^k y^{m-k} \quad (1.7)$$

Právě binomická věta nám umožní si počítání zjednodušit. Ptáme-li se, jaký zbytek r dává nějaký výraz a po dělení n , ptáme se vlastně, čemu je a kongruentní modulo n . V zadání máme mocniny. Libovolné $a \in \mathbb{Z}$ můžeme psát ve tvaru $a = nq + r$. Dosazením do (1.7), kde bereme $x = nq$ a $y = r$, dostáváme

$$(nq + r)^m = \sum_{k=0}^m \binom{m}{k} n^k q^k r^{m-k}.$$

Vidíme, že jedině člen s $k = 0$, tedy r^m není dělitelný n . (To už víme z faktu, že kongruence zachovávají násobení, tj. je-li $a \equiv r \pmod{n}$, je $a^m \equiv r^m \pmod{n}$.) Navíc však je u členů $k \neq 0$ koeficient $\binom{m}{k} \neq 1$, tudíž hledáme-li zbytek po dělení a^m nějakým N , stačí uvažovat třídy kongruence a pouze modulo n takovým, aby pro každé $k = 1, 2, \dots, m$ byl výraz $\binom{m}{k} n^k$ dělitelný N . Přirozeně hledáme n mezi děliteli N . To si ukážeme na příkladech.

Začněme a). Máme mocninu a^2 , tedy $m = 2$, $N = 4$ a vidíme, že jak $\binom{2}{1} 2^1$, tak $\binom{2}{2} 2^2$ jsou dělitelné 4. Stačí tedy uvažovat jen třídy kongruence modulo 2. Je-li $a \equiv 0 \pmod{2}$, je $a^2 \equiv 0 \pmod{4}$. Obdobně je-li $a \equiv 1 \pmod{2}$, je $a^2 \equiv 1 \pmod{4}$.

Pokračujeme b). Zde je $m = 2$ a $N = 8$. Hledáme n takové, že pro každé k mezi 1 a 4 bylo $\binom{2}{k} n^k$ dělitelné 8. Snadno se ukáže, že stačí brát $n = 4$. (Pro $n = 4$ máme $\binom{2}{1} 4 = 8$ dělitelné 8 a pro vyšší k již $8 \mid 4^k$. Podobně se ukáže, že $n = 2$ nestačí.) Tudíž máme výsledek.

$$\begin{array}{lll} a \equiv 0 \pmod{4} & \Rightarrow & a^2 \equiv 0 \pmod{8} \\ a \equiv 1 \pmod{4} & \Rightarrow & a^2 \equiv 1 \pmod{8} \\ a \equiv 2 \pmod{4} & \Rightarrow & a^2 \equiv 4 \pmod{8} \\ a \equiv 3 \pmod{4} & \Rightarrow & a^2 \equiv 9 \equiv 1 \pmod{8} \end{array}$$

Nyní vyřešíme c). Máme $m = 4$ a $N = 16$. Hledáme příhodné n . Vidíme, že $n = 2$ nebude stačit, neboť $\binom{4}{1} 2^1 = 8$ není dělitelné 16. Zkusíme $n = 4$. Máme $\binom{4}{1} 4^1 = 16$ dělitelné 16 a pro $k > 1$ je 4^k dělitelné 16 samo o sobě. Obdobně jako minule máme tedy výsledek.

$$\begin{array}{lll} a \equiv 0 \pmod{4} & \Rightarrow & a^4 \equiv 0 \pmod{16} \\ a \equiv 1 \pmod{4} & \Rightarrow & a^4 \equiv 1 \pmod{16} \\ a \equiv 2 \pmod{4} & \Rightarrow & a^4 \equiv 16 \equiv 0 \pmod{16} \\ a \equiv 3 \pmod{4} & \Rightarrow & a^4 \equiv 81 \equiv 1 \pmod{16} \end{array} \quad \triangle$$

Příklad 1.2.3. Pomocí kongruencí ukažte, že pro každé $n \in \mathbb{N}$ platí:

- a) číslo 3 dělí číslo $4^n - 1$,
 b) číslo 5 dělí číslo $n^5 - n$

c) číslo 5 dělí číslo $3^{3n+1} + 2^{n+1}$.

Řešení. Vyřešíme a). Máme $4 \equiv 1 \pmod{3}$, odtud

$$4^n - 1 \equiv 1^n - 1 = 1 - 1 = 0 \pmod{3},$$

tedy je skutečně $4^n - 1$ dělitelné 3. Přejdeme k b). Zde již budeme muset uvažovat všechny zbytkové třídy modulo 5. (Pokud bychom chtěli použít postup z příkladu 1.2.2, zjistili bychom, že nejmenší n je 5.) Pro $n \equiv 0 \pmod{5}$ je $n^5 - n \equiv 0 \pmod{5}$ zadarmo. Je-li $n \equiv 1 \pmod{5}$, máme

$$n^5 - n \equiv 1^5 - 1 = 1 - 1 = 0 \pmod{5}.$$

Pro $n \equiv 2 \pmod{5}$ dostaneme

$$n^5 - n \equiv 2^5 - 2 = 32 - 2 = 30 \equiv 0 \pmod{5},$$

pro $n \equiv 3 \pmod{5}$ pak

$$n^5 - n \equiv 3^5 - 3 = (3^2)^2 \cdot 3 - 3 \equiv 4^2 \cdot 3 - 3 = 16 \cdot 3 - 3 \equiv 1 \cdot 3 - 3 = 0 \pmod{5}$$

a pro $n \equiv 4 \pmod{5}$ následně

$$n^5 - n \equiv 4^5 - 4 = (2^5)^2 - 4 = 32^2 - 4 \equiv 2^2 - 4 = 4 - 4 = 0 \pmod{5},$$

tedy je vždy $n^5 - n$ dělitelné 5. Nyní vyřešíme c) podobně jako a), přičemž použijeme pravidla pro počítání s mocninami (1.6).

$$3^{3n+1} + 2^{n+1} = 3 \cdot (3^3)^n + 2 \cdot 2^n = 3 \cdot 27^n + 2 \cdot 2^n \equiv 3 \cdot 2^n + 2 \cdot 2^n = 5 \cdot 2^n \equiv 0 \pmod{5} \quad \triangle$$

Příklad 1.2.4. Jaká je poslední cifra čísel 7^{14} a 3^{59} ?

Řešení. Hledáme vlastně zbytky po dělení 10, tedy ptáme se, čemu jsou daná čísla kongruentní modulo 10. Počítáme postupně:

$$\begin{aligned} 7^1 &= 7, \\ 7^2 &\equiv 9 \equiv -1 \pmod{10}, \\ 7^3 &= 7^2 \cdot 7 \equiv -1 \cdot 7 = -7 \equiv 3 \pmod{10}, \\ 7^4 &\equiv 3 \cdot 7 = 21 \equiv 1 \pmod{10}. \end{aligned}$$

Vidíme, že $7^4 \equiv 1$. Pomocí (1.6) máme

$$7^{14} = 7^{4 \cdot 3 + 2} = (7^4)^3 \cdot 7^2 \equiv 1^3 \cdot 7^2 = 7^2 \equiv 9 \pmod{10},$$

tedy poslední cifra čísla 7^{14} je 9. Obdobně počítáme s 3:

$$\begin{aligned} 3^1 &= 3, & 3^3 &\equiv 7 \pmod{10}, \\ 3^2 &= 9, & 3^4 &\equiv 1 \pmod{10}. \end{aligned}$$

Máme tedy opět

$$3^{59} = 3^{4 \cdot 14 + 3} = (3^4)^{14} \cdot 3^3 \equiv 1^{14} \cdot 3^3 = 3^3 \equiv 7 \pmod{10}$$

a poslední cifra čísla 3^{59} je 7. $\triangle$

Příklad 1.2.5. Jak poznáme, že je celé číslo dělitelné 3, 4, 8, 9, 11? Odpovědi odvoďte a zdůvodněte s využitím kongruencí.

Řešení. Využijeme dekadický zápis.⁶ Libovolné číslo $x \in \mathbb{N}$ lze psát ve tvaru

$$x = \sum_{k=0}^n a_k 10^k,$$

kde $a_k \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ jsou číslice. Nejprve odvodíme pravidlo pro dělitelnost 3 a 9. Vzhledem k tomu, že $10 \equiv 1 \pmod{9}$ (a tudíž i modulo 3), je

$$x = \sum_{k=0}^n a_k 10^k \equiv \sum_{k=0}^n a_k 1^k = \sum_{k=0}^n a_k \pmod{9} \text{ i } \pmod{3}$$

tedy bude x dělitelné 9 nebo 3 právě tehdy, když bude dělitelný jeho ciferný (po iteraci superciferný) součet. Obdobně odvodíme pravidlo pro dělitelnost 11. Jelikož je $10 \equiv -1 \pmod{11}$, máme

$$x = \sum_{k=0}^n a_k 10^k \equiv \sum_{k=0}^n a_k (-1)^k = \sum_{k \text{ sudé}} a_k - \sum_{k \text{ liché}} a_k \pmod{11}$$

tedy vidíme, že x je dělitelné 11 právě tehdy, když je dělitelný alternující součet jeho číslic (přičemž nezáleží na tom, jestli začneme s plus, nebo s mínus, protože znaménko zachovává dělitelnost). Pro dělitelnost 4 využijeme faktu, že $4 \mid 10^k$ pro $k \geq 2$, tedy

$$x = \sum_{k=0}^n a_k 10^k \equiv 10 a_1 + a_0 \pmod{4},$$

takže x je dělitelné 4 tehdy, a jen tehdy, je-li dělitelné poslední dvojčíslí. Obdobně pro dělitelnost 8 máme $8 \mid 10^k$ pro $k \geq 3$, tudíž

$$x = \sum_{k=0}^n a_k 10^k \equiv 100 a_2 + 10 a_1 + a_0 \pmod{8}$$

a x je dělitelné 8 pokud je dělitelné poslední trojčíslí. Zajímavá jsou také pravidla pro dělitelnost 7 a 13, viz Příklad 2.8 na straně 15 ve sbírce k předmětu MB154 Diskrétní matematika.⁷ $\triangle$

⁶Pomocí jiných zápisů by to bylo snazší. V zápise o základu n se dělitelnost n pozná tak, že poslední číslice je 0.

⁷<https://www.math.muni.cz/~prochazka/vyuka/sbirka.pdf>

Příklad 1.2.6. Nalezněte celá čísla x a y tak, aby $883x + 487y = d$ byl největší společný dělitel čísel 883 a 487. Spočtěte x a y i pro následující dvojice čísel 227, 133 a 3 441, 2 665.

Řešení. Platí, že pro celá čísla m a n existují koeficienty k, l takové, že

$$km + ln = d$$

kde d je největší společný dělitel čísel m a n . Tato čísla nejsou určena jednoznačně – existují totiž také čísla r, s taková, že

$$rm + sn = 0$$

a pak přičtením násobků r , resp. s k k , resp. l dostaneme jiné koeficienty. K nalezení d , jakož i k a l bychom mohli použít přímo Eukleidův algoritmus, nicméně to bývá zdlouhavé – viz alternativní řešení. My budeme postupovat metodou úpravy rovnic. Soustavu

$$1 \cdot m + 0 \cdot n = m$$

$$0 \cdot m + 1 \cdot n = n$$

upravíme pomocí úprav „výměna rovnic“, „vynásobení jedné rovnice ± 1 “ a „přičtení násobku jedné rovnice k druhé“ (což jsou elementární řádkové úpravy nad $\mathbb{Z}$) upravíme na tvar

$$k \cdot m + l \cdot n = d$$

$$r \cdot m + s \cdot n = 0$$

(tedy vynulujeme jeden z členů napravo od rovnítky), přičemž dostaneme největší společný dělitel a hledané koeficienty, zvané Bézoutovy. Provádění úprav odpovídá běhu Eukleidova algoritmu na pravé straně rovnic. Bude se nám hodit maticový zápis soustavy. Uvažme první dvojici 883 a 487.

$$\begin{aligned} \left(\begin{array}{cc|c} 1 & 0 & 883 \\ 0 & 1 & 487 \end{array} \right) &\sim \left(\begin{array}{cc|c} 1 & -2 & -91 \\ 0 & 1 & 487 \end{array} \right) \sim \left(\begin{array}{cc|c} 1 & -2 & -91 \\ 5 & -9 & 32 \end{array} \right) \sim \left(\begin{array}{cc|c} 16 & -29 & 5 \\ 5 & -9 & 32 \end{array} \right) \sim \\ &\sim \left(\begin{array}{cc|c} 16 & -29 & 5 \\ -91 & 165 & 2 \end{array} \right) \sim \left(\begin{array}{cc|c} 198 & -359 & 1 \\ -91 & 165 & 2 \end{array} \right) \sim \left(\begin{array}{cc|c} 198 & -359 & 1 \\ -487 & 883 & 0 \end{array} \right) \end{aligned}$$

Máme tedy rovnost $198 \cdot 883 - 359 \cdot 487 = 1$ a tato čísla jsou nesoudělná. Můžeme obdobně počítat pro ostatní dvojice. Nejprve 227 a 133.

$$\begin{aligned} \left(\begin{array}{cc|c} 1 & 0 & 227 \\ 0 & 1 & 133 \end{array} \right) &\sim \left(\begin{array}{cc|c} 1 & -2 & -39 \\ 0 & 1 & 133 \end{array} \right) \sim \left(\begin{array}{cc|c} 1 & -2 & -39 \\ 3 & -5 & 16 \end{array} \right) \sim \left(\begin{array}{cc|c} 7 & -12 & -7 \\ 3 & -5 & 16 \end{array} \right) \sim \\ &\sim \left(\begin{array}{cc|c} 7 & -12 & -7 \\ 17 & -29 & 2 \end{array} \right) \sim \left(\begin{array}{cc|c} 75 & -128 & 1 \\ 17 & -29 & 2 \end{array} \right) \sim \left(\begin{array}{cc|c} 75 & -128 & 1 \\ -133 & 227 & 0 \end{array} \right) \end{aligned}$$

Nakonec počítejme pro 3 441 a 2 665.

$$\begin{aligned}
\left(\begin{array}{cc|c} 1 & 0 & 3441 \\ 0 & 1 & 2665 \end{array} \right) &\sim \left(\begin{array}{cc|c} 1 & -1 & 776 \\ 0 & 1 & 2665 \end{array} \right) \sim \left(\begin{array}{cc|c} 1 & -1 & 776 \\ -3 & 4 & 337 \end{array} \right) \sim \\
&\sim \left(\begin{array}{cc|c} 7 & -9 & 102 \\ -3 & 4 & 337 \end{array} \right) \sim \left(\begin{array}{cc|c} 7 & -9 & 102 \\ -24 & 31 & 31 \end{array} \right) \sim \left(\begin{array}{cc|c} 79 & -102 & 9 \\ -24 & 31 & 31 \end{array} \right) \sim \\
&\sim \left(\begin{array}{cc|c} 79 & -102 & 9 \\ -261 & 337 & 4 \end{array} \right) \sim \left(\begin{array}{cc|c} 601 & -776 & 1 \\ -261 & 337 & 4 \end{array} \right) \sim \left(\begin{array}{cc|c} 601 & -776 & 1 \\ -2665 & 3441 & 0 \end{array} \right) \quad \triangle
\end{aligned}$$

Jiné řešení. Jinou metodou je zpětné dosazování do Eukleidova algoritmu. Dělíme postupně větší číslo menším se zbytkem, přičemž se budou hodit záporné zbytky. Čísla si pro přehlednost vyznačíme barevně.

$$\begin{array}{ll}
883 = 2 \cdot 487 - 91 & \rightsquigarrow 91 = 2 \cdot 487 - 883 \\
487 = 5 \cdot 91 + 32 & \rightsquigarrow 32 = 487 - 5 \cdot 91 \\
91 = 3 \cdot 32 - 5 & \rightsquigarrow 5 = 3 \cdot 32 - 91 \\
32 = 6 \cdot 5 + 2 & \rightsquigarrow 2 = 32 - 6 \cdot 5 \\
5 = 2 \cdot 2 + 1 & \rightsquigarrow 1 = 5 - 2 \cdot 2
\end{array}$$

Vidíme, že největším společným dělitelem čísel 883 a 487 je 1. Následně počítáme a zpětně dosazujeme do Eukleidova algoritmu.

$$\begin{aligned}
1 &= 5 - 2 \cdot 2 = 5 - 2 \cdot (32 - 6 \cdot 5) = 13 \cdot 5 - 2 \cdot 32 \\
&= 13 \cdot (2 \cdot 32 - 91) - 2 \cdot 32 = 37 \cdot 32 - 13 \cdot 91 \\
&= 37 \cdot (487 - 5 \cdot 91) - 13 \cdot 91 = 37 \cdot 487 - 198 \cdot 91 \\
&= 37 \cdot 487 - 198 \cdot (2 \cdot 487 - 883) = 198 \cdot 883 - 359 \cdot 487
\end{aligned}$$

Hledaná čísla x a y jsou 198 a -359 , přičemž $d = 2$. Obdobně můžeme postupovat i pro další dvojice čísel.

$$\begin{aligned}
227 &= 2 \cdot 133 - 39 \\
133 &= 3 \cdot 39 + 16 \\
39 &= 2 \cdot 16 + 7 \\
16 &= 2 \cdot 7 + 2 \\
7 &= 3 \cdot 2 + 1
\end{aligned}$$

I čísla 227 a 133 jsou nesoudělná. Zpětným dosazováním dostaneme koeficienty do Bézoutovy rovnosti.

$$\begin{aligned}
1 &= 7 - 3 \cdot 2 = 7 - 3 \cdot (16 - 2 \cdot 7) = 7 \cdot 7 - 3 \cdot 16 \\
&= 7 \cdot (39 - 2 \cdot 16) - 3 \cdot 16 = 7 \cdot 39 - 17 \cdot 16 \\
&= 7 \cdot 39 - 17 \cdot (133 - 3 \cdot 39) = 58 \cdot 39 - 17 \cdot 133 \\
&= 58 \cdot (2 \cdot 133 - 227) - 17 \cdot 133 = 99 \cdot 133 - 58 \cdot 227
\end{aligned}$$

Nakonec nalezneme koeficienty i pro dvojici 3 441 a 2 665.

$$\begin{aligned}
 3\,441 &= 2\,665 + 776 \\
 2\,665 &= 3 \cdot 776 + 337 \\
 776 &= 2 \cdot 337 + 102 \\
 337 &= 3 \cdot 102 + 31 \\
 102 &= 3 \cdot 31 + 9 \\
 31 &= 3 \cdot 9 + 4 \\
 9 &= 2 \cdot 4 + 1
 \end{aligned}$$

Koeficienty dostaneme zpětným dosazováním.

$$\begin{aligned}
 1 &= 9 - 2 \cdot 4 = 9 - 2 \cdot (31 - 3 \cdot 9) = 7 \cdot 9 - 2 \cdot 31 \\
 &= 7 \cdot (102 - 3 \cdot 31) - 2 \cdot 31 = 7 \cdot 102 - 23 \cdot 31 \\
 &= 7 \cdot 102 - 23 \cdot (337 - 3 \cdot 102) = 76 \cdot 102 - 23 \cdot 337 \\
 &= 76 \cdot (776 - 2 \cdot 337) - 23 \cdot 337 = 76 \cdot 776 - 175 \cdot 337 \\
 &= 76 \cdot 776 - 175 \cdot (2\,665 - 3 \cdot 776) = 601 \cdot 776 - 175 \cdot 2\,665 \\
 &= 601 \cdot (3\,441 - 2\,665) - 175 \cdot 2\,665 = 601 \cdot 3\,441 - 776 \cdot 2\,665 \quad \triangle
 \end{aligned}$$

Příklad 1.2.7. Najděte inverzní prvek k číslu 157 modulo 2 475.

Řešení. Hledáme vlastně takové m , že $157 \cdot m \equiv 1 \pmod{2\,475}$. Platí, že modulární inverze existuje právě tehdy, když jsou daná čísla nesoudělná. Nesoudělnost 157 a 2 475 ověříme pomocí Eukleidova algoritmu a modulární iniverzi najdeme pomocí Bézoutových koeficientů.

$$\begin{aligned}
 \left(\begin{array}{cc|c} 1 & 0 & 2\,475 \\ 0 & 1 & 157 \end{array} \right) &\sim \left(\begin{array}{cc|c} 1 & -16 & -37 \\ 0 & 1 & 157 \end{array} \right) \sim \left(\begin{array}{cc|c} 1 & -16 & -37 \\ 4 & -63 & 9 \end{array} \right) \sim \\
 &\sim \left(\begin{array}{cc|c} 17 & -268 & -1 \\ 4 & -63 & 9 \end{array} \right) \sim \left(\begin{array}{cc|c} -17 & 268 & 1 \\ 157 & -2\,475 & 0 \end{array} \right)
 \end{aligned}$$

Protože $-17 \cdot 2\,475 \equiv 0 \pmod{2\,475}$, vidíme, že

$$268 \cdot 157 \equiv 1 \pmod{2\,475}$$

a 268 je inverze k 157 modulo 2 475. △

1.3 Polynomy

Příklad 1.3.1. V oboru komplexních čísel řešte následující kvadratické rovnice:

$$\text{a) } x^2 - 6x + 58 = 0, \quad \text{b) } 9x^2 - 8x + 29 = 0, \quad \text{c) } 3x^2 + 4x + 5 = 0.$$

Řešení. Postupujeme klasicky. Nejprve spočítáme diskriminant, poté jeho odmocninu (vzpomeneme si na příklad 1.1.3) a následně zjistíme kořeny podle vzorce. Začneme a). Máme

$$D = (-6)^2 - 4 \cdot 58 = -196 = -14^2,$$

tedy kořeny jsou

$$x_{1,2} = \frac{6 \pm 14i}{2} = 3 \pm 7i.$$

V b) vyjde diskriminant

$$D = (-8)^2 - 4 \cdot 9 \cdot 29 = -980 = -4 \cdot 5 \cdot 49$$

a kořeny

$$x_{1,2} = \frac{8 \pm 14i\sqrt{5}}{18} = \frac{4 \pm 7i\sqrt{5}}{9}.$$

Při řešení c) máme diskriminant

$$D = 4^2 - 4 \cdot 3 \cdot 5 = -44 = -4 \cdot 11$$

a kořeny polynomu pak jsou

$$x_{1,2} = \frac{-4 \pm 2i\sqrt{11}}{6} = \frac{-2 \pm i\sqrt{11}}{3}. \quad \triangle$$

Příklad 1.3.2. Dokažte následující tvrzení.

- a) Jestliže polynom $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ s celočíselnými koeficienty, $a_n \neq 0$, má kořen $x_0 \in \mathbb{Z}$, pak x_0 dělí koeficient a_0 .
- b) Jestliže polynom $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ s celočíselnými koeficienty, $a_n \neq 0$, má racionální kořen $x_0 = \frac{r}{s}$, kde r a s jsou nesoudělná celá čísla, pak r dělí koeficient a_0 a s dělí koeficient a_n .

Řešení. K řešení části a) můžeme použít kongruencí. Pro každé $x_1 \in \mathbb{Z}$ je $p(x_1) \equiv a_0 \pmod{x_1}$. Je-li x_0 kořenem polynomu p , pak

$$0 = p(x_0) \equiv a_0 \pmod{x_0},$$

tudíž a_0 musí být dělitelné x_0 .

Nyní vyřešíme část b). Dosadíme kořen $x_0 = \frac{r}{s}$ do polynomu p .

$$a_n \frac{r^n}{s^n} + a_{n-1} \frac{r^{n-1}}{s^{n-1}} + \dots + a_1 \frac{r}{s} + a_0 = 0$$

Vynásobením rovnosti s^n dostaneme následující tvar.

$$\overbrace{a_n r^n + a_{n-1} r^{n-1} s + a_{n-2} r^{n-2} s^2 + \cdots + a_1 r s^{n-1} + a_0 s^n}^{r \cdot q} = 0$$

$s \cdot q'$

Protože rovnost zřejmě implikuje kongruenci modulo libovolné m , platí zřejmě následující kongruence.

$$a_0 s^n \equiv 0 \pmod{r} \qquad a_n r^n \equiv 0 \pmod{s}$$

Jinými slovy $r \mid a_0 s^n$ a $s \mid a_n r^n$. Protože jsou však r a s nesoudělná, musí r dělit a_0 a s dělit a_n . $\triangle$

Příklad 1.3.3. Na základě předchozího cvičení a s pomocí Hornerova schématu najděte kořeny následujících polynomů v množině komplexních čísel:

a) $a(x) = x^3 - x^2 - 7x + 3$, c) $c(x) = 5x^4 + 8x^3 - 14x^2 + 19x - 6$.

b) $b(x) = 2x^4 + 5x^3 + 7x^2 + 10x + 6$,

Řešení. Připomeňme si Hornerovo schéma. Mějme polynom

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0.$$

Můžeme si jej pomocí postupného vytýkání x ze všech členů kromě „absolutního“ napsat také následujícím způsobem.

$$p(x) = \left(\left(\left(\left(a_n \cdot x + a_{n-1} \right) \cdot x + a_{n-2} \right) \cdot x + \cdots + a_2 \right) \cdot x + a_1 \right) \cdot x + a_0$$

Při zjišťování hodnoty p v nějakém bodě x_0 proto stačí vzít a_n , vynásobit x_0 a přičíst a_{n-1} , následně zase vynásobit x_0 a přičíst a_{n-2} , atd. až nakonec přičteme a_0 . Hornerovo schéma vypadá tak, že si do nultého řádku tabulky zapíšeme koeficienty polynomu p , pak do nultého sloupce si zapíšeme x_0 a do řádku tabulky příslušnému danému číslu si zapisujeme mezivýsledky při počítání funkční hodnoty p v bodě x_0 . V posledním sloupci nám vyjde příslušná funkční hodnota. Navíc je-li x_0 kořenem p (tedy vyjde-li 0), jsou příslušné mezivýsledky koeficienty polynomu $\frac{p(x)}{x-x_0}$.

Začneme a). Na základě minulého příkladu 1.3.2 víme, že má-li polynom a racionální kořeny, musí (v základním tvaru) jejich čitatel dělit 3 a jmenovatel 1. Jedinými kandidáty na racionální kořeny jsou tedy ± 1 a ± 3 . Hledejme je tedy pomocí Hornerova schématu,

	1	-1	-7	3
1	1	0	-7	-4
-1	1	-2	-5	8
3	1	2	-1	0

Vidíme, že $x_0 = 3$ je kořenem a navíc

$$a(x) = x^3 - x^2 - 7x + 3 = (x - 3)(x^2 + 2x - 1).$$

Zbývající kořeny najdeme pomocí diskriminantu $D = 4 + 4 = 8$ kvadratického polynomu a máme

$$x_{1,2} = \frac{-2 \pm 2\sqrt{2}}{2} = -1 \pm \sqrt{2}.$$

Přejdeme k b). Všechny koeficienty polynomu b jsou kladné, proto musí být $b((0, \infty)) \subseteq (0, \infty)$, proto jediné reálné kořeny polynomu b mohou být záporné. Navíc má-li b racionální kořeny, musí jejich čitatel dělit 6, jejich jmenovatel 2 a tyto musí být nesoudělné. Hledejme je tedy pomocí Hornorova schématu. Pakliže narazíme na kořen, můžeme dále hledat kořeny s tím, že narazíme-li na kořen, můžeme vzít hodnoty v předešlém řádku za nové koeficienty.

	2	5	7	10	6
-1	2	3	4	6	0
-1	2	1	3	3	
-2	2	-1	6	-6	
-3	2	-3	12	-30	
-6	2	-9	58	-342	
$-\frac{1}{2}$	2	2	3	$\frac{9}{2}$	
$-\frac{3}{2}$	2	0	4	0	

Vidíme, že

$$b(x) = (x + 1) \left(x + \frac{3}{2}\right) (2x^2 + 4) = (x + 1)(2x + 3)(x^2 + 2),$$

přičemž kořeny polynomu $x^2 + 2$ jsou $\pm i\sqrt{2}$ (viz příklad 1.1.3). Celkem tedy máme čtyři kořeny, -1 , $-\frac{3}{2}$ a $\pm i\sqrt{2}$.

Nakonec c). Má-li polynom c racionální kořeny, musí čitatel dělit 6 a jmenovatel 5. Polynom c již má i záporné koeficienty, proto musíme zkusit kladné i záporné kandidáty na kořeny.

	5	8	-14	19	-6
1	5	13	-1	18	12
2	5	18	22	63	120
3	5	23	55	184	546
6	5	38	214	1303	7812
-1	5	3	-17	36	-42
-2	5	-2	-10	39	-84
-3	5	-7	7	-2	0 ⁸
$\frac{1}{5}$	5	-6	$\frac{29}{5}$	$-\frac{21}{25}$	
$-\frac{1}{5}$	5	-8	$\frac{43}{5}$	$-\frac{93}{25}$	
$\frac{2}{5}$	5	-5	5	0	

Máme rozklad

$$c(x) = (x+3) \left(x - \frac{2}{5}\right) (5x^2 - 5x + 5) = (x+3) (5x-2) (x^2 - x + 1)$$

a poslední dva kořeny najdeme klasicky, tedy $D = 1 + 4 = 5$

$$x_{3,4} = \frac{1 \pm \sqrt{5}}{2}.$$

Celkem máme kořeny -3 , $\frac{2}{5}$ a $\frac{1 \pm \sqrt{5}}{2}$.

△

Příklad 1.3.4. V $\mathbb{Z}_5$ a v $\mathbb{Z}_6$ najděte všechny kořeny polynomů

a) $x^2 + 2x + 3$,

b) $x^3 - x^2 + 3x + 2$.

Řešení. Protože se pohybujeme v konečných okruzích, můžeme vyzkoušet všechny možnosti, kterých je 5, resp. 6. Můžeme opět použít Hornerovo schéma, přičemž nás zajímají pouze zbytky po dělení 5, resp. 6. Začneme a).

$\mathbb{Z}_5$	1	2	3
0	1	2	3
1	1	3	1
2	1	4	1
3	1	0	3
4	1	1	2

$\mathbb{Z}_6$	1	2	3
0	1	2	3
1	1	3	0
2	1	4	5
3	1	5	0
4	1	0	3
5	1	1	2

Vidíme, že v $\mathbb{Z}_5$ nemá polynom $x^2 + 2x + 3$ kořeny, zatímco v $\mathbb{Z}_6$ má kořeny 1 a 3. Tedy kongruence

$$x^2 + 2x + 3 \equiv 0 \pmod{5}$$

nemá řešení, zatímco kongruenci

$$x^2 + 2x + 3 \equiv 0 \pmod{6}$$

řeší jakékoli celé číslo dávající po dělení 6 zbytek 1 nebo 3.

Přejdeme k b). Využijeme záporných zbytků. Reprezentanty tříd kongruence tedy budou v $\mathbb{Z}_5$: 0, ± 1 a ± 2 ; v $\mathbb{Z}_6$ pak 0, ± 1 , ± 2 a 3.

$\mathbb{Z}_5$	1	-1	-2	2
0	1	-1	-2	2
1	1	0	-2	0
2	1	1	0	2
-2	1	2	-1	-1
-1	1	-2	0	2

$\mathbb{Z}_6$	1	-1	3	2
0	1	-1	3	2
1	1	0	3	-1
2	1	1	-1	0
3	1	2	3	-1
-2	1	3	3	2
-1	1	-2	-1	3

⁸Protože je -3 kořenem, máme ve schématu koeficienty podílu. Nový odhad na racionální kořeny tedy říká, že číselník musí dělit -2 a jmenovatel 5. Proto nemusíme znovu zkoušet -3 ani -6 .

Nad $\mathbb{Z}_5$ tedy máme jediný kořen 1 a nad $\mathbb{Z}_6$ máme kořen 2. Opět lze říci, že kongruenci

$$x^3 - x^2 + 3x + 2 \equiv 0 \pmod{5}$$

řeší kterékoli čísla tvaru $5k + 3$, $k \in \mathbb{Z}$, kongruenci

$$x^3 - x^2 + 3x + 2 \equiv 0 \pmod{6}$$

řeší všechna celá čísla kongruentní 2 modulo 6. △

1.4 Soustavy lineárních rovnic

Příklad 1.4.1. Řešte následující soustavu rovnic s neznámými v $\mathbb{R}$.

$$\begin{array}{rrrrrrrcl} x_1 & + & 2x_2 & + & x_3 & + & 3x_4 & + & 2x_5 & = & -8 \\ 2x_1 & + & x_2 & + & x_3 & + & x_4 & + & 3x_5 & = & 1 \\ x_1 & & & & + & x_3 & - & x_4 & + & 2x_5 & = & 0 \\ x_1 & + & 2x_2 & + & 2x_3 & + & 2x_4 & + & 3x_5 & = & 0 \end{array}$$

Řešte stejnou soustavu v $\mathbb{Z}_{13}$, zbytkových třídách modulo 13.

Řešení. Můžeme si soustavu napsat do matice, kde prvky matice jsou koeficienty před proměnnými. Používáme *elementárních řádkových úprav*, tj. „prohození dvou řádků matice“, „vynásobení jednoho z řádků nenulovým⁹ číslem“ a „přičtení násobku jednoho řádku k jinému“. Vybereme (pomocí prohazování řádků) vedoucí koeficient – tj. prvek takový, aby ve všech sloupcích nalevo od něj a zároveň ve všech řádcích pod ním byly nuly. Následně se pomocí tohoto prvku a elementárních řádkových úprav snažíme vynulovat všechny prvky ve sloupci pod vedoucím koeficientem. Poté postup opakujeme – určíme nový vedoucí koeficient atd. Tomuto postupu říkáme *Gaußova eliminace*. Takto matici upravíme do *schodovitého tvaru* – kdy před a pod vedoucími koeficienty jsou nuly. Ve sloupcích napravo od vedoucího koeficientu musí být pod daným řádkem buď nuly, nebo nový vedoucí koeficient.

Ze schodovitého tvaru již umíme vyjádřit řešení – dosadíme za *volné proměnné* (tedy ty, v k nimž příslušných sloupcích se nenachází vedoucí koeficient v žádném řádku) parametry, následně postupně od nejnižšího řádku nahoru vyjadřujeme *vázané proměnné* (tj. příslušné danému vedoucímu koeficientu) pomocí volných a již dříve vyjádřených vázaných proměnných.

Druhou možností řešení je upravit matici pomocí *zětné Gaußovy eliminace* do *redukováného schodovitého tvaru*, tedy do tvaru kde ve sloupcích s vedoucími koeficienty je daný vedoucí koeficient jediným nenulovým prvkem. V tomto tvaru již můžeme rovnou vyjadřovat vázané proměnné pouze pomocí volných, a tudíž v libovolném pořadí.

⁹obecněji invertibilním

Nejprve prohodíme první a třetí řádek.

$$\left(\begin{array}{ccccc|c} 1 & 2 & 1 & 3 & 2 & -8 \\ 2 & 1 & 1 & 1 & 3 & 1 \\ 1 & 0 & 1 & -1 & 2 & 0 \\ 1 & 2 & 2 & 2 & 3 & 0 \end{array} \right) \sim \left(\begin{array}{ccccc|c} 1 & 0 & 1 & -1 & 2 & 0 \\ 1 & 2 & 1 & 3 & 2 & -8 \\ 2 & 1 & 1 & 1 & 3 & 1 \\ 1 & 2 & 2 & 2 & 3 & 0 \end{array} \right)$$

Následně pomocí nového prvního řádku vynulujeme ostatní čísla v prvním sloupci.

$$\sim \left(\begin{array}{ccccc|c} 1 & 0 & 1 & -1 & 2 & 0 \\ 0 & 2 & 0 & 4 & 0 & -8 \\ 0 & 1 & -1 & 3 & -1 & 1 \\ 0 & 2 & 1 & 3 & 1 & 0 \end{array} \right)$$

Druhý řádek si vydělíme dvěma, přičemž výsledek bude opět celočíselný.

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

Následně použijeme druhý řádek k vynulování prvků ve druhém sloupci pod vedoucím koeficientem.

$$\sim \left(\begin{array}{ccccc|c} 1 & 0 & 1 & -1 & 2 & 0 \\ 0 & 1 & 0 & 2 & 0 & -4 \\ 0 & 0 & -1 & 1 & -1 & 5 \\ 0 & 0 & 1 & -1 & 1 & 8 \end{array} \right)$$

Sečtením posledních dvou řádků dospějeme k následující soustavě.

$$\sim \left(\begin{array}{ccccc|c} 1 & 0 & 1 & -1 & 2 & 0 \\ 0 & 1 & 0 & 2 & 0 & -4 \\ 0 & 0 & 1 & -1 & 1 & -5 \\ 0 & 0 & 0 & 0 & 0 & 13 \end{array} \right)$$

Odtud vidíme, že soustava nemá nad $\mathbb{R}$ řešení. Ovšem $13 \equiv 0 \pmod{13}$, tedy nad $\mathbb{Z}_{13}$ můžeme pokračovat. (Soustavu bychom od začátku řešili stejně – vždy jsme přičítali násobek řádku k jinému a jediný případ, kdy jsme dělili, vyšel celočíselný.) Nad $\mathbb{Z}_{13}$ máme tedy následující soustavu.

$$\left(\begin{array}{ccccc|c} 1 & 2 & 1 & 3 & 2 & -8 \\ 2 & 1 & 1 & 1 & 3 & 1 \\ 1 & 0 & 1 & -1 & 2 & 0 \\ 1 & 2 & 2 & 2 & 3 & 0 \end{array} \right) \sim \left(\begin{array}{ccccc|c} 1 & 0 & 1 & -1 & 2 & 0 \\ 0 & 1 & 0 & 2 & 0 & -4 \\ 0 & 0 & 1 & -1 & 1 & -5 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

Pro zpětnou Gaußovu eliminaci pouze odečteme od prvního řádku třetí.

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

Máme tedy volné proměnné $x_4 = t$ a $x_5 = s$, následně $x_3 = -5 + t - s$, $x_2 = -4 - 2t$ a $x_1 = 5 - s$, kde $t, s \in \mathbb{Z}_{13}$ a výrazy chápeme nad $\mathbb{Z}_{13}$ – zajímá nás zbytek po dělení 13. $\triangle$

Příklad 1.4.2. Řešte následující soustavu rovnic.

$$\begin{array}{rrrrrrrcl} x_1 & + & 2x_2 & + & x_3 & - & x_4 & + & x_5 & = & 0 \\ 2x_1 & + & x_2 & + & 2x_3 & - & 2x_4 & + & 2x_5 & = & 0 \\ 2x_1 & & & + & x_3 & - & x_4 & + & 2x_5 & = & -1 \\ x_1 & + & x_2 & + & 2x_3 & - & 2x_4 & + & x_5 & = & 1 \end{array}$$

Řešení. Postupujeme stejně jako v příkladu 1.4.1 – nejprve Gaußovou a poté zpětnou Gaußovou eliminací. (Samozřejmě by stačila pouze „dopředná“ eliminace, ale pak bychom museli dopočítávat vázané proměnné) Opět použijeme maticový zápis. Nejprve pomocí prvního řádku vynulujeme ostatní prvky v prvním sloupci.

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

Následně vidíme, že $x_2 = 0$. Vedoucí koeficient druhého řádku můžeme vydělit -3 , poté s jeho pomocí vynulujeme ostatní prvky ve druhém sloupci. Protože jsou ostatní prvky druhého řádku nulové, můžeme rovnou nulovat i prvky nad vedoucím koeficientem.

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

Nyní jen sečteme poslední dva řádky.

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

Nakonec odečteme třetí řádek od prvního.

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

Máme tedy volné proměnné $x_4 = t$ a $x_5 = s$, vázané proměnné jsou $x_1 = -1 - s$, $x_2 = 0$ a $x_3 = 1 + t$, t a $s \in \mathbb{R}$ jsou parametry.¹⁰ Ve vektorovém tvaru má tedy řešení tvar

$$X = [-1, 0, 1, 0, 0] + t \cdot (0, 0, 1, 1, 0) + s \cdot (-1, 0, 0, 0, 1),$$

kde hranaté závorky označují bod a kulaté vektory. $\triangle$

Příklad 1.4.3. Řešte následující soustavu rovnic, nejprve nad $\mathbb{R}$, poté nad $\mathbb{Z}_7$.

$$\begin{array}{rrrrrrcl} 2x_1 & - & x_2 & + & x_3 & - & x_4 & = & 1 \\ 2x_1 & - & x_2 & & & - & 3x_4 & = & 2 \\ 3x_1 & & & - & x_3 & + & x_4 & = & -3 \\ 2x_1 & + & 2x_2 & - & 2x_3 & + & 5x_4 & = & -6 \end{array}$$

Řešení. Využijeme maticový zápis a budeme postupova Gaußovou eliminací s výběrem pivotu. Nejprve si za pivotu zvolíme prvek ve druhém řádku a druhém sloupci. Následně pomocí něj vynulujeme ostatní prvky ve druhém sloupci (nad ním i pod ním). Také se budeme snažit so nejdéle udržet čísla v matici celá.

$$\left(\begin{array}{cccc|c} 2 & -1 & 1 & -1 & 1 \\ 2 & -1 & 0 & -3 & 2 \\ 3 & 0 & -1 & 1 & -3 \\ 2 & 2 & -2 & 5 & -6 \end{array} \right) \sim \left(\begin{array}{cccc|c} 0 & 0 & 1 & 2 & -1 \\ 2 & -1 & 0 & -3 & 2 \\ 3 & 0 & -1 & 1 & -3 \\ 6 & 0 & -2 & -1 & -2 \end{array} \right)$$

Druhý řádek si vynásobíme -1 . Novým pivotem bude prvek v prvním řádku a třetím sloupci. Pomocí prvního řádku tedy vynulujeme ostatní prvky ve třetím sloupci.

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

Nyní odečteme od čtvrtého řádku třetí.

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

Čtvrtý řádek můžeme vydělit 3 a prvky budou stále celočíselné. Vidíme, že $x_1 = 0$. Následně bude pivotem prvek ve čtvrtém řádku a prvním sloupci, pomocí nějž vynulujeme zbytek prvního sloupce.

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

¹⁰Hledali-li bychom řešení nad jiným tělesem (okruhem), zvolili bychom příslušné parametry. Například pro racionální řešení bychom se omezili na $t, s \in \mathbb{Q}$.

Posledním pivotem bude prvek ve třetím řádku a čtvrtém sloupci. Nejprve odečteme od druhého řádku třetí, následně od trojnásobku prvního řádku dvojnásobek třetího.

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

Máme tedy nad $\mathbb{R}$ řešení $x_3 = \frac{5}{3}$, $x_2 = 2$, $x_4 = -\frac{4}{3}$ a $x_1 = 0$. Jak je to s řešením nad $\mathbb{Z}_7$? Musíme dělit třemi, chceme tedy najít modulární inverzi k 3 modulo 7. Vidíme, že $3 \cdot 5 = 15 \equiv 1 \pmod{7}$, tedy dělení 3 je v $\mathbb{Z}_7$ totéž co násobení 5. Nad $\mathbb{Z}_7$ máme řešení $x_1 \equiv 0$, $x_2 \equiv 2$, $x_3 \equiv 5 \cdot 5 = 25 \equiv 2$ a $x_4 \equiv -4 \cdot 5 = -20 \equiv 1 \pmod{7}$. $\triangle$

Příklad 1.4.4. Řešte soustavu rovnic pro neznámé x , y , z v závislosti na hodnotách parametru $a \in \mathbb{R}$:

$$\begin{aligned} x + y + az &= 1 \\ x + ay + z &= a \\ ax + y + z &= a^2 \end{aligned} \tag{1.8}$$

Řešení. Postupujeme klasicky s využitím maticového zápisu do chvíle, než musíme dělit výrazem s a . Nejprve pomocí prvního řádku vynulujeme ostatní složky v prvním sloupci.

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

Následně ke třetímu řádku přičteme druhý s využitím $1 - a^2 + (1 - a) = (1 + a)(1 - a) + (1 - a) = (2 + a)(1 - a)$.

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

Nyní máme tři možnosti. Pro $a \in \mathbb{R} \setminus \{-2, 1\}$ můžeme poslední řádek vydělit výrazem $(2 + a)(1 - a)$, přičemž $1 - a$ se zkrátí, a druhý řádek výrazem $a - 1$.

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

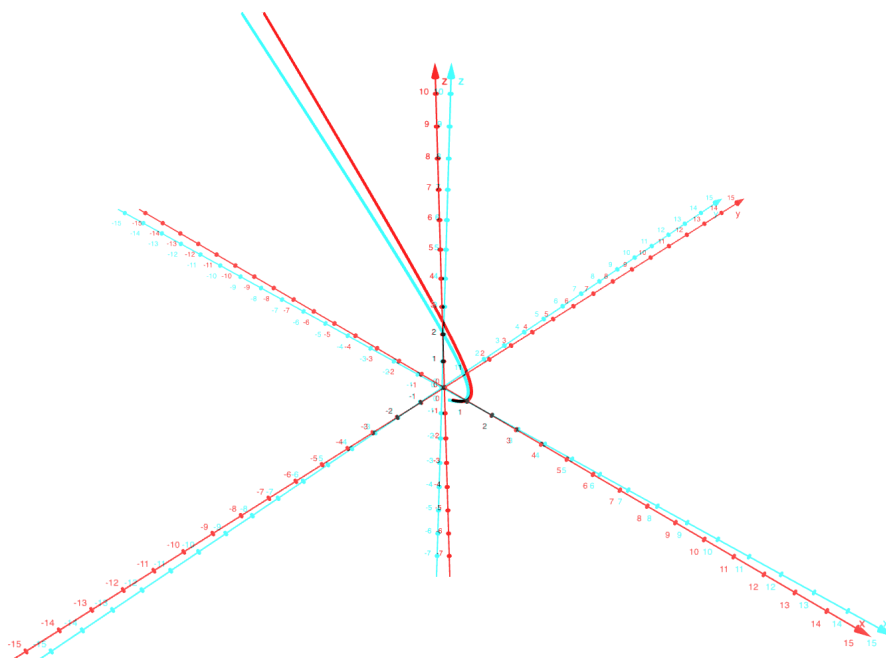
Následně zredukujeme třetí sloupec pomocí třetího řádku.

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

Nakonec zredukujeme druhý sloupec podle druhého řádku.

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

Máme tedy řešení $x = \frac{1-a^2}{2+a}$, $y = \frac{1}{2+a}$ a $z = -\frac{1+a}{2+a}$. Pro $a \in (-2, 1)$ máme *křivku* řešení pro různé parametry a , jejíž anaglyf je znázorněn na obrázku 1.2.



Obrázek 1.2: Křivka jednoznačných řešení soustavy (1.8) pro $a \in (-2, 1)$.

Pro $a = 1$ dostaneme tři shodné rovnice tvaru

$$x + y + z = 1$$

řešené trojicemi tvaru $x = 1 - t - s$, $y = t$, $z = s$, $t, s \in \mathbb{R}$. Pro $a = -2$ dostaneme po úpravě soustavu s maticí

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

která nemá řešení.

△

Příklad 1.4.5. Najděte všechny dvojice parametrů $a, b \in \mathbb{R}$, pro které je množina řešení soustavy rovnic

$$\begin{array}{rcrcrcrcrcl} x & + & y & + & az & = & 1 \\ x & + & ay & + & 2z & = & 1 \\ ax & + & y & & & = & b \end{array}$$

o neznámých $x, y, z \in \mathbb{R}$

a) prázdná,

b) nekonečná.

V druhém případě soustavu vyřešte.

Řešení. Opět využijeme maticový tvar a stejně jako v příkladu 1.4.4 budeme postupovat Gaußovou eliminací dokud nebudeme muset dělit výrazem s a nebo b . Pomocí prvního řádku zredukujeme první sloupec.

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

Následně ke třetímu řádku přičteme druhý.

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

S využitím rozkladu $2-a-a^2 = (2+a)(1-a)$ (viz příklad 1.4.4) vidíme, že

- pokud $a \in \{-2, 1\}$ a $b \neq a$, soustava nemá řešení;
- pokud $a \notin \{-2, 1\}$, má soustava jediné řešení;
- pokud $a \in \{-2, 1\}$ a $b = a$, má soustava nekonečně mnoho řešení.

V posledním případě máme pro $a = b = 1$ následující soustavu, zadanou pomocí matice. Pomocí druhého řádku zredukujeme třetí sloupec.

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

Máme $z = 0$, $y = t$ a $x = 1 - t$, $t \in \mathbb{R}$. Pro $a = b = -2$ máme soustavu s následující maticí.

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

Máme řešení $z = 3t$, pak $y = 4t$ a $x = 1 - 2t$, $t \in \mathbb{R}$.

△

1.5 Maticový počet

Příklad 1.5.1. Uvažujme následující matice.

$$A = \begin{pmatrix} 3 & 5 & 6 & 7 \\ -2 & 1 & 0 & 5 \end{pmatrix} \quad B = \begin{pmatrix} 2 & 8 \\ -1 & -5 \\ 9 & 11 \end{pmatrix}$$

$$C = \begin{pmatrix} 2 & 8 & 3 & 21 & 5 \end{pmatrix} \quad D = \begin{pmatrix} 2 \\ -1 \\ 9 \\ -6 \\ 3 \end{pmatrix}$$

Zjistěte, jestli existují součiny $A \cdot B$, $B \cdot A$, $C \cdot D$ a $D \cdot C$. Pokud ano, určete je.

Řešení. Existuje pouze součin matic tvaru $m \times n$ a $n \times p$, přičemž výsledkem bude matice tvaru $m \times p$. Protože A je tvaru 2×4 a B tvaru 3×2 , součin $A \cdot B$ neexistuje. Součin $B \times A$ existuje.

$$B \cdot A = \begin{pmatrix} 2 & 8 \\ -1 & -5 \\ 9 & 11 \end{pmatrix} \cdot \begin{pmatrix} 3 & 5 & 6 & 7 \\ -2 & 1 & 0 & 5 \end{pmatrix} = \begin{pmatrix} -10 & 2 & 12 & -26 \\ 7 & -10 & -6 & -32 \\ 5 & 56 & 54 & 118 \end{pmatrix}$$

Protože C je tvaru 1×5 a D je tvaru 5×1 , existují oba součiny.

$$C \cdot D = \begin{pmatrix} 2 & 8 & 3 & 21 & 5 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ -1 \\ 9 \\ -6 \\ 3 \end{pmatrix} = (-88)$$

$$D \cdot C = \begin{pmatrix} 2 \\ -1 \\ 9 \\ -6 \\ 3 \end{pmatrix} \cdot \begin{pmatrix} 2 & 8 & 3 & 21 & 5 \end{pmatrix} = \begin{pmatrix} 4 & 16 & 6 & 42 & 10 \\ -2 & -8 & -3 & -21 & -5 \\ 18 & 72 & 27 & 189 & 45 \\ -12 & -48 & -18 & -126 & -30 \\ 6 & 24 & 9 & 63 & 15 \end{pmatrix} \quad \triangle$$

Příklad 1.5.2. Ukažte, že soustavu k lineárních rovnic o neznámých $x_1, x_2, \dots, x_n$ s koeficienty $a_{i,j}$ a pravou stranou b_j lze zapsat pomocí maticového násobení takto

$$A \cdot x = b,$$

kde $A = (a_{i,j})$ je matice tvaru $k \times n$, $x = (x_j)$ je sloupec velikosti n a $b = (b_i)$ je sloupec velikosti k .

Řešení. Máme následující soustavu rovnic.

$$\begin{aligned} a_{1,1} x_1 + a_{1,2} x_2 + \cdots + a_{1,n} x_n &= b_1 \\ a_{2,1} x_1 + a_{2,2} x_2 + \cdots + a_{2,n} x_n &= b_2 \\ &\vdots \\ a_{k,1} x_1 + a_{k,2} x_2 + \cdots + a_{k,n} x_n &= b_k \end{aligned}$$

Podívejme se na i -tou rovnici. Levá strana je

$$a_{i,1} x_1 + a_{i,2} x_2 + \cdots + a_{i,n} x_n,$$

což je ale přesně součin i -tého řádku matice A se sloupcem x . Pravá strana je b_i , tedy i -tá složka sloupce b . Je zřejmé, že porovnáním všech složek dostaneme požadovaný tvar $Ax = b$. $\triangle$

Příklad 1.5.3. Matice A a B tvaru $n \times n$ jsou dány předpisem:

$$a_{ij} = \begin{cases} 1, & i \geq j, \\ 2, & i < j, \end{cases} \quad b_{ij} = \begin{cases} 1, & i \leq j, \\ 3, & i > j. \end{cases}$$

Napište je a vypočtěte, čemu se rovná jejich součin.

Řešení. A je matice, kde čistě nad hlavní diagonálou jsou 2, jinak 1. B má čistě pod hlavní diagonálou 3, jinak 1.

$$A = \begin{pmatrix} 1 & 2 & 2 & \cdots & 2 \\ 1 & 1 & 2 & \cdots & 2 \\ \vdots & & \ddots & & \vdots \\ 1 & 1 & 1 & \cdots & 2 \\ 1 & 1 & 1 & \cdots & 1 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ 3 & 1 & \cdots & 1 & 1 \\ \vdots & & \ddots & & \vdots \\ 3 & 3 & \cdots & 1 & 1 \\ 3 & 3 & \cdots & 3 & 1 \end{pmatrix}$$

Počítejme součin $A \cdot B =: C$. Máme vzorec

$$c_{ik} = \sum_{j=1}^n a_{ij} b_{jk}.$$

Ze zadání si přepíšeme podmínku na b_{jk} .

$$b_{jk} = \begin{cases} 1, & j \leq k \\ 3, & j > k \end{cases}$$

Máme tři případy.

- $i < k$

$$\sum_{j=1}^i 1 \cdot 1 + \sum_{j=i+1}^k 2 \cdot 1 + \sum_{j=k+1}^n 2 \cdot 3 = i + 2(k-i) + 6(n-k) = 6n - 4k - i$$

- $i = k$

$$\sum_{j=1}^i 1 \cdot 1 + \sum_{j=i+1}^n 2 \cdot 3 = i + 6(n-i) = 6n - 5i$$

- $i > k$

$$\sum_{j=1}^k 1 \cdot 1 + \sum_{j=k+1}^i 3 \cdot 1 + \sum_{j=i+1}^n 2 \cdot 3 = k + 3(i-k) + 6(n-i) = 6n - 3i - 2k$$

Vidíme, že případ, kdy $i = k$ odpovídá oběma případům s ostrou nerovností nahrazenou neostrou. Máme tedy vzorec pro součin $A \cdot B$.

$$c_{ij} = \begin{cases} 6n - 4j - i & i \leq j \\ 6n - 3i - 2j & i \geq j \end{cases}$$

Počítejme nyní $B \cdot A =: D = (d_{ik})$. Dosadíme do vzorce pro součin

$$d_{ik} = \sum_{j=1}^n b_{ij} a_{jk}$$

za b_{ij} a a_{jk} , přičemž si podmínku pro a_{jk} zapíšeme pomocí j a k .

$$a_{jk} = \begin{cases} 1, & j \geq k, \\ 2, & j < k, \end{cases}$$

Opět si výpočet rozdělíme na tři případy.

- $i < k$

$$\sum_{j=1}^{i-1} 3 \cdot 2 + \sum_{i=j}^{k-1} 1 \cdot 2 + \sum_{j=k}^n 1 \cdot 1 = 6(i-1) + 2(k-i) + (n-k+1) = 4i + k + n - 5$$

- $i = k$

$$\sum_{j=1}^{i-1} 2 \cdot 3 + \sum_{j=i}^n 1 \cdot 1 = 6(i-1) + (n-i+1) = 5i + n - 5$$

- $i > k$

$$\sum_{j=1}^{k-1} 2 \cdot 3 + \sum_{j=k}^{i-1} 3 \cdot 1 + \sum_{j=i}^n 1 \cdot 1 = 6(k-1) + 3(i-k) + (n-i+1) = 3k + 2i + n - 5$$

Stejně jako minule je případ, kdy $i = k$ zahrnut v ostatních vzorcích, uvažujeme-li je s neostrou nerovností. Máme tedy i vzorec pro prvky součinu $B \cdot A$.

$$d_{ij} = \begin{cases} n + 4i + j - 5 & i \leq j \\ n + 3j + 2i - 5 & i \geq j \end{cases} \quad \triangle$$

Příklad 1.5.4. Uvažujme orientovaný graf s uzly $1, 2, \dots, n$. Tomuto grafu můžeme přiřadit čtvercovou matici $A = (a_{i,j})$ tak, že $a_{i,j} = 1$ jestliže v grafu existuje orientovaná hrana z i do j , jinak je $a_{i,j} = 0$. Jaký význam mají mocniny matice A , to je maticové součiny

$$A^2 = A \cdot A,$$

$$A^3 = A \cdot A \cdot A?$$

Řešení. Uvažme matici $A^2 = (b_{i,j})$. Máme dle definice maticového násobení

$$b_{i,j} = \sum_{k=1}^n a_{i,k} a_{k,j}$$

přičemž součiny napravo jsou vždy 0 nebo 1 a budou 1 jen pro k , pro kteráž existuje orientovaná hrana z i do k a z k do j . Suma takovýchto jedniček pak dá počet takovýchto k , tedy počet cest délky právě 2 z i do j . Pro matici $A^3 = (c_{i,j})$ máme podobně

$$c_{i,j} = \sum_{k,\ell} a_{i,k} a_{k,\ell} a_{\ell,j}$$

kde na pravé straně máme opět buď 0 nebo 1 a 1 jen pro ty dvojice k, ℓ , kde existuje orientovaná cesta

$$i \longrightarrow k \longrightarrow \ell \longrightarrow j$$

a součet nám opět dá počet takovýchto dvojic. Pak $c_{i,j}$ zadává počet cest délky právě 3 z i do j . Obecně A^k zadává počet cest délky právě k mezi danými vrcholy. $\triangle$

Příklad 1.5.5. Uvažujme matici

$$A = \begin{pmatrix} 3 & 5 & 6 & 7 \\ -2 & 1 & 0 & 5 \\ 1 & 3 & -2 & 1 \end{pmatrix}$$

a označme písmenem e postupně tyto elementární řádkové operace

- a) vynásobení druhého řádku číslem 3,
- b) výměna prvního a třetího řádku,
- c) přičtení dvojnásobku prvního řádku ke třetímu.

Nechť E je jednotková matice 3×3 . Označme $e(A)$ a $e(E)$ matice, které vzniknou aplikací elementární řádkové operace e na matici A a E . Ukažte, že platí

$$e(E) \cdot A = e(A).$$

Řešení. Začneme a). Napišme si, jak vypadá matice $e(E) \cdot A$ a počítejme. Vidíme, že na konci vyjde $e(A)$.

$$e(E) \cdot A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 & 5 & 6 & 7 \\ -2 & 1 & 0 & 5 \\ 1 & 3 & -2 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 5 & 6 & 7 \\ -6 & 3 & 0 & 15 \\ 1 & 3 & -2 & 1 \end{pmatrix} = e(A)$$

Obdobně vyřešíme b).

$$e(E) \cdot A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 3 & 5 & 6 & 7 \\ -2 & 1 & 0 & 5 \\ 1 & 3 & -2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & -2 & 1 \\ -2 & 1 & 0 & 5 \\ 3 & 5 & 6 & 7 \end{pmatrix} = e(A)$$

Nakonec c).

$$e(E) \cdot A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 & 5 & 6 & 7 \\ -2 & 1 & 0 & 5 \\ 1 & 3 & -2 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 5 & 6 & 7 \\ -2 & 1 & 0 & 5 \\ 7 & 13 & 10 & 15 \end{pmatrix} = e(A) \quad \triangle$$

Příklad 1.5.6. Spočítejte inverzní matici k matici

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

Proveďte zkoušku.

Řešení. Provádíme elementární řádkové úpravy v rozšířené matici. Nejprve pomocí prvního řádku zredukujeme první sloupec.

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

Následně vynásobíme poslední řádek -1 a poslední dva řádky prohodíme.

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

Ke třetímu řádku přičteme dvojnásobek druhého.

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

K prvním dvěma řádkům přičteme dvojnásobek posledního, který následně vynásobíme -1 .

$$\sim \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 7 & 2 & -4 \\ 0 & 1 & 0 & 8 & 2 & -5 \\ 0 & 0 & 1 & -3 & -1 & 2 \end{array} \right)$$

Nakonec od prvního řádku odečteme druhý.

$$\sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -1 & 0 & 1 \\ 0 & 1 & 0 & 8 & 2 & -5 \\ 0 & 0 & 1 & -3 & -1 & 2 \end{array} \right)$$

Zkoušku provedeme pomocí maticového násobení.

$$\begin{aligned} \begin{pmatrix} 1 & 1 & 2 \\ 1 & -1 & -3 \\ 2 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 & 1 \\ 8 & 2 & -5 \\ -3 & -1 & 2 \end{pmatrix} &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ \begin{pmatrix} -1 & 0 & 1 \\ 8 & 2 & -5 \\ -3 & -1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 2 \\ 1 & -1 & -3 \\ 2 & 1 & 2 \end{pmatrix} &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{aligned} \quad \triangle$$

Příklad 1.5.7. Spočítejte inverzní matici k matici

$$\begin{pmatrix} 1 & 4 & -2 & 3 \\ 2 & 9 & 3 & -2 \\ -1 & -6 & -11 & 4 \\ 0 & -1 & -6 & 0 \end{pmatrix}.$$

Zkoušku proveďte aspoň částečně.

Řešení. Opět upravujeme rozšířenou matici pomocí elementárních řádkových úprav. Nejprve pomocí prvního řádku zredukujeme první sloupec.

$$\left(\begin{array}{cccc|cccc} 1 & 4 & -2 & 3 & 1 & 0 & 0 & 0 \\ 2 & 9 & 3 & -2 & 0 & 1 & 0 & 0 \\ -1 & -6 & -11 & 4 & 0 & 0 & 1 & 0 \\ 0 & -1 & -6 & 0 & 0 & 0 & 0 & 1 \end{array} \right) \sim \left(\begin{array}{cccc|cccc} 1 & 4 & -2 & 3 & 1 & 0 & 0 & 0 \\ 0 & 1 & 7 & -8 & -2 & 1 & 0 & 0 \\ 0 & -2 & -13 & 7 & 1 & 0 & 1 & 0 \\ 0 & -1 & -6 & 0 & 0 & 0 & 0 & 1 \end{array} \right)$$

Následně pomocí druhého řádku zredukujeme druhý sloupec. Odečteme jeho čtyřnásobek od prvního řádku, jeho dvojnásobek přičteme k řádku třetímu a nakonec jej přičteme ke čtvrtému řádku.

$$\sim \left(\begin{array}{cccc|cccc} 1 & 0 & -30 & 35 & 9 & -4 & 0 & 0 \\ 0 & 1 & 7 & -8 & -2 & 1 & 0 & 0 \\ 0 & 0 & 1 & -9 & -3 & 2 & 1 & 0 \\ 0 & 0 & 1 & -8 & -2 & 1 & 0 & 1 \end{array} \right)$$

Nyní pomocí třetího řádku zredukujeme třetí sloupec. Odečteme jej od čtvrtého řádku, od druhého jeho sedminásobek a k prvnímu přičteme jeho třicetinásobek.

$$\sim \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & -235 & -81 & 56 & 30 & 0 \\ 0 & 1 & 0 & 55 & 19 & -13 & -7 & 0 \\ 0 & 0 & 1 & -9 & -3 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & -1 & -1 & 1 \end{array} \right)$$

Zbývá zredukovat poslední sloupec pomocí posledního řádku. Ke třetímu přičteme jeho devítinásobek, k prvnímu zase jeho dvě stě pětaticetinásobek a od druhého odečteme jeho pětapadesátinásobek.

$$\sim \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 154 & -179 & -205 & 235 \\ 0 & 1 & 0 & 0 & -36 & 42 & 48 & -55 \\ 0 & 0 & 1 & 0 & 6 & -7 & -8 & 9 \\ 0 & 0 & 0 & 1 & 1 & -1 & -1 & 1 \end{array} \right)$$

Zkoušku provedeme pomocí maticového násobení.

$$\begin{pmatrix} 154 & -179 & -205 & 235 \\ -36 & 42 & 48 & -55 \\ 6 & -7 & -8 & 9 \\ 1 & -1 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 4 & -2 & 3 \\ 2 & 9 & 3 & -2 \\ -1 & -6 & -11 & 4 \\ 0 & -1 & -6 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Při počítání inverzní matice jsme používali pouze úpravu „přičtení násobku jednoho řádku k jinému“, která nemění determinant. Můžeme tedy říci, že determinant naší matice je 1 a že má inverzi, přičemž díky výše spočítanému to musí být právě naše matice.¹¹ $\triangle$

Příklad 1.5.8. Spočítejte inverzní matici k matici

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

Proveďte zkoušku.

Řešení. Opět postupujeme pomocí řádkových úprav rozšířené matice. Od čtvrtého řádku odečteme a -násobek pátého. Následně od třetího odečteme a -násobek nového čtvrtého, atd., načež dostaneme inverzi.

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

¹¹Má-li matice inverzi a levou inverzi (což jsme spočítali), pak nutně se musejí tyto rovnat, tedy levá inverze je i pravou inverzí.

Zkoušku provedeme pomocí násobení matic. Při násobení inverze původní maticí zleva vlastně ve druhé matici přičítáme a -násobek následujícího řádku k předchozímu, čímž máme hned výsledek.

$$\begin{pmatrix} 1 & a & 0 & 0 & 0 \\ 0 & 1 & a & 0 & 0 \\ 0 & 0 & 1 & a & 0 \\ 0 & 0 & 0 & 1 & a \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -a & a^2 & -a^3 & a^4 \\ 0 & 1 & -a & a^2 & -a^3 \\ 0 & 0 & 1 & -a & a^2 \\ 0 & 0 & 0 & 1 & -a \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Obdobně bychom provedli i opačný součin – k následujícímu sloupci bychom přičítali a -násobek předchozího. $\triangle$

1.6 Vektorové prostory a podprostory

Příklad 1.6.1. Ukažte si, že následující množiny jsou s vhodnými operacemi vektorové prostory.

- a) množina n -tic reálných čísel $\mathbb{R}^n$,
- b) množina všech polynomů s koeficienty v $\mathbb{R}$, označení $\mathbb{R}[x]$,
- c) množina všech matic 3×3 s prvky v $\mathbb{Z}_5$, označení $\text{Mat}_{3 \times 3}(\mathbb{Z}_5)$,
- d) množina všech posloupností reálných čísel, kterou lze chápat jako množinu všech zobrazení množiny přirozených čísel $\mathbb{N}$ do $\mathbb{R}$.

Řešení. Začněme a). Jednotlivé n -tice zapisujeme

$$\mathbf{x} = (x_1, x_2, \dots, x_n) \text{ nebo } \mathbf{x} = (x_i)_{i=1}^n.$$

Definujeme sčítání po složkách, tedy

$$\mathbf{x} + \mathbf{y} := (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n) = (x_i + y_i)_{i=1}^n.$$

Násobení skalárem definujeme rovněž po složkách,

$$a \cdot \mathbf{x} = (a x_1, a x_2, \dots, a x_n) = (a x_i)_{i=1}^n.$$

Ověříme axiomy vektorového prostoru. Sčítání vektorů je *asociativní* a *komutativní* díky tomu, že je definováno po složkách a díky vlastnostem $\mathbb{R}$. Neutrálním prvkem bude vektor

$$\mathbf{o} = (\underbrace{0, 0, \dots, 0}_n) = (0)_{i=1}^n.$$

Pak totiž

$$\mathbf{x} + \mathbf{o} = (x_i + 0)_{i=1}^n = (x_i)_{i=1}^n = \mathbf{x}.$$

Opačným prvkem k $\mathbf{x} = (x_i)_{i=1}^n$ bude $-\mathbf{x} = (-x_i)_{i=1}^n$, protože pak

$$\mathbf{x} + (-\mathbf{x}) = (x_i - x_i)_{i=1}^n = (0)_{i=1}^n = \mathbf{o}.$$

Ověřme nyní axiomy pro násobení skalárem.

$$\begin{aligned} a \cdot (\mathbf{x} + \mathbf{y}) &= a \cdot (x_i + y_i)_{i=1}^n = (a(x_i + y_i))_{i=1}^n = (ax_i + ay_i)_{i=1}^n = a \cdot \mathbf{x} + a \cdot \mathbf{y} \\ (a + b) \cdot \mathbf{x} &= ((a + b)x_i)_{i=1}^n = (ax_i + bx_i)_{i=1}^n = a \cdot \mathbf{x} + b \cdot \mathbf{x} \\ a \cdot (b \cdot \mathbf{x}) &= a \cdot (bx_i)_{i=1}^n = (a(bx_i))_{i=1}^n = ((ab)x_i)_{i=1}^n = (ab) \cdot \mathbf{x} \\ 1 \cdot \mathbf{x} &= (1x_i)_{i=1}^n = (x_i)_{i=1}^n = \mathbf{x} \end{aligned}$$

Vidíme, že $\mathbb{R}^n$ je vektorovým prostorem nad $\mathbb{R}$.

Přejdeme k b). Můžeme se na situaci dívat dvěma způsoby. První je nahlížet na polynomy jako na funkce $\mathbb{R} \rightarrow \mathbb{R}$. Pak je součet polynomů definován tak, že funkční hodnota součtu je součtem funkčních hodnot a skalární násobek je definován jako násobek funkčních hodnot. Axiomy vektorového prostoru jsou následně splněny díky vlastnostem sčítání a násobení v $\mathbb{R}$.¹²

Druhý způsob je definovat sčítání polynomů jako polynom, jehož koeficienty jsou součty koeficientů při stejných mocninách x , skalární násobení je pak rovněž definováno vynášením všech koeficientů. Ověření axiomů vektorového prostoru je pak analogické k části a). Více k tomuto přístupu u části d).

Nyní vyřešíme c). Sčítání matic je definováno po složkách, díky tomu (a díky vlastnostem sčítání v $\mathbb{Z}_5$) bude sčítání matic asociativní, komutativní, neutrálním prvkem bude nulová matice a opačným prvkem k matici $A = (a_{ij})_{i,j=1}^3$ bude matice $-A = (5 - a_{ij})_{i,j=1}^3$. Násobení skalárem je rovněž definováno po složkách, takže (opět díky vlastnostem násobení a sčítání v $\mathbb{Z}_5$) máme splněny všechny axiomy vektorového prostoru.

Zajímavá je část d). Sčítání i násobení skalárem je definováno *po složkách*, díky tomu máme splněny všechny axiomy vektorového prostoru. Ověření je analogické jako v a), jen s tím rozdílem, že vektory píšeme jako $\mathbf{x} = (x_i)_{i=1}^\infty$, jinak je vše stejné. S určitým typem posloupností můžeme identifikovat i *polynomy*: Polynom $p(x) = p_0 + p_1 x + \dots + p_n x^n$ můžeme psát jako posloupnost

$$(p_0, p_1, \dots, p_n, 0, 0, \dots),$$

tedy lze polynomy identifikovat s množinou všech posloupností, které jsou od jistého indexu nulové. Tato charakterizace nám zredukuje ověření b) na d) (stačí si rozmyslet, že sčítáním konečně mnoha takových posloupností jakožto jejich skalárním násobením z prostoru nevypadneme).¹³ $\triangle$

¹²Takto lze definovat součet a skalární násobek *obecných funkcí* $\mathbb{R} \rightarrow \mathbb{R}$. Není těžké si rozmyslet, že i prostor všech funkcí $\mathbb{R} \rightarrow \mathbb{R}$ je vektorovým prostorem nad reálnými čísly. Podobně jsou vektorovými prostory i prosotry všech *spojitých* funkcí, funkcí *spojitě diferencovatelných* apod.

¹³Vidíme tedy, že polynomy jsou dokonce *vektorovým podprostorem* prostoru všech posloupností reálných čísel.

Příklad 1.6.2. Najděte všechny vektorové podprostory v $\mathbb{R}^2$, resp. v $\mathbb{R}^3$. Dělejte to „geometricky.“

Řešení. Uvažujme nejprve všechny podprostory v $\mathbb{R}^2$. Musí obsahovat nulový vektor $\mathbf{o} = (0, 0)$. Pokud jiný vektor neobsahují, jedná se o nulový podprostor. Mějme tedy vektor $\mathbf{u} \neq \mathbf{o}$. Každý vektorový podprostor, který jej obsahuje, musí obsahovat i všechny jeho skalární násobky $t \cdot \mathbf{u}$, $t \in \mathbb{R}$. Podprostor obsahující $\mathbf{u}$ tedy musí obsahovat i přímku zadanou $\mathbf{u}$. Uvažme jiný vektor $\mathbf{v}$. Pokud je s vektorem $\mathbf{u}$ lineárně závislý, jedná se o jeho skalární násobek a leží tedy v přímce generované $\mathbf{u}$. Pokud jsou $\mathbf{u}$ a $\mathbf{v}$ lineárně nezávislé, tvoří již bázi $\mathbb{R}^2$. Jedinými podprostory v $\mathbb{R}^2$ jsou tedy počátek, přímky procházející počátkem a celé $\mathbb{R}^2$.

Obdobně postupujeme v $\mathbb{R}^3$. Máme počátek a všechny přímky procházející počátkem. Dva lineárně nezávislé vektory v $\mathbb{R}^3$ určují rovinu procházející počátkem, tedy takovéto roviny jsou také *vlastními vektorovými podprostory*. Nakonec máme celé $\mathbb{R}^3$. $\triangle$

Příklad 1.6.3. Rozhodněte, zda následující množiny jsou vektorové podprostory.

- a) $U = \{f \in \mathbb{R}[x] \mid f(3) = f(-1) = 0\} \subset \mathbb{R}[x]$,
- b) $V = \{A \in \text{Mat}_{2 \times 2}(\mathbb{R}) \mid a_{1,1} + a_{2,2} = 1\} \subset \text{Mat}_{2 \times 2}(\mathbb{R})$,
- c) $W = \{A \in \text{Mat}_{2 \times 2}(\mathbb{R}) \mid a_{1,1} + a_{2,2} = 0\} \subset \text{Mat}_{2 \times 2}(\mathbb{R})$,
- d) $Z = \{f: \mathbb{N} \rightarrow \mathbb{R} \mid f(n+1) = f(n) + f(n-1)\} \subset \{f: \mathbb{N} \rightarrow \mathbb{R}\}$.

Řešení. Nejprve si připomeneme určující vlastnost vektorových podprostorů. Jsou to neprázdné podmnožiny uzavřené na sčítání vektorů a jejich násobení skalárem. To nastane právě tehdy, když je uzavřená na lineární kombinace délky 2 (nebo na lineární kombinace konečné délky), tj. T je vektorový podprostor, jestliže $T \neq \emptyset$ (ekvivalentně $\mathbf{o} \in T$) a pro každé vektory $\mathbf{u}, \mathbf{v} \in T$ a každé dva skaláry α, β platí $\alpha \cdot \mathbf{u} + \beta \cdot \mathbf{v} \in T$.

Přejdeme k řešení a). Zřejmě $0(3) = 0(-1) = 0$. Mějme dva polynomy $f, g \in U$ (tj. $f(3) = f(-1) = g(3) = g(-1) = 0$) a $\alpha, \beta \in \mathbb{R}$. Pak

$$\begin{aligned}(\alpha \cdot f + \beta \cdot g)(3) &= \alpha \cdot f(3) + \beta \cdot g(3) = 0 + 0 = 0, \\(\alpha \cdot f + \beta \cdot g)(-1) &= \alpha \cdot f(-1) + \beta \cdot g(-1) = 0 + 0 = 0.\end{aligned}$$

Je tedy U vektorovým podprostorem v $\mathbb{R}[x]$. Alternativně lze úlohu řešit pomocí následujícího pozorování. Polynomy $f, g \in U$ právě tehdy, když $f(x) = (x-3)(x+1)p(x)$ a $g(x) = (x-3)(x+1)q(x)$ pro nějaké $p, q \in \mathbb{R}[x]$. Pak

$$\alpha \cdot f + \beta \cdot g = (x-3)(x+1)(\alpha \cdot p + \beta \cdot q),$$

tedy fakt, že je U vektorový podprostor, lze ověřit také pomocí vytýkání polynomů. Obdobně by byl vektorovým podprostorem i prostor všech (polynomiálních) násobků nějakého polynomu.

Nyní vyřešíme b). Vidíme, že V není vektorovým podprostorem v $\text{Mat}_{2 \times 2}(\mathbb{R})$, neboť neobsahuje nulovou matici. Přejdeme rovnou k c). Množina W zřejmě obsahuje nulovou matici. Nechť tedy $A = (a_{i,j})$, $B = (b_{i,j}) \in W$, tj. $a_{1,1} + a_{2,2} = 0 = b_{1,1} + b_{2,2}$, a $\alpha, \beta \in \mathbb{R}$. Pak pro matici $\alpha \cdot A + \beta \cdot B$ platí

$$\alpha a_{1,1} + \beta b_{1,1} + \alpha a_{2,2} + \beta b_{2,2} = \alpha (a_{1,1} + a_{2,2}) + \beta (b_{1,1} + b_{2,2}) = 0 + 0 = 0,$$

takže W je vektorovým podprostorem v $\text{Mat}_{2 \times 2}(\mathbb{R})$.

Nakonec máme d). Pro nulovou posloupnost $o: \mathbb{N} \rightarrow \mathbb{R}$, $o(n) = 0$ platí

$$o(n+1) = 0 = 0 + 0 = o(n) + o(n-1),$$

tedy $o \in Z$. Nechť $f, g: \mathbb{N} \rightarrow \mathbb{R}$ jsou prvky Z , tedy

$$f(n+1) = f(n) + f(n-1) \qquad g(n+1) = g(n) + g(n-1).$$

Pak pro posloupnost $\alpha \cdot f + \beta \cdot g$, $\alpha, \beta \in \mathbb{R}$, platí

$$\begin{aligned} (\alpha \cdot f + \beta \cdot g)(n+1) &= \alpha f(n+1) + \beta g(n+1) \\ &= \alpha (f(n) + f(n-1)) + \beta (g(n) + g(n-1)) \\ &= \alpha f(n) + \alpha f(n-1) + \beta g(n) + \beta g(n-1) \\ &= (\alpha \cdot f + \beta \cdot g)(n) + (\alpha \cdot f + \beta \cdot g)(n-1), \end{aligned}$$

tudíž Z je vektorovým podprostorem v prostoru všech posloupností reálných čísel. $\triangle$

Příklad 1.6.4. Zjistěte, zda vektor $\mathbf{u} = (1, -2, 3, 4) \in \mathbb{R}^4$ leží v lineárním obalu vektorů $\mathbf{v}_1 = (1, 0, 1, -2)$, $\mathbf{v}_2 = (3, -1, -1, -1)$ a $\mathbf{v}_3 = (0, 1, -5, 4)$.

Řešení. Zjišťujeme, zda existují $k_1, k_2, k_3 \in \mathbb{R}$ taková, že

$$\mathbf{u} = k_1 \cdot \mathbf{v}_1 + k_2 \cdot \mathbf{v}_2 + k_3 \cdot \mathbf{v}_3.$$

Vzhledem k tomu, jak je definováno násobení skalárem na $\mathbb{R}^4$, dostáváme v každé složce rovnici pro tři neznámé. Celkem máme čtyři složky, tedy čtyři rovnice. Získáme tak soustavu čtyř rovnic o třech neznámých.

$$\begin{array}{rrcrcl} k_1 & + & 3k_2 & & = & 1 \\ & & -k_2 & + & k_3 & = & 0 \\ k_1 & - & k_2 & - & 5k_3 & = & 1 \\ -2k_1 & - & k_2 & + & 4k_3 & = & -2 \end{array}$$

Tu řešíme pomocí maticového zápisu. Všimněte si, že sloupce matice odpovídají souřadnicím vektorů $\mathbf{v}_1$, $\mathbf{v}_2$, $\mathbf{v}_3$ a $\mathbf{u}$.

$$\begin{pmatrix} 1 & 3 & 0 & | & 1 \\ 0 & -1 & 1 & | & 0 \\ 1 & -1 & -5 & | & 1 \\ -2 & -1 & 4 & | & -2 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 & 0 & | & 1 \\ 0 & -1 & 1 & | & 0 \\ 0 & -4 & -5 & | & 3 \\ 0 & 5 & 4 & | & 6 \end{pmatrix} \sim$$

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

Vidíme, že soustava nemá řešení, tedy vektor $\mathbf{u}$ nepatří do lineárního obalu vektorů $\mathbf{v}_1$, $\mathbf{v}_2$ a $\mathbf{v}_3$. $\triangle$

Jiné řešení. Zjišťujeme, zda má soustava

$$k_1 \cdot \mathbf{v}_1 + k_2 \cdot \mathbf{v}_2 + k_3 \cdot \mathbf{v}_3 + k_4 \cdot \mathbf{u} = \mathbf{o} \quad (1.9)$$

netriviální řešení. To můžeme dělat po složkách – dostaneme soustavu čtyř rovnic o čtyřech neznámých. Matice soustavy bude mít ve sloupcích postupně složky vektorů $\mathbf{v}_1$, $\mathbf{v}_2$, $\mathbf{v}_3$ a $\mathbf{u}$. V našem případě to bude matice

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

Postupovat lze Gaußovou eliminací, ovšem v našem případě máme stejný počet rovnic jako neznámých, tj. matice je čtvercová a máme definovaný determinant této matice. Pomocí softwaru spočítáme, že $\det A = 54$, tedy matice je regulární a (1.9) má pro danou pravou stranu jediné řešení. Vidíme, že $\mathbf{u}$ neleží v lineárním obalu $\mathbf{v}_1$, $\mathbf{v}_2$ a $\mathbf{v}_3$. $\triangle$

Poznámka. Postup s determinantom v alternativním řešení funguje pouze pro čtvercové matice, tedy pro $n - 1$ vektorů v n -rozměrném prostoru.

Příklad 1.6.5. Nechť M je podprostor $\mathbb{R}^5$ generovaný vektory $\mathbf{v}_1 = (1, 2, 1, 0, 1)$, $\mathbf{v}_2 = (2, -1, 0, 1, 1)$, $\mathbf{v}_3 = (1, -3, -1, 1, 0)$ a $\mathbf{v}_4 = (1, 7, 3, -1, 2)$. Rozhodněte, zda jsou tyto vektory lineárně nezávislé. Pokud ne, vyberte z nich bázi podprostoru M a zbylé vektory vyjádřete v této bázi.

Řešení. Zjišťujeme, zda má soustava

$$k_1 \cdot \mathbf{v}_1 + k_2 \cdot \mathbf{v}_2 + k_3 \cdot \mathbf{v}_3 + k_4 \cdot \mathbf{v}_4 = \mathbf{o}$$

netriviální řešení. Po složkách dostaneme soustavu pěti rovnic o čtyřech neznámých, kterou si můžeme zapsat do matice. Sloupce levé strany matice budou složky vektorů $\mathbf{v}_1$, $\mathbf{v}_2$, $\mathbf{v}_3$ a $\mathbf{v}_4$. Na pravé straně máme vždy nuly, nemusíme ji tedy vůbec psát. Postupujeme Gaußovou

eliminací. Nejprve eliminujeme první sloupec podle třetího řádku. Následně eliminujeme druhý sloupec podle čtvrtého řádku

$$\begin{pmatrix} 1 & 2 & 1 & 1 \\ 2 & -1 & -3 & 7 \\ 1 & 0 & -1 & 3 \\ 0 & 1 & 1 & -1 \\ 1 & 1 & 0 & 2 \end{pmatrix} \sim \begin{pmatrix} 0 & 2 & 2 & -2 \\ 0 & -1 & -1 & 1 \\ 1 & 0 & -1 & 3 \\ 0 & 1 & 1 & -1 \\ 0 & 1 & 1 & -1 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 3 \\ 0 & 1 & 1 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad (1.10)$$

Vidíme, že máme systém řešení $k_4 = s$, $k_3 = t$, $k_2 = s - t$ a $k_1 = t - 3s$ pro $t, s \in \mathbb{R}$. Vektory jsou lineárně závislé. Vybereme z nich bázi. Vidíme, že první dva sloupce všech matic v (1.10) jsou lineárně nezávislé. (Elementární řádkové úpravy zachovávají dimenzi.) Systém řešení lze přepsat do tvaru

$$t \cdot \mathbf{v}_3 + s \cdot \mathbf{v}_4 = (3s - t) \cdot \mathbf{v}_1 + (t - s) \cdot \mathbf{v}_2. \quad (1.11)$$

Dosazením $t = 1$, $s = 0$ do (1.11) dostaneme vyjádření $\mathbf{v}_3 - \mathbf{v}_1 + \mathbf{v}_2$ a dosazením $t = 0$, $s = 1$ vyjádření $\mathbf{v}_4 = 3 \cdot \mathbf{v}_1 - \mathbf{v}_2$. $\triangle$

Příklad 1.6.6. Spočítejte souřadnice polynomu $1 + 3x + 5x^2 + 10x^3$ v bázi

$$\alpha = (1 + x + 2x^2 - x^3, 1 + 2x + x^3, 1 + x + 3x^2 - x^3, 2 + 2x + 4x^2 + 5x^3)$$

prostoru $\mathbb{R}_3[x]$.

Řešení. Hledáme k_1, k_2, k_3 a k_4 tak, aby

$$1 + 3x + 5x^2 + 10x^3 = k_1 \cdot (1 + x + 2x^2 - x^3) + k_2 \cdot (1 + 2x + x^3) + k_3 \cdot (1 + x + 3x^2 - x^3) + k_4 \cdot (2 + 2x + 4x^2 + 5x^3).$$

Roznásobením pravé strany a vytknutím mocnin x dostaneme následující rovnici.

$$1 + 3x + 5x^2 + 10x^3 = (k_1 + k_2 + k_3 + 2k_4) + (k_1 + 2k_2 + k_3 + 2k_4)x + (2k_1 + 3k_3 + 4k_4)x^2 + (-k_1 + k_2 - k_3 + 5k_4)x^3$$

Dva polynomy jsou si rovny právě tehdy, když se rovnají koeficienty u příslušných mocnin x . (To je dáno tím, že mocniny x tvoří bázi $\mathbb{R}[x]$.) Získáváme soustavu čtyř rovnic o čtyřech neznámých.

$$\begin{array}{rrrrrcl} k_1 & + & k_2 & + & k_3 & + & 2k_4 & = & 1 \\ k_1 & + & 2k_2 & + & k_3 & + & 2k_4 & = & 3 \\ 2k_1 & & & + & 3k_3 & + & 4k_4 & = & 5 \\ -k_1 & + & k_2 & - & k_3 & + & 5k_4 & = & 10 \end{array}$$

Tuto soustavu řešíme Gaußovou eliminací pomocí maticového zápisu. Nejprve pomocí prvního řádku zredukujeme první sloupec. Následně podle druhého řádku zredukujeme druhý

sloupec.

$$\left(\begin{array}{cccc|c} 1 & 1 & 1 & 2 & 1 \\ 1 & 2 & 1 & 2 & 3 \\ 2 & 0 & 3 & 4 & 5 \\ -1 & 1 & -1 & 5 & 10 \end{array} \right) \sim \left(\begin{array}{cccc|c} 1 & 1 & 1 & 2 & 1 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & -2 & 1 & 0 & 3 \\ 0 & 2 & 0 & 7 & 11 \end{array} \right) \sim \left(\begin{array}{cccc|c} 1 & 0 & 1 & 2 & -1 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 & 7 \\ 0 & 0 & 0 & 7 & 7 \end{array} \right)$$

Poslední řádek vydělíme sedmi a poté pomocí něj zredukujeme čtvrtý sloupec. Nakonec pomocí třetího řádku zredukujeme třetí sloupec.

$$\sim \left(\begin{array}{cccc|c} 1 & 0 & 1 & 0 & -3 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 & 7 \\ 0 & 0 & 0 & 1 & 1 \end{array} \right) \sim \left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & -10 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 & 7 \\ 0 & 0 & 0 & 1 & 1 \end{array} \right)$$

Vidíme, že souřadnice polynomu $1 + 3x + 5x^2 + 10x^3$ v bázi α jsou $(-10, 2, 7, 1)$. $\triangle$

Příklad 1.6.7. Najděte bázi a dimenzi podprostoru U v $\mathbb{R}^5$ všech řešení následující soustavy rovnic.

$$\begin{aligned} 2x_1 - 3x_2 + 4x_3 - 8x_4 + x_5 &= 0 \\ x_1 + 2x_2 - 3x_3 + x_4 + 5x_5 &= 0 \end{aligned}$$

Řešení. Řešíme soustavu Gaußovou eliminací s pomocí maticového zápisu, přičemž nulovou pravou stranu nepíšeme.

$$\begin{aligned} \left(\begin{array}{ccccc} 2 & -3 & 4 & -8 & 1 \\ 1 & 2 & -3 & 1 & 5 \end{array} \right) &\sim \left(\begin{array}{ccccc} 0 & -7 & 10 & -10 & -9 \\ 1 & 2 & -3 & 1 & 5 \end{array} \right) \sim \\ &\sim \left(\begin{array}{ccccc} 0 & -7 & 10 & -10 & -9 \\ 7 & 14 & -21 & 7 & 35 \end{array} \right) \sim \left(\begin{array}{ccccc} 0 & -7 & 10 & -10 & -9 \\ 7 & 0 & -1 & -13 & 17 \end{array} \right) \end{aligned}$$

Položme $x_3 = 7r$, $x_4 = 7t$ a $x_5 = 7s$. Pak $x_1 = r + 13t - 17s$ a $x_2 = 10r - 10t - 9s$. Máme parametrický popis vektorů $\mathbf{x} = (x_1, x_2, x_3, x_4, x_5)$ z U :

$$\begin{aligned} \mathbf{x} &= (r + 13t - 17s, 10r - 10t - 9s, 7r, 7t, 7s) \\ &= r \cdot (1, 10, 7, 0, 0) + t \cdot (13, -10, 0, 7, 0) + s \cdot (-17, -9, 0, 0, 7) \end{aligned}$$

Položme $\mathbf{u}_1 = (1, 10, 7, 0, 0)$, $\mathbf{u}_2 = (13, -10, 0, 7, 0)$ a $\mathbf{u}_3 = (-17, -9, 0, 0, 7)$. Pak $\{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\}$ tvoří bázi U a je vidět, že $\dim U = 3$. $\triangle$

Příklad 1.6.8. Najděte báze a dimenze podprostorů

$$P = \{f \in \mathbb{R}_4[x] \mid f(1) = f(2) = 0\}, \quad Q = \{g \in \mathbb{R}_4[x] \mid g(x) = g(-x)\}.$$

Řešení. Všimněme si, že všechny polynomy v P musí být tvaru

$$p(x) = (x-1)(x-2)q(x) = (x^2 - 3x + 2)q(x) \quad (1.12)$$

kde q je vhodný polynom (viz příklad 1.6.3 a)). Aby byl polynom p stupně nejvýše 4, musí být q stupně nejvýše 2. (Stupeň součinu polynomů je roven součtu stupňů.) Pak ale $q \in \mathbb{R}_2[x]$ a lze psát $q(x) = q_0 + q_1 x + q_2 x^2$. Z (1.12) platí, že polynomy v P lze psát jako

$$\begin{aligned} p(x) &= (x^2 - 3x + 2)(q_0 + q_1 x + q_2 x^2) \\ &= q_0(x^2 - 3x + 2) + q_1(x^3 - 3x^2 + 2x) + q_2(x^4 - 3x^3 + 2x^2). \end{aligned} \quad (1.13)$$

Vidíme, že dimenze P je 3 a báze je (například) $(x^2 - 3x + 2, x^3 - 3x^2 + 2x, x^4 - 3x^3 + 2x^2)$.

Ověřme nejprve, že Q je skutečně lineární podprostor. Nulový polynom jistě do Q patří, nechť $f, g \in Q$, $\alpha, \beta \in \mathbb{R}$.

$$(\alpha \cdot f + \beta \cdot g)(-x) = \alpha f(-x) + \beta g(-x) = \alpha f(x) + \beta g(x) = (\alpha \cdot f + \beta \cdot g)(x)$$

Q je vektorovým podprostorem. Podívejme se na charakterizaci polynomů z Q . Je-li $f \in Q$, platí $f(x) = f(-x)$. Píšeme-li $f(x) = f_0 + f_1 x + f_2 x^2 + f_3 x^3 + f_4 x^4$, pak

$$f(-x) = f_0 - f_1 x + f_2 x^2 - f_3 x^3 + f_4 x^4.$$

Má-li být $f(x) = f(-x)$ pro každé x , pak musí být $f_1 = f_3 = 0$. Lze tedy psát $f(x) = f_0 + f_2 x^2 + f_4 x^4$. Odtud je zřejmé, že $\dim Q = 3$ a báze Q je (například) $(1, x^2, x^4)$. $\triangle$

Poznámka. Z charakterizace P pomocí (1.12) vidíme, že P je obraz lineárního zobrazení $\mathbb{R}_2[x] \rightarrow \mathbb{R}_4[x]$ daného násobením polynomem $x^2 - 3x + 2$. Toto zobrazení má (ve standardních bázích mocnin x seřazené shora od největší k nejmenší) předpis s maticí

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

kterou jsme získali pomocí (1.13). Pokud polynom $q(x) = q_2 x^2 + q_1 x + q_0$ ztotožníme s vektorem $\mathbf{q} = (q_2, q_1, q_0)^T$, pak polynom $(x^2 - 3x + 2)q(x)$ ztotožníme s vektorem $A \cdot \mathbf{q}$.

Podobně bychom mohli popsat Q . Zobrazení $\mathbb{R}_2[x] \rightarrow \mathbb{R}_4[x]$ zadané předpisem $g(x) \mapsto g(x^2)$ je lineární a má (ve stejných bázích jako výše) matici

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

Tato charakterizace by fungovala i pro ekvivalenty P a Q v prostoru *všech* polynomů $\mathbb{R}[x]$, kde však již nemáme popis pomocí matic (byly by nekonečné).

1.7 Determinant

Příklad 1.7.1. Připomeňte si základní vlastnosti determinantů matic nad tělesem.

Řešení. Mějme čtvercovou matici $A = (a_{i,j})_{i,j=1}^n$. Definujeme její determinant jako

$$\det A := \sum_{\sigma \in \mathbb{S}_n} (-1)^{|\sigma|} a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} \cdot \dots \cdot a_{n,\sigma(n)} \quad (1.14)$$

kde suma probíhá přes všechny permutace n -prvkové množiny. Na permutace se lze také dívat jako na výběry prvků matice tak, abychom z každého řádku i sloupce vybrali právě jeden prvek. Determinant A značíme $\det A$ nebo $|A|$. Číslo $(-1)^{|\sigma|}$ známe *znaménko permutace* a počítáme jej jako -1 na počet transpozic (záměn dvou prvků), kterými utvoříme σ z identity. (Počet $|\sigma|$ není jednoznačný, ale je vždy buď sudý, nebo lichý.) Protože jsme místo σ mohli vzít σ^{-1} se stejným znaménkem, máme

$$\det A = \sum_{\sigma \in \mathbb{S}_n} (-1)^{|\sigma|} a_{\sigma^{-1}(1),1} \cdot a_{\sigma^{-1}(2),2} \cdot \dots \cdot a_{\sigma^{-1}(n),n} = \det A^T, \quad (1.15)$$

kde A^T je matice transponovaná, $A^T = (a_{j,i})_{i,j=1}^n$. Determinant má následující vlastnosti.

- (i) Vyměníme-li dva řádky matice A , determinant se vynásobí -1 .
- (ii) Vynásobíme-li nějaký řádek matice A číslem a , determinant se vynásobí tímž číslem a .
- (iii) Přičteme-li a -násobek jednoho řádku k jinému, determinant se nezmění.
- (iv) $\det(A \cdot B) = \det A \cdot \det B$
- (v) $\det(A^{-1}) = \frac{1}{\det A}$
- (vi) Je-li některý řádek matice nulový, je determinant matice nulový.
- (vii) Je-li matice A singulární (nemá-li inverzi), je $\det A = 0$.
- (viii) Determinant jednotkové matice je 1.
- (ix) Determinant horní nebo dolní trojúhelníkové matice je součin prvků na diagonále.

Důkaz těchto (a jiných) vlastností determinantů je možné najít například v 10. kapitole učebnice *Lineární algebra a geometrie* od P. Zlatoše,¹⁴ nicméně některé lze dokázat poměrně jednoduše.

Vlastnost (i) plyne z toho, že výměna řádků po dosazení do (1.14) přidá jednu transpozici ke každé permutaci, což znaménka všech permutací změni na opačnou, takže -1 můžeme vytknout z (1.14) a dostaneme determinant původní matice. Stejně tak vynásobíme-li řádek nějakým číslem a , bude toto číslo v každém sčítanci v (1.14) právě jednou, což dává (ii).

¹⁴http://thales.doa.fmph.uniba.sk/zlatos/la/LAG_A4.pdf

Vynásobíme-li celou matici číslem a , je to jako násobit každý z n řádků, tedy determinant se vynásobí a^n . Vlastnosti (i) – (iii) mají i své sloupcové obdoby díky (1.15).

Vlastnost (vi) je zřejmá – v každém sčítanci v (1.15) bude 0. Jejím přímým důsledkem je vlastnost (vii), protože v singulární matici umíme pomocí elementárních řádkových úprav vyrobit nulový řádek. Vlastnosti (viii) a (ix) jsou dokázány obdobně – jediná transpozice, která nebude mít ani v jednom činiteli v součinu nulu, bude identita s kladným znaménkem. Vlastnost (iv) je známá jako *Cauchyho věta o součinu determinantů*.

Definujme $A_{i,j}$ matici, která vznikla z A odebráním i -tého řádku a j -tého sloupce. Poté pro i -tý řádek matice A platí, že

$$\det A = \sum_{j=1}^n (-1)^{i+j} a_{i,j} \det A_{i,j}. \quad (1.16)$$

Vztah (1.16), dokázaný v sekci 10.4 Lineární algebry a geometrie a nazývaný *Laplaceův rozvoj determinantu*, má i svoji sloupcovou variantu. Pro j -tý sloupec A platí

$$\det A = \sum_{i=1}^n (-1)^{i+j} a_{i,j} \det A_{i,j}. \quad \triangle$$

Příklad 1.7.2. Spočítejte determinant matice

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

a) pomocí řádkových úprav,

b) pomocí Laplaceova rozvoje vhodného řádku.

Řešení. Začneme a). Upravujeme matici do horního trojúhelníkového tvaru a přitom sledujeme, jak úpravy mění determinant. Nejprve pomocí druhého řádku zredukujeme první sloupec, což determinant nezmění. Následně prohodíme první a druhý řádek, a potom druhý a nový třetí. Toto vynásobí determinant $(-1)^2 = 1$, tedy jej opět nezmění.

$$\begin{pmatrix} 2 & -1 & 0 & 3 \\ 1 & 0 & -2 & 0 \\ -1 & 1 & 2 & 1 \\ -3 & -2 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & -1 & 4 & 3 \\ 1 & 0 & -2 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & -2 & -5 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & -2 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & -1 & 4 & 3 \\ 0 & -2 & -5 & 1 \end{pmatrix}$$

Nový druhý řádek přičteme ke třetímu a jeho dvojnásobek ke čtvrtému. Ani tato operace nezmění determinant. Poté třetí řádek vydělíme čtyřmi, což vydělí čtyřmi i determinant. Nakonec přičteme k poslednímu řádku pětinašobek předchozího, což determinant nezmění.

$$\sim \begin{pmatrix} 1 & 0 & -2 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 4 & 4 \\ 0 & 0 & -5 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & -2 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & -5 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & -2 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 8 \end{pmatrix}$$

Máme horní trojúhelníkovou matici. Její determinant je 8 – součin prvků na diagonále. Protože při úpravách se determinant vydělil 4, byl determinant původní matice 32.

Pro b) postupujeme Laplaceovým rozvojem podle 2. řádku. Máme

$$\begin{aligned} \det \begin{pmatrix} 2 & -1 & 0 & 3 \\ 1 & 0 & -2 & 0 \\ -1 & 1 & 2 & 1 \\ -3 & -2 & 1 & 1 \end{pmatrix} &= (-1)^{2+1} \cdot 1 \cdot \det \begin{pmatrix} -1 & 0 & 3 \\ 1 & 2 & 1 \\ -2 & 1 & 1 \end{pmatrix} \\ &\quad + (-1)^{2+3} \cdot (-2) \cdot \det \begin{pmatrix} 2 & -1 & 3 \\ -1 & 1 & 1 \\ -3 & -2 & 1 \end{pmatrix} \\ &= 2 \cdot \det \begin{pmatrix} 2 & -1 & 3 \\ -1 & 1 & 1 \\ -3 & -2 & 1 \end{pmatrix} - \det \begin{pmatrix} -1 & 0 & 3 \\ 1 & 2 & 1 \\ -2 & 1 & 1 \end{pmatrix} \end{aligned}$$

Spočítáme determinanty submatic 3×3 . Pro první matici postupujeme Laplaceovým rozvojem podle druhého řádku.

$$\begin{aligned} \det \begin{pmatrix} 2 & -1 & 3 \\ -1 & 1 & 1 \\ -3 & -2 & 1 \end{pmatrix} &= (-1)^{2+1+1} \det \begin{pmatrix} -1 & 3 \\ -2 & 1 \end{pmatrix} + (-1)^{2+2} \det \begin{pmatrix} 2 & 3 \\ -3 & 1 \end{pmatrix} \\ &\quad + (-1)^{2+3} \det \begin{pmatrix} 2 & -1 \\ -3 & -2 \end{pmatrix} \\ &= (-1 \cdot 1 - (-2) \cdot 3) + (3 \cdot 1 - (-3) \cdot 3) \\ &\quad - (2 \cdot (-2) - (-3) \cdot (-1)) \\ &= -1 + 6 + 2 + 9 + 4 + 3 = 23 \end{aligned}$$

Determinant druhé matice spočítáme opět Laplaceovým rozvojem podle prvního řádku.

$$\begin{aligned} \det \begin{pmatrix} -1 & 0 & 3 \\ 1 & 2 & 1 \\ -2 & 1 & 1 \end{pmatrix} &= (-1)^{1+1+1} \det \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} + (-1)^{1+3} \cdot 3 \cdot \det \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix} \\ &= -(2 \cdot 1 - 1 \cdot 1) + 3 \cdot (1 \cdot 1 - (-2) \cdot 2) \\ &= -1 + 15 = 14 \end{aligned}$$

Celkem tak máme determinant původní matice.

$$\det \begin{pmatrix} 2 & -1 & 0 & 3 \\ 1 & 0 & -2 & 0 \\ -1 & 1 & 2 & 1 \\ -3 & -2 & 1 & 1 \end{pmatrix} = 2 \cdot 23 - 14 = 32 \quad \triangle$$

Příklad 1.7.3. Zjistěte, pro které parametry $a, b, c \in \mathbb{R}$ je soustava rovnic

$$\begin{array}{rcl} ax_1 + bx_2 & & = c \\ cx_1 & + ax_3 & = b \\ & cx_2 + bx_3 & = a \end{array}$$

jednoznačně řešitelná. Pro tyto parametry najděte řešení pomocí Cramerova pravidla.

Řešení. Soustava je jednoznačně řešitelná právě tehdy, je-li determinant matice soustavy nenulový. Soustava matice je

$$A := \begin{pmatrix} a & b & 0 \\ c & 0 & a \\ 0 & c & b \end{pmatrix}.$$

Spočítáme $\det A$ Laplaceovým rozvojem podle prvního řádku.

$$\begin{aligned} \det A &= (-1)^{1+1} \cdot a \cdot \det \begin{pmatrix} 0 & a \\ c & b \end{pmatrix} + (-1)^{1+2} \cdot b \cdot \det \begin{pmatrix} c & a \\ 0 & b \end{pmatrix} \\ &= a \cdot (-c \cdot a) - b \cdot c \cdot b = -c(a^2 + b^2) \end{aligned}$$

Vidíme tedy, že $\det A = 0$ právě tehdy, když je $c = 0$ nebo $a = b = 0$. Obměnou vidíme, že $\det A \neq 0$ právě tehdy, když $c \neq 0$ a alespoň jedno z a, b je nenulové. Tuto podmínku lze psát tak, že $a^2 + b^2 > 0$.¹⁵ Pak podle Cramerova pravidla platí

$$x_i = \frac{\det A_i}{\det A},$$

kde A_i je matice, kde jsme i -tý sloupec matice A nahradili sloupcem z pravé strany rovnice. Máme

$$A_1 = \begin{pmatrix} c & b & 0 \\ b & 0 & a \\ a & a & b \end{pmatrix},$$

tedy opět počítáme determinant Laplaceovým rozvojem podle prvního řádku.

$$\begin{aligned} \det A_1 &= (-1)^{1+1} \cdot c \cdot \det \begin{pmatrix} 0 & a \\ b & b \end{pmatrix} + (-1)^{1+2} \cdot b \cdot \det \begin{pmatrix} b & a \\ a & b \end{pmatrix} \\ &= -ca^2 - b^3 + ba^2 \end{aligned}$$

Obdobně

$$A_2 = \begin{pmatrix} a & c & 0 \\ c & b & a \\ 0 & a & b \end{pmatrix}$$

a počítáme $\det A_2$ Laplaceovým rozvojem podle prvního řádku.

$$\det A_2 = a \cdot \det \begin{pmatrix} b & a \\ a & b \end{pmatrix} - b \cdot \det \begin{pmatrix} c & a \\ 0 & b \end{pmatrix}$$

¹⁵Platí totiž $a^2 + b^2 \geq 0$ a výraz je roven nule jen pro $a = b = 0$.

$$= a b^2 - a^3 - b c^2$$

Nakonec

$$A_3 = \begin{pmatrix} a & b & c \\ c & 0 & b \\ 0 & a & a \end{pmatrix},$$

takže nyní počítáme determinant Laplaceovým rozvojem podle prvního sloupce.

$$\begin{aligned} \det A_3 &= a \cdot \det \begin{pmatrix} 0 & b \\ a & a \end{pmatrix} - c \cdot \det \begin{pmatrix} b & c \\ a & a \end{pmatrix} \\ &= -a^2 b - a b c + a c^2 \end{aligned}$$

Máme tedy řešení

$$x_1 = \frac{b^3 - a^2 b + a^2 c}{c(a^2 + b^2)} \quad x_2 = \frac{a^3 + b c^2 - a c^2}{c(a^2 + b^2)} \quad x_3 = \frac{a^2 b + a b c - a c^2}{c(a^2 + b^2)}$$

pro všechna $a, b \in \mathbb{R}$ tak, že $a^2 + b^2 > 0$ a $c \in \mathbb{R} \setminus \{0\}$.

△

Příklad 1.7.4. Spočítejte determinant matice

$$A_5 = \begin{pmatrix} a & 1 & 1 & 1 & 1 \\ 1 & a & 1 & 1 & 1 \\ 1 & 1 & a & 1 & 1 \\ 1 & 1 & 1 & a & 1 \\ 1 & 1 & 1 & 1 & a \end{pmatrix}$$

a) pomocí řádkových úprav,

b) pomocí Laplaceova rozvoje 1. řádku a indukce.

Řešení. Označme $A_n = (a_{i,j})$ matici $n \times n$ definovanou předpisem

$$a_{i,j} = \begin{cases} a & i = j, \\ 1 & i \neq j. \end{cases}$$

Odtud plyne označení naší matice A_5 . Začneme a). Budeme používat řádkové i sloupcové úpravy. Nejprve odečteme poslední řádek od všech ostatních. Následně k poslednímu sloupci přičteme všechny ostatní. Tyto operace nemění determinant.

$$\begin{pmatrix} a & 1 & 1 & 1 & 1 \\ 1 & a & 1 & 1 & 1 \\ 1 & 1 & a & 1 & 1 \\ 1 & 1 & 1 & a & 1 \\ 1 & 1 & 1 & 1 & a \end{pmatrix} \sim \begin{pmatrix} a-1 & 0 & 0 & 0 & 1-a \\ 0 & a-1 & 0 & 0 & 1-a \\ 0 & 0 & a-1 & 0 & 1-a \\ 0 & 0 & 0 & a-1 & 1-a \\ 1 & 1 & 1 & 1 & a \end{pmatrix}$$

$$\begin{pmatrix} a-1 & 0 & 0 & 0 & 0 \\ 0 & a-1 & 0 & 0 & 0 \\ 0 & 0 & a-1 & 0 & 0 \\ 0 & 0 & 0 & a-1 & 0 \\ 1 & 1 & 1 & 1 & a+4 \end{pmatrix}$$

Na konci dostaneme dolní trojúhelníkovou matici, jejíž determinant je součin prvků na diagonále. Dostáváme

$$\det A_5 = (a-1)^4 (a+4).$$

Stejný postup by samozřejmě fungoval pro libovolnou matici A_n , přičemž bychom nejprve dostali na diagonále $a-1$ a mimo ni $1-a$, následně přičtením prvních $n-1$ sloupců k poslednímu bychom získali v pravém dolním rohu $a+n-1$. Máme tak vzorec

$$\det A_n = (a-1)^{n-1} (a+n-1).$$

Vidíme například, že A_n je invertibilní pro všechna a s výjimkou $a=1$ a $a=1-n$.

Počítejme b).

$$\begin{aligned} \det A_5 &= a \cdot \det A_4 - \det \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & a & 1 & 1 \\ 1 & 1 & a & 1 \\ 1 & 1 & 1 & a \end{pmatrix} + \det \begin{pmatrix} 1 & a & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & a & 1 \\ 1 & 1 & 1 & a \end{pmatrix} \\ &\quad - \det \begin{pmatrix} 1 & a & 1 & 1 \\ 1 & 1 & a & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & a \end{pmatrix} + \det \begin{pmatrix} 1 & a & 1 & 1 \\ 1 & 1 & a & 1 \\ 1 & 1 & 1 & a \\ 1 & 1 & 1 & 1 \end{pmatrix} \\ &= a \cdot \det A_4 - 4 \det B_4 \end{aligned}$$

Poslední čtyři matice jsou si vzájemně řádkově podobné, přičemž pro převod druhé a čtvrté matice na první potřebujeme provést lichý počet výměn řádků a pro převod třetí je to sudý počet řádků.

Označením $B_n = (b_{i,j})$ matice $n \times n$, která vznikla nahrazením $a_{1,1}$ v matici A_n jedničkou získáme poslední řádek. Navíc odečtením prvního řádku od ostatních je matice B_n řádkově podobná matici s prvním řádkem samých jedniček, $a-1$ jinde na diagonále a 0 jinak, je tedy $\det B_n = (a-1)^{n-1}$, v našem případě je $\det B_4 = (a-1)^3$.

Indukcí předpokládáme $\det A_4 = (a-1)^3 (a+3)$. Počítejme

$$\begin{aligned} \det A_5 &= a \det A_4 - 4 \det B_4 = a(a-1)^3 (a+3) - 4(a-1)^3 \\ &= (a-1)^3 (a^2 + 3a - 4) = (a-1)^4 (a+4). \end{aligned}$$

Poslední rovnost máme díky rozkladu $a^2 + 3a - 4 = (a-1)(a+4)$. Obdobně bychom dostali obecný vzorec – stačí použít rozklad $a^2 + (n-2)a - (n-1) = (a-1)(a+n-1)$.

$$\begin{aligned} \det A_n &= a \det A_{n-1} - (n-1) \det B_{n-1} \\ &= a(a-1)^{n-2} (a+n-2) - (n-1)(a-1)^{n-2} \\ &= (a-1)^{n-2} (a^2 + (n-2)a - (n-1)) = (a-1)^{n-1} (a+n-1) \quad \triangle \end{aligned}$$

Kapitola 2

Geometrie

2.1 Lineární zobrazení

Příklad 2.1.1. Rozhodněte, zda následující zobrazení mezi vektorovými prostory jsou lineární.

a) $\varphi: \mathbb{R}^2 \rightarrow \mathbb{R}, \varphi(x_1, x_2) = \frac{x_1^3 + x_2^3}{x_1^2 + x_2^2},$

b) $\psi: \mathbb{R}^3 \rightarrow \mathbb{R}^2, \psi(x_1, x_2, x_3) = (2x_1 - x_2, 2x_2 - x_3),$

c) $\xi: \mathbb{R}[x] \rightarrow \mathbb{R}^2, \xi(p) = (p(0), p'(0)).$

Řešení. Začneme a). Vidíme, že $\varphi(0, 0)$ není definované. Definujeme hodnotu pomocí limity.

$$\lim_{(x_1, x_2) \rightarrow (0, 0)} \varphi(x_1, x_2) = \lim_{(x_1, x_2) \rightarrow (0, 0)} \frac{x_1^3 + x_2^3}{x_1^2 + x_2^2}$$

Zavedeme polární souřadnice $x_1 = \varrho \cos \theta, x_2 = \varrho \sin \theta$.

$$\begin{aligned} &= \lim_{\varrho \rightarrow 0} \frac{\varrho^3 (\cos^3 \theta + \sin^3 \theta)}{\varrho^3 \underbrace{(\cos^2 \theta + \sin^2 \theta)}_1} \\ &= \lim_{\varrho \rightarrow 0} \varrho (\sin^3 \theta + \cos^3 \theta) = 0 \end{aligned}$$

Poslední rovnost jsme získali, jelikož je $\sin^3 \theta + \cos^3 \theta$ konečná hodnota pro libovolné θ . Definujme tedy $\varphi(0, 0) = 0$. Vidíme (z počítání limity), že $\varphi(kx_1, kx_2) = k\varphi(x_1, x_2)$. Zobrazení φ však není lineární, protože nerespektuje sčítání vektorů. Vidíme například, že

$$\varphi(1, 0) = \frac{1+0}{1+0} = 1 = \frac{0+1}{0+1} = \varphi(0, 1),$$

ale

$$\varphi(1, 1) = \frac{1+1}{1+1} = \frac{2}{2} = 1 \neq 2 = \varphi(1, 0) + \varphi(0, 1).$$

Pokračujme b). Zobrazení ψ je lineární. Mějme vektory $\mathbf{x} = (x_1, x_2, x_3)$ a $\mathbf{y} = (y_1, y_2, y_3) \in \mathbb{R}^3$ a skaláry $\alpha, \beta \in \mathbb{R}$.

$$\begin{aligned}\psi(\alpha \cdot \mathbf{x} + \beta \cdot \mathbf{y}) &= \psi(\alpha x_1 + \beta y_1, \alpha x_2 + \beta y_2, \alpha x_3 + \beta y_3) = \\ &= (2(\alpha x_1 + \beta y_1) - (\alpha x_2 + \beta y_2), 2(\alpha x_2 + \beta y_2) - (\alpha x_3 + \beta y_3)) = \\ &= (\alpha(2x_1 - x_2) + \beta(2y_1 - y_2), \alpha(2x_2 - x_3) + \beta(2y_2 - y_3)) = \\ &= \alpha \cdot \psi(\mathbf{x}) + \beta \cdot \psi(\mathbf{y})\end{aligned}$$

Píšeme-li vektory jako sloupce, pak má ve standardních bázích matici

$$(\psi)_{\varepsilon, \varepsilon} = \begin{pmatrix} 2 & -1 & 0 \\ 0 & 2 & -1 \end{pmatrix}.$$

Nakonec c). Mějme polynom

$$p(x) = p_0 + p_1 x + \cdots + p_n x^n. \quad (2.1)$$

Zderivováním p dostaneme

$$p'(x) = p_1 + 2p_2 x + \cdots + n p_n x^{n-1}. \quad (2.2)$$

Dosazením 0 do (2.1) dostaneme $p(0) = 0$, do (2.2) pak $p'(0) = p_1$. Máme tedy předpis

$$\xi(p) = (p_0, p_1).$$

Díky vlastnostem sčítání polynomů a jejich násobení skalárem je ξ lineární (viz příklad 1.6.1 b)). $\triangle$

Jiné řešení c). Zobrazení ξ lze psát jako složení $\xi_2 \circ \xi_1$, kde $\xi_1: \mathbb{R}[x] \rightarrow \mathbb{R}[x]^2$ je dané předpisem $p \mapsto (p, p')$ a $\xi_2: \mathbb{R}[x]^2 \rightarrow \mathbb{R}^2$ pak přepisem $(f, g) \mapsto (f(0), g(0))$. Jelikož

$$(\alpha f + \beta g)' = \alpha f' + \beta g'$$

pro libovolné polynomy (dokonce diferencovatelné funkce), je zobrazení ξ_1 lineární. Linearity ξ_2 se ukáže jako původně. Pak je ξ lineární jako složení dvou lineárních zobrazení. $\triangle$

Příklad 2.1.2. Ve vektorovém prostoru $\mathbb{R}^3$ uvažujme bázi $\mathbf{u}_1 = (1, -1, 1)^T$, $\mathbf{u}_2 = (1, 1, 0)^T$, $\mathbf{u}_3 = (2, 1, 1)^T$. Nechť $\varphi: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ je lineární zobrazení, o němž víme, že

$$\varphi(\mathbf{u}_1) = \mathbf{u}_2, \quad \varphi(\mathbf{u}_2) = \mathbf{u}_3, \quad \varphi(\mathbf{u}_3) = \mathbf{u}_1.$$

Najděte matici A tvaru 3×3 tak, aby v souřadnicích standardní báze bylo $\varphi(\mathbf{x}) = A \cdot \mathbf{x}$.

Řešení. Označme $\alpha = (\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$ bázi danou vektory ze zadání a $\epsilon = (\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3)$ standardní bázi. Budeme-li mít na vstupu i na výstupu vektory psané v souřadnicích báze α , bude φ zadané maticí

$$\varphi_{\alpha, \alpha} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Chceme však vektory psát ve standardních souřadnicích. Budeme muset uvažovat *změnu báze*. Vezměme matici

$$P_{\epsilon, \alpha} = \begin{pmatrix} 1 & 1 & 2 \\ -1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix},$$

jejíž sloupce jsou složky vektorů báze α . Všimněme si, že budeme-li psát vektory na vstupu v souřadnicích vzhledem k bázi α , dá nám násobení maticí $P_{\epsilon, \alpha}$ souřadnice vzhledem k bázi ϵ . To plyne z následujícího pozorování. Podíváme-li se na vektory $\mathbf{u}_1, \mathbf{u}_2$ a $\mathbf{u}_3$, mají vzhledem k bázi α souřadnice $(1, 0, 0)^T$, $(0, 1, 0)^T$ a $(0, 0, 1)^T$. Vynásobíme-li tyto sloupce maticí $P_{\alpha, \epsilon}$, získáme ve sloupcích složky vektorů $\mathbf{u}_1, \mathbf{u}_2$ a $\mathbf{u}_3$, jejich souřadnice v bázi ϵ . Zbytek plyne z linearitě násobení vektorů maticí. Umíme tedy změnit souřadnice z báze α k bázi ϵ . Matice $P_{\epsilon, \alpha}$ se nazývá *maticí přechodu* od báze α k bázi ϵ .¹

Nyní chceme obrátit proces, tj. vektory psané ve standardních souřadnicích chceme psát v souřadnicích báze α . Je zřejmé, že změníme-li souřadnice od báze α k bázi ϵ a pak zpět, dostaneme identitu. Pak tedy nutně musí být matice přechodu $P_{\alpha, \epsilon}$ inverzní maticí k $P_{\epsilon, \alpha}$, tj.

$$P_{\alpha, \epsilon} = P_{\epsilon, \alpha}^{-1}.$$

Inverzní matici najdeme standardním způsobem.

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

Vidíme, že

$$P_{\alpha, \epsilon} = \begin{pmatrix} 1 & -1 & -1 \\ 2 & -1 & -3 \\ -1 & 1 & 2 \end{pmatrix}.$$

¹Indexy jsou psány zprava doleva, protože sloupcové vektory násobíme maticemi zleva, tedy napravo máme souřadnice vzhledem k bázi α , a po vynásobení maticí přechodu zleva dostaneme souřadnice v bázi ϵ .

Pak máme $A = \varphi_{\epsilon, \epsilon} = P_{\epsilon, \alpha} \cdot \varphi_{\alpha, \alpha} \cdot P_{\alpha, \epsilon}$.

$$A = \begin{pmatrix} 1 & 1 & 2 \\ -1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 & -1 \\ 2 & -1 & -3 \\ -1 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 3 & -2 & -3 \\ -2 & 1 & 4 \\ 3 & -2 & -4 \end{pmatrix} \quad \triangle$$

Příklad 2.1.3. Necht φ je zobrazení $\mathbb{R}^3$ do sebe, které je symetrií podle roviny ρ , zadané rovnicí $x_2 + x_3 = 0$. Najděte matici B takovou, že v souřadnicích standardní báze je $\varphi(\mathbf{x}) = B \cdot \mathbf{x}$.

Algebraické řešení. Najdeme si vhodnou bázi prostoru $\mathbb{R}^3$, ve které bude mít zobrazení φ vhodnou matici. Poté pomocí změny báze maticemi přechodu zjistíme matici B . Rovnice $x_2 + x_3 = 0$ je zřejmě řešena vektory tvaru

$$\mathbf{x} = (t, s, -s) = t \cdot (1, 0, 0)^T + s \cdot (0, 1, -1)^T.$$

Označme $\mathbf{u}_1 := (1, 0, 0)^T = \mathbf{e}_1$, $\mathbf{u}_2 := (0, 1, -1)^T$. Vektory $\mathbf{u}_1, \mathbf{u}_2$ tvoří bázi roviny ρ . Vektor $\mathbf{u}_3 := (0, 1, 1)^T$ je kolmý na ρ , jedná se o *normálový vektor roviny* ρ . (Je to vektor, jehož složky jsou koeficienty zadávající rovnice.) Platí, že $\alpha = (\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$ tvoří bázi $\mathbb{R}^3$. (Vektory jsou celkem zřejmě lineárně nezávislé.)

Zobrazení φ nechá vektory $\mathbf{u}_1$ a $\mathbf{u}_2$ na místě, jelikož leží v rovině ρ . Vektor $\mathbf{u}_3$ se zobrazí na $-\mathbf{u}_3$, neboť je kolmý na ρ a jeho symetrií podle této roviny tak bude vektor k němu opačný. V bázi α tak má φ matici

$$\varphi_{\alpha, \alpha} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Nyní již můžeme postupovat jako v příkladu 2.1.2. Najdeme matice přechodu a složením získáme matici $B = \varphi_{\epsilon, \epsilon}$, kde $\epsilon = (\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3)$ značí opět standardní bázi. Matice přechodu od α k ϵ je

$$P_{\epsilon, \alpha} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & -1 & 1 \end{pmatrix},$$

matice opačného přechodu $P_{\alpha, \epsilon} = P_{\epsilon, \alpha}^{-1}$ je k ní inverzní.

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

Máme tedy

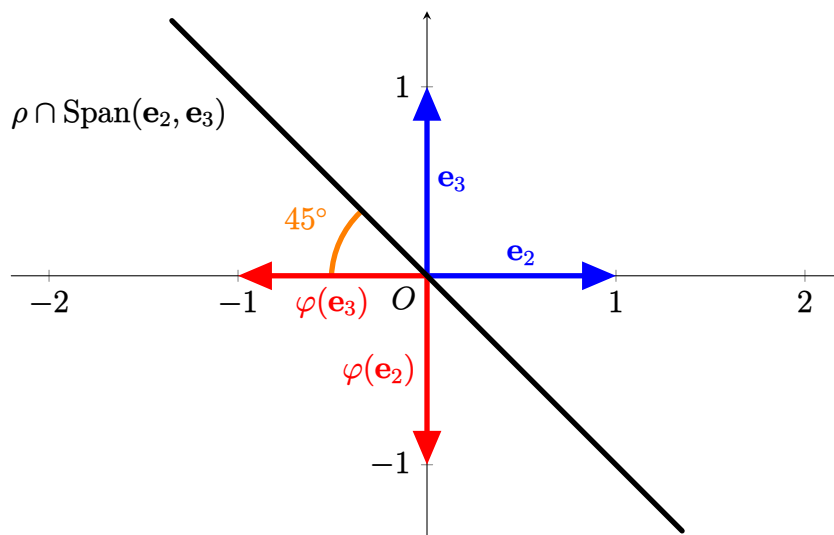
$$P_{\alpha, \epsilon} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{1}{2} \\ 0 & \frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

Pak $B = \varphi_{\epsilon, \epsilon} = P_{\epsilon, \alpha} \cdot \varphi_{\alpha, \alpha} \cdot P_{\alpha, \epsilon}$.

$$B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{1}{2} \\ 0 & \frac{1}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix} \quad \triangle$$

Geometrické řešení. Zjistíme, co dělá φ s vektory standardní báze. Rovina ρ obsahuje osu x_1 a s osami x_2 a x_3 svírá úhel 45° . Na obrázku 2.1 je vidět průřez $\mathbb{R}^3$ rovinou os y a z , na obrázku 2.2 je pak 3-D anaglyf situace. Z obrázků je zřejmé, že $\varphi(\mathbf{e}_1) = \mathbf{e}_1$, $\varphi(\mathbf{e}_2) = -\mathbf{e}_3$ a $\varphi(\mathbf{e}_3) = -\mathbf{e}_2$. Díky tomuto vyjádření máme rovnou matici $B = \varphi_{\epsilon, \epsilon}$.

$$B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix} \quad \triangle$$



Obrázek 2.1: Průřez $\mathbb{R}^3$ rovinou os x_2 a x_3 , tj. osa x_1 i rovina ρ je kolmá na obrázek. Odtud je vidět, že φ zobrazí $\mathbf{e}_2$ na $-\mathbf{e}_3$ a $\mathbf{e}_3$ na $-\mathbf{e}_2$.

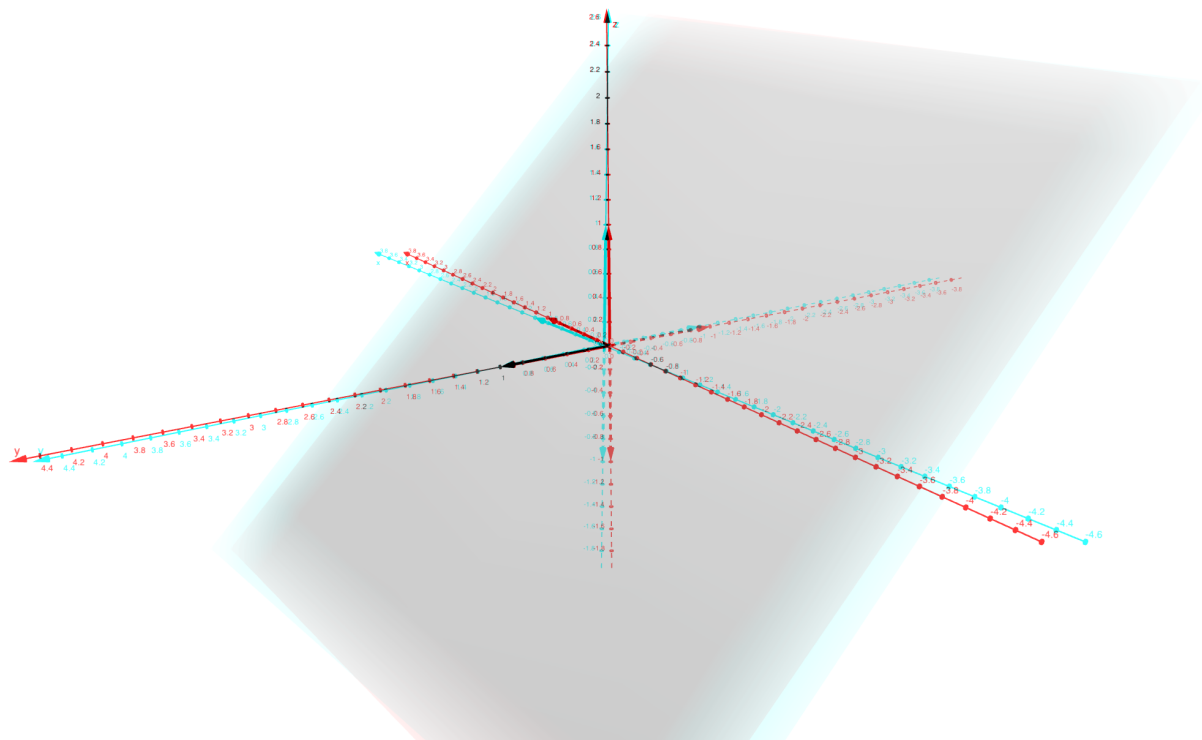
2.2 Vlastní čísla a vektory

Příklad 2.2.1. Najděte vlastní čísla a vlastní vektory zobrazení $\varphi: \mathbb{R}^2 \rightarrow \mathbb{R}^2$

$$\varphi(\mathbf{x}) = \begin{pmatrix} 2 & 1 \\ 3 & 0 \end{pmatrix} \cdot \mathbf{x}.$$

Řešení. Nejprve si připomeneme vlastní čísla a vektory. Číslo λ je *vlastním číslem* zobrazení φ , jestliže existuje nenulový vektor $\mathbf{u}$ takový, že

$$\varphi(\mathbf{u}) = \lambda \cdot \mathbf{u}.$$



Obrázek 2.2: Anaglyf zachycující celkovou situaci. Rovina ρ je zakreslena šedě. Osy x_1 , x_2 a x_3 jsou popsány x , y , resp. z . Vektory standardní báze jsou značeny plnými šipkami. Přerušované šipky značí obrazy vektorů. Vektor v ose x se zobrazí na sebe, jelikož leží v rovině ρ . Vektor v ose y se překlápí na záporný vektor v ose z a analogicky se vektor v ose z zobrazí na záporný vektor v ose y .

To nastane právě tehdy, když $\varphi(\mathbf{u}) - \lambda \cdot \mathbf{u} = \mathbf{o}$, tedy pokud

$$(\varphi - \lambda \cdot \text{id})(\mathbf{u}) = \mathbf{o}, \quad (2.3)$$

což nastane pro nějaký nenulový vektor $\mathbf{u}$ právě tehdy, když $\varphi - \lambda \cdot \text{id}$ je singulární. Je-li φ zadané maticí A , nastane to právě tehdy, je-li

$$\det(A - \lambda E) = 0. \quad (2.4)$$

Hledáme-li vlastní čísla matice A , spočítáme determinant (2.4), což bude polynom v λ , nazývaný *charakteristický polynom* matice A . Vlastní čísla budou právě kořeny charakteristického polynomu. Násobnost kořenů se nazývá *algebraickou násobností* vlastních čísel. Jim příslušné vlastní vektory pak budou nenulová řešení rovnice (2.3). Jako množina řešení homogenní soustavy rovnic tvoří vlastní vektory *vektorový podprostor*. Jeho dimenze se nazývá *geometrickou násobností* onoho vlastního čísla, která je ohraničena zdola 1 a shora algebraickou násobností. Navíc, je-li $\mathbf{u}$ vlastní vektor příslušný λ a zároveň μ , pak z

$$\lambda \cdot \mathbf{u} = \mu \cdot \mathbf{u}$$

a z nenulovosti $\mathbf{u}$ plyne $\lambda = \mu$, tedy průniky vlastních podprostorů jsou triviální. (Obsahují pouze nulový vektor.)

Přejdeme k řešení úlohy. Počítáme determinant matice 2×2 , což můžeme dělat přímo z definice (1.14).

$$\det \begin{pmatrix} 2-\lambda & 1 \\ 3 & -\lambda \end{pmatrix} = (2-\lambda)(-\lambda) - 3 = \lambda^2 - 2\lambda - 3 = (\lambda - 3)(\lambda + 1)$$

Vidíme, že máme vlastní čísla $\lambda_1 = 3$ a $\lambda_2 = -1$, obě s algebraickou násobností 1. Počítejme vlastní vektory pro λ_1 .

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

Vidíme, že vlastním vektorem je například $\mathbf{v}_1 = (1, 1)^T$ a všechny jeho nenulové násobky. Počítejme vlastní vektory pro λ_2 .

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

Vlastními vektory jsou nenulové násobky vektoru $\mathbf{v}_2 = (1, -3)^T$. Geometrická násobnost obou vlastních čísel je 1. $\triangle$

Příklad 2.2.2. Najděte vlastní čísla a vlastní vektory zobrazení $\varphi: \mathbb{R}^2 \rightarrow \mathbb{R}^2$

$$\varphi(\mathbf{x}) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.$$

Algebraické řešení. Počítejme determinant.

$$\det \begin{pmatrix} -\lambda & -1 \\ 1 & -\lambda \end{pmatrix} = \lambda^2 + 1$$

Vidíme, že zobrazení φ nemá reálná vlastní čísla, tedy ani vlastní vektory.

Jako zobrazení $\mathbb{C}^2 \rightarrow \mathbb{C}^2$ má φ vlastní čísla $\pm i$. Vlastní vektory příslušné k i jsou nenulová řešení soustavy

$$\begin{pmatrix} -i & -1 \\ 1 & -i \end{pmatrix} \sim \begin{pmatrix} 1 & -i \\ 0 & 0 \end{pmatrix},$$

tedy nenulové násobky $\mathbf{v}_1 = (i, 1)^T$. Vlastní vektory příslušné k $-i$ jsou nenulová řešení soustavy

$$\begin{pmatrix} i & -1 \\ 1 & i \end{pmatrix} \sim \begin{pmatrix} 1 & i \\ 0 & 0 \end{pmatrix},$$

nenulové násobky $\mathbf{v}_1 = (1, i)^T$. $\triangle$

Geometrické řešení. Vlastní vektory příslušné vlastnímu číslu λ jsou takové, vůči kterým se φ chová jako *stejnolehlost* podle počátku s koeficientem λ . Vidíme, že naše zobrazení je *rotací* o $+90^\circ$ podle počátku, které se jako *stejnolehlost* chová pouze pro nulový vektor. Zobrazení φ tedy nemá vlastní vektory ani vlastní čísla. $\triangle$

Příklad 2.2.3. Najděte vlastní čísla a vlastní vektory matice

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

Řešení. Počítáme determinant Laplaceovým rozvojem podle prvního řádku.

$$\begin{aligned} \det \begin{pmatrix} 2-\lambda & 1 & 0 \\ -1 & -\lambda & 3 \\ 1 & 1 & 1-\lambda \end{pmatrix} &= (2-\lambda) \cdot \det \begin{pmatrix} -\lambda & 3 \\ 1 & 1-\lambda \end{pmatrix} - \det \begin{pmatrix} -1 & 3 \\ 1 & 1-\lambda \end{pmatrix} \\ &= (2-\lambda)(\lambda^2 - \lambda - 3) - (\lambda - 1 - 3) \\ &= 2\lambda^2 - 2\lambda - 6 - \lambda^3 + \lambda^2 + 3\lambda - \lambda + 4 \\ &= -\lambda^3 + 3\lambda^2 - 2 = (1-\lambda)(\lambda^2 - 2\lambda - 2) \end{aligned}$$

Máme vlastní číslo $\lambda_1 = 1$. Zbývající vlastní čísla určíme pomocí diskriminantu $D = 4 + 8 = 12$, pak

$$\lambda_{2,3} = \frac{2 \pm 2\sqrt{3}}{2} = 1 \pm \sqrt{3}.$$

Počítejme vlastní vektory pro $\lambda_1 = 1$.

$$B - E = \begin{pmatrix} 1 & 1 & 0 \\ -1 & -1 & 3 \\ 1 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Máme vlastní vektor $\mathbf{v}_1 = (1, -1, 0)^T$ (a jeho nenulové násobky). Počítejme vlastní vektory pro $\lambda_2 = 1 + \sqrt{3}$.

$$B - (1 + \sqrt{3})E = \begin{pmatrix} 1 - \sqrt{3} & 1 & 0 \\ -1 & -1 - \sqrt{3} & 3 \\ 1 & 1 & -\sqrt{3} \end{pmatrix}$$

Ke druhému řádku přičteme $\sqrt{3}$ -násobek třetího.

$$\sim \begin{pmatrix} 1 - \sqrt{3} & 1 & 0 \\ -1 + \sqrt{3} & -1 & 0 \\ 1 & 1 & -\sqrt{3} \end{pmatrix}$$

První řádek přičteme ke druhému a odečteme jej od třetího.

$$\sim \begin{pmatrix} 1-\sqrt{3} & 1 & 0 \\ 0 & 0 & 0 \\ \sqrt{3} & 0 & -\sqrt{3} \end{pmatrix} \sim \begin{pmatrix} 1-\sqrt{3} & 1 & 0 \\ -1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Vlastními vektory jsou nenulové násobky $\mathbf{v}_2 = (1, \sqrt{3} - 1, 1)^T$. Nakonec počítejme vlastní vektory pro $\lambda_3 = 1 - \sqrt{3}$.

$$B - (1 - \sqrt{3})E = \begin{pmatrix} 1 + \sqrt{3} & 1 & 0 \\ -1 & -1 + \sqrt{3} & 3 \\ 1 & 1 & \sqrt{3} \end{pmatrix}$$

Od druhého řádku odečteme $\sqrt{3}$ -násobek třetího.

$$\sim \begin{pmatrix} 1 + \sqrt{3} & 1 & 0 \\ -1 - \sqrt{3} & -1 & 0 \\ 1 & 1 & \sqrt{3} \end{pmatrix}$$

První řádek přičteme ke druhému a odečteme jej od třetího.

$$\sim \begin{pmatrix} 1 + \sqrt{3} & 1 & 0 \\ 0 & 0 & 0 \\ -\sqrt{3} & 0 & \sqrt{3} \end{pmatrix} \sim \begin{pmatrix} 1 + \sqrt{3} & 1 & 0 \\ -1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Vlastními vektory jsou nenulové násobky $\mathbf{v}_3 = (1, -1 - \sqrt{3}, 1)^T$.

△

Příklad 2.2.4. Zjistěte, zda v $\mathbb{R}^3$ existuje báze tvořená vlastními vektory matice

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

Pokud ano, najděte ji.

Řešení. Báze tvořená vlastními vektory existuje, pokud

- charakteristický polynom má plný počet kořenů v $\mathbb{R}$ a²
- geometrická násobnost každého vlastního čísla je rovna té algebraické.

²Případně v daném tělese. Zejména pro $\mathbb{C}$ tato podmínka odpadá.

Pak totiž můžeme vybrat bázi pro každý podprostor vlastních vektorů a tyto vektory dohromady dají bázi celého prostoru. Počítejme proto vlastní čísla.

$$\begin{aligned}\det(C - \lambda E) &= \det \begin{pmatrix} -\lambda & -1 & 2 \\ 3 & 4 - \lambda & -2 \\ 3 & 1 & 1 - \lambda \end{pmatrix} = \\ &= -\lambda \det \begin{pmatrix} 4 - \lambda & -2 \\ 1 & 1 - \lambda \end{pmatrix} - (-1) \det \begin{pmatrix} 3 & -2 \\ 3 & 1 - \lambda \end{pmatrix} + 2 \det \begin{pmatrix} 3 & 4 - \lambda \\ 3 & 1 \end{pmatrix} = \\ &= \lambda ((4 - \lambda)(1 - \lambda) + 2) + (3 - 3\lambda + 6) + 2(3 - 12 + 3\lambda) = \\ &= -\lambda^3 + 5\lambda^2 - 6\lambda + 9 - 3\lambda - 18 + 6\lambda = \\ &= -\lambda^3 + 5\lambda^2 - 3\lambda - 9 = -(\lambda + 1)(\lambda - 3)^2\end{aligned}$$

Máme jednoduché vlastní číslo $\lambda_1 = -1$. Počítejme jemu příslušné vlastní vektory.

$$C + E = \begin{pmatrix} 1 & -1 & 2 \\ 3 & 5 & -2 \\ 3 & 1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & -1 & 2 \\ 0 & 8 & -8 \\ 0 & 4 & -4 \end{pmatrix} \sim \begin{pmatrix} 1 & -1 & 2 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{pmatrix}$$

Máme vlastní vektor $\mathbf{v}_1 = (1, -1, -1)^T$, který generuje podprostor vlastních vektorů. Vidíme, že algebraická násobnost λ_1 je rovna geometrické, což je u jednoduchých vlastních čísel vždy. Dále máme dvojnásobné vlastní číslo $\lambda_2 = 3$. Počítejme vlastní vektory pro něj.

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

Vidíme, že soustavu řeší vektory $\mathbf{x} = (t, 2s - 3t, s)^T$, $t, s \in \mathbb{R}$. Označme $\mathbf{v}_2 := (1, -3, 0)^T$ a $\mathbf{v}_3 = (0, 2, 1)^T$. Tyto vektory tvoří bázi podprostoru vlastních vektorů příslušných 3, tedy jeho dimenze je 2, stejně jako algebraická násobnost 3. Tudíž $\mathbf{v}_1$, $\mathbf{v}_2$ a $\mathbf{v}_3$ jsou vlastní vektory C , které tvoří bázi $\mathbb{R}^3$. $\triangle$

Příklad 2.2.5. Spočítejte vlastní čísla a vlastní vektory matice

$$D = \begin{pmatrix} 1 & 1 & 2 & 1 \\ 1 & -2 & 1 & -4 \\ 0 & -1 & -1 & -1 \\ -1 & 0 & -1 & 2 \end{pmatrix}.$$

Řešení. Počítejme

$$\det(D - \lambda E) = \det \begin{pmatrix} 1 - \lambda & 1 & 2 & 1 \\ 1 & -2 - \lambda & 1 & -4 \\ 0 & -1 & -1 - \lambda & -1 \\ -1 & 0 & -1 & 2 - \lambda \end{pmatrix}$$

pomocí řádkových úprav. Nejprve ke druhému řádku přičteme čtvrtý.

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

Následně z druhého řádku vytkneme $-2-\lambda$.

$$= (-2-\lambda) \det \begin{pmatrix} 1-\lambda & 1 & 2 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & -1 & -1-\lambda & -1 \\ -1 & 0 & -1 & 2-\lambda \end{pmatrix}$$

Nový druhý řádek použijeme k eliminaci prvků ve druhém sloupci.

$$= (-2-\lambda) \det \begin{pmatrix} 1-\lambda & 0 & 2 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & -1-\lambda & 0 \\ -1 & 0 & -1 & 2-\lambda \end{pmatrix}$$

Nyní použijeme Laplaceův rozvoj podle druhého sloupce.

$$= (-2-\lambda)(-1)^{2+2} \det \begin{pmatrix} 1-\lambda & 2 & 0 \\ 0 & -1-\lambda & 0 \\ -1 & -1 & 2-\lambda \end{pmatrix}$$

Opět použijeme Laplaceův rozvoj, tentokrát podle druhého řádku.

$$= (-2-\lambda)(-1-\lambda)(-1)^{2+2} \det \begin{pmatrix} 1-\lambda & 0 \\ -1 & 2-\lambda \end{pmatrix}$$

Máme dolní trojúhelníkovou matici, takže determinant bude součin prvků na diagonále.

$$= (2+\lambda)(1+\lambda)(2-\lambda)(1-\lambda)$$

Máme vlastní čísla $\lambda_{1,2} = \pm 1$ a $\lambda_{3,4} = \pm 2$. Počítejme vlastní vektory pro $\lambda_1 = 1$.

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

Máme vlastní vektor $\mathbf{v}_1 = (1, -1, 0, 1)^T$. Počítejme vlastní vektory pro $\lambda_2 = -1$.

$$\begin{pmatrix} 2 & 1 & 2 & 1 \\ 1 & -1 & 1 & -4 \\ 0 & -1 & 0 & -1 \\ -1 & 0 & -1 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 1 & -3 \\ 0 & 1 & 0 & 7 \\ 0 & -1 & 0 & -1 \\ 0 & -1 & 0 & -1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 1 & -3 \\ 0 & 1 & 0 & 7 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Máme vlastní vektor $\mathbf{v}_2 = (1, 0, -1, 0)^T$. Počítejme vlastní vektory pro $\lambda_3 = 2$.

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

Máme vlastní vektor $\mathbf{v}_3 = (0, 1, 0, -1)^T$. Počítejme vlastní vektory pro $\lambda_4 = -2$.

$$\begin{pmatrix} 3 & 1 & 2 & 1 \\ 1 & 0 & 1 & -4 \\ 0 & -1 & 1 & -1 \\ -1 & 0 & -1 & 4 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & -1 & 13 \\ 1 & 0 & 1 & -4 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & -4 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Máme vlastní vektor $\mathbf{v}_4 = (1, -1, -1, 0)^T$. $\triangle$

2.3 Afinní geometrie

Příklad 2.3.1. Zopakujte definici skalárního součinu v $\mathbb{R}^2$ a v $\mathbb{R}^3$.

Řešení. Standardní skalární součin vektorů $\mathbf{x} = (x_1, \dots, x_n)$ a $\mathbf{y} = (y_1, \dots, y_n) \in \mathbb{R}^n$ definujeme jako

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^n x_i \cdot y_i. \quad (2.5)$$

Zejména v $\mathbb{R}^2$ máme $\langle \mathbf{x}, \mathbf{y} \rangle = x_1 y_1 + x_2 y_2$; v $\mathbb{R}^3$ pak $\langle \mathbf{x}, \mathbf{y} \rangle = x_1 y_1 + x_2 y_2 + x_3 y_3$.

Oobecně v $\mathbb{R}^n$ platí $\langle \mathbf{x}, \mathbf{x} \rangle \geq 0$.³ Můžeme definovat *velikost vektoru* jako

$$\|\mathbf{x}\| = \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle}. \quad (2.6)$$

Velikost (2.6) je definována jednoznačně pro všechny vektory jako jediná nezáporná odmocnina. *Vzdálenost dvou vektorů* pak definujeme jako $\|\mathbf{x} - \mathbf{y}\|$. *Odchylku* dvou nenulových vektorů definujeme pomocí (2.5) a (2.6) pomocí

$$\cos |\angle \mathbf{x}, \mathbf{y}| = \frac{\langle \mathbf{x}, \mathbf{y} \rangle}{\|\mathbf{x}\| \cdot \|\mathbf{y}\|}. \quad (2.7)$$

³Totéž platí pro komplexní prostory. Na $\mathbb{C}^n$ definujeme skalární součin vektorů podobně jako (2.5), ovšem klademe $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^n x_i \cdot \overline{y_i}$. Pak vidíme, že opět $\langle \mathbf{x}, \mathbf{x} \rangle \geq 0$.

Úhel $|\angle \mathbf{x}\mathbf{y}| \in [0, \pi]$ je jednoznačně určen (2.7). Kolmost dvou vektorů můžeme definovat i bez znalosti kosinu. Kolmost dvou (ne nutně nenulových) vektorů definujeme pomocí

$$\mathbf{x} \perp \mathbf{y} \iff \langle \mathbf{x}, \mathbf{y} \rangle = 0. \quad (2.8)$$

Vidíme, že jakýkoli vektor je kolmý na nulový vektor. Navíc, jelikož je díky definici skalární součin s pevným vektorem lineární zobrazení, tak je-li vektor kolmý na množinu jiných vektorů, je kolmý na celý podprostor jimi generovaný. *Ortogonalní doplněk* množiny $M \subseteq V$ ve vektorovém prostoru V definujeme jako

$$M^\perp = \{\mathbf{x} \in V \mid (\forall \mathbf{m} \in M)(\mathbf{x} \perp \mathbf{m})\}. \quad (2.9)$$

Ortogonalní doplněk množiny je stejný jako doplněk podprostoru jí generovaného. Chceme-li tedy určit orthogonalní doplněk nějakého podprostoru, stačí určit doplněk libovolné jeho generující množiny, nebo nějaké jeho báze. Stejně tak je orthogonalní doplněk nějaké množiny vektorový podprostor. Ke hledání kolmých vektorů v $\mathbb{R}^2$ lze použít jednoduché pozorování: vektor $(-x_2, x_1)$ je kolmý na (x_1, x_2) . $\triangle$

Příklad 2.3.2. Napište nejdříve parametrický a potom implicitní popis nejmenšího afinního podprostoru v $\mathcal{A}_3$, který obsahuje body $A = [5, 2, 1]$, $B = [4, 1, 0]$, a $C = [-3, 1, 0]$.

Řešení. Spočítejme si vektory $\overrightarrow{AB} = B - A = (-1, -1, -1)$ a $\overrightarrow{AC} = C - A = (-8, -1, -1)$. Vidíme, že jsou lineárně nezávislé, *afinním obalem* bodů A, B, C (jak se takový prostor nazývá) bude rovina zadaná parametrickou rovnicí

$$A + t \cdot \overrightarrow{AB} + s \cdot \overrightarrow{AC} = [5, 2, 1] + t \cdot (-1, -1, -1) + s \cdot (-8, -1, -1),$$

$s, t \in \mathbb{R}$. Pro implicitní popis potřebujeme najít vektor $\mathbf{n}$ kolmý na oba vektory $\overrightarrow{AB}$ i $\overrightarrow{AC}$ (vzhledem ke standardnímu skalárnímu součinu). Vidíme, že můžeme vzít například $\mathbf{n} = (0, 1, -1)$. Zadávací rovnice pak bude

$$x_2 - x_3 = 1,$$

kde koeficienty na levé straně jsou složky vektoru $\mathbf{n}$ a pravou stranu jsme získali dosazením bodu A . Skutečně pro body roviny, parametrizované jako $[5 - s - 8t, 2 - s - t, 1 - s - t]$ platí

$$2 - s - t - 1 + s + t = 1. \quad \triangle$$

Příklad 2.3.3. Najděte průnik rovin $\mathcal{M}$ a $\mathcal{N}$ v $\mathcal{A}_3$ zadaných parametricky

$$\begin{aligned} \mathcal{M} &= \{[2, 3, 4] + a \cdot (1, 1, 1) + b \cdot (0, 0, 1) \in \mathcal{A}_3 \mid a, b \in \mathbb{R}\}, \\ \mathcal{N} &= \{[2, 2, 4] + c \cdot (1, 0, 1) + d \cdot (2, 0, 1) \in \mathcal{A}_3 \mid c, d \in \mathbb{R}\}. \end{aligned}$$

Řešení. Je výhodné mít jednu rovinu zadanou implicitně, kupříkladu rovinu $\mathcal{M}$. Najdeme normálový vektor $\mathbf{m}$, který je kolmý na vektory $(1, 1, 1)$ a $(0, 0, 1)$. Celkem snadno se vidí,

že můžeme vzít $\mathbf{m} = (1, -1, 0)$. (Normálový vektor $\mathcal{M}$ není kolmý na směrové vektory $\mathcal{N}$. Roviny jsou proto různoběžné.) Máme zadávající rovnici pro rovinu $\mathcal{M}$, kde pravou stranu jsme získali dosazením bodu $[2, 3, 4]$.

$$x_1 - x_2 = -1 \quad (2.10)$$

Body roviny $\mathcal{N}$ máme vyjádřeny parametricky.

$$\begin{aligned} x_1 &= 2 + c + 2d \\ x_2 &= 2 \\ x_3 &= 4 + c + d \end{aligned} \quad (2.11)$$

Dosazením (2.11) do (2.10) dostaneme rovnici pro parametry c a d , kterou vyřešíme například vůči c .

$$\begin{aligned} 2 + c + 2d - 2 &= -1 \\ c &= -1 - 2d \end{aligned}$$

Parametrické vyjádření průniku získáme dosazením $c = -1 - 2d$ do (2.11), čímž získáme parametrické vyjádření průsečnice rovin $\mathcal{M}$ a $\mathcal{N}$.

$$\begin{aligned} \mathcal{M} \cap \mathcal{N} &= \{[2, 2, 4] - (1 + 2d) \cdot (1, 0, 1) + d \cdot (2, 0, 1)\} \\ &= \{[1, 2, 3] - d \cdot (0, 0, 1)\} \end{aligned} \quad \triangle$$

Příklad 2.3.4. V $\mathcal{A}_3$ určete vzájemnou polohu rovin

$$\rho = \{[3, -1, 0] + s \cdot (-1, 1, 1) + t \cdot (2, 1, 0) \in \mathcal{A}_3 \mid s, t \in \mathbb{R}\}$$

a přímek p , q a r , které mají parametrická vyjádření

$$\text{a) } p = \{[7, 4, 2] + a \cdot (5, -2, -3) \in \mathcal{A}_3 \mid a \in \mathbb{R}\},$$

$$\text{b) } q = \{[1, 2, 3] + b \cdot (1, 5, 3) \in \mathcal{A}_3 \mid b \in \mathbb{R}\},$$

$$\text{c) } r = \{[1, 2, 3] + c \cdot (1, 1, 1) \in \mathcal{A}_3 \mid c \in \mathbb{R}\}.$$

Řešení. Než začneme se samotným řešením, bude výhodné si vyjádřit ρ implicitně. Vidíme, že normálový vektor je například $\mathbf{n} = (1, -2, 3)$. (Je jistě kolmý na $(2, 1, 0)$, třetí souřadnici dopočítáme tak, aby byl kolmý i na $(-1, 1, 1)$.) Dosazením bodu $[3, -1, 0]$ získáme zadávající rovnici pro ρ .

$$x - 2y + 3z = 5 \quad (2.12)$$

Začneme řešením a). Parametrizaci p dosadíme do (2.12). Na levé straně máme

$$7 + 5a - 2(4 - 2a) + 3(2 - 3a) = 7 + 5a - 8 + 4a + 6 - 9a = 5,$$

zatímco na pravé straně máme 5. Rovnice je splněna vždy a proto $p \subseteq \rho$. Skutečně, směrový vektor p je kolmý na $\mathbf{n}$ a proto jej lze vyjádřit jako lineární kombinaci směrových vektorů ρ

$$(5, -2, -3) = (2, 1, 0) - 3 \cdot (-1, 1, 1)$$

a bod $[7, 4, 2] \in \rho$, neboť splňuje zadávající rovnici ρ (jako všechny body p).

V b) dostaneme po dosazení na pravé straně opět 5, na levé pak

$$1 + b - 2(2 + 5b) + 3(3 + 3b) = 6,$$

tudíž rovnice nemá řešení, neexistuje průnik a q a ρ jsou rovnoběžné. Skutečně, směrový vektor q je kolmý na $\mathbf{n}$, lze jej tedy vyjádřit jako lineární kombinací směrových vektorů ρ .

$$(1, 5, 3) = 3 \cdot (-1, 1, 1) + 2 \cdot (2, 1, 0)$$

Bod $[1, 2, 3]$ však nepatří do ρ , neboť nesplňuje (2.12).

Část c) řešíme stejně, dosazením parametrického vyjádření r do (2.12). Na pravé straně máme 5, na levé pak

$$1 + c - 2(2 + c) + 3(3 + c) = 1 + c - 4 - 2c + 9 + 3c = 6 + 2c.$$

Porovnáním dostaneme rovnici

$$2c = -1,$$

tedy průnikem bude jediný bod, průsečík P se souřadnicemi

$$P = [1, 2, 3] - \frac{1}{2} \cdot (1, 1, 1) = \left[\frac{1}{2}, \frac{3}{2}, \frac{5}{2}\right]$$

a r a ρ jsou různoběžné. △

Příklad 2.3.5. V $\mathcal{A}_3$ určete vzájemnou polohu přímky p a roviny ρ , přičemž přímka p je zadána implicitně rovnicemi

$$\begin{array}{rrcrcl} 3x_1 & + & x_2 & + & 2x_3 & = & 5 \\ 5x_1 & - & x_2 & & & = & 3 \end{array}$$

a rovina ρ je zadána parametricky.

$$\rho = \{[-3, 0, 0] + a \cdot (3, 1, 2) + b \cdot (5, -1, 0) \in \mathcal{A}_3 \mid a, b \in \mathbb{R}\}$$

Řešení. Zadávající rovnice přímky p říkají, že vektory $\mathbf{u}_1 = (3, 1, 2)$ a $\mathbf{u}_2 = (5, -1, 0)$ jsou kolmé na p . Tyto vektory jsou ovšem směrovými vektory roviny ρ . Proto nutně musí být $p \perp \rho$, tedy budou p a ρ různoběžné a bude existovat jediný průsečík. Spočítejme jej dvěma způsoby.

Jednou možností je zjistit implicitní zadání roviny ρ . Normálový vektor $\mathbf{n}$ bude kolmý na oba směrové vektory $\mathbf{u}_1$ a $\mathbf{u}_2$. Je zřejmé, že každý vektor $(1, 5, z)$ bude kolmý na $\mathbf{u}_2$. Hodnotu

z zjistíme pomocí skalárního součinu s $\mathbf{u}_1$, který musí dát nulu. Vidíme, že $\mathbf{n} = (1, 5, -4)$. Dosazením bodu $[-3, 0, 0]$ získáme zadávající rovnici.

$$x_1 + 5x_2 - 4x_3 = -3$$

Průsečík P bude ležet v průniku, bude tedy vyhovovat všem třem rovnicím. Jeho hledání se tedy redukuje na řešení soustavy rovnic. V maticovém tvaru ji řešíme pomocí Gaußovy eliminace s výběrem pivotu.

$$\begin{aligned} \left(\begin{array}{ccc|c} 3 & 1 & 2 & 5 \\ 5 & -1 & 0 & 3 \\ 1 & 5 & -4 & -3 \end{array} \right) &\sim \left(\begin{array}{ccc|c} 8 & 0 & 2 & 8 \\ 5 & -1 & 0 & 3 \\ 26 & 0 & -4 & 12 \end{array} \right) \sim \left(\begin{array}{ccc|c} 4 & 0 & 1 & 4 \\ 5 & -1 & 0 & 3 \\ 21 & 0 & 0 & 14 \end{array} \right) \sim \\ &\sim \left(\begin{array}{ccc|c} 12 & 0 & 3 & 12 \\ -15 & 3 & 0 & -9 \\ 3 & 0 & 0 & 2 \end{array} \right) \sim \left(\begin{array}{ccc|c} 0 & 0 & 3 & 4 \\ 0 & 3 & 0 & 1 \\ 3 & 0 & 0 & 2 \end{array} \right) \end{aligned}$$

Vidíme, že $P = \left[\frac{2}{3}, \frac{1}{3}, \frac{4}{3} \right]$.

Druhým způsobem řešení je dosadit parametrické vyjádření ρ do zadávajících rovnic p . Tím získáme soustavu dvou rovnic pro dva neznámé parametry.

$$\begin{aligned} 3(-3 + 3a + 5b) + (a - b) + 2(2a) &= 5 \\ 5(-3 + 3a + 5b) - (a - b) &= 3 \end{aligned}$$

Úpravou výrazů dostaneme následující soustavu.

$$\begin{aligned} 14a + 14b &= 14 \\ 14a + 26b &= 18 \end{aligned}$$

Tuto soustavu řešíme po zkrácení v maticovém zápisu pomocí Gaußovy eliminace.

$$\left(\begin{array}{cc|c} 1 & 1 & 1 \\ 7 & 13 & 9 \end{array} \right) \sim \left(\begin{array}{cc|c} 1 & 1 & 1 \\ 0 & 6 & 2 \end{array} \right) \sim \left(\begin{array}{cc|c} 3 & 0 & 2 \\ 0 & 3 & 1 \end{array} \right)$$

Vidíme, že musíme vzít $a = \frac{2}{3}$ a $b = \frac{1}{3}$. Dosazením do parametrického vyjádření ρ získáme souřadnice průsečíku.

$$P = [-3, 0, 0] + \frac{2}{3} \cdot (3, 1, 2) + \frac{1}{3} \cdot (5, -1, 0) = \left[\frac{2}{3}, \frac{1}{3}, \frac{4}{3} \right] \quad \triangle$$

Příklad 2.3.6. Určete příčku mimoběžek

$$\begin{aligned} p &= \{[1, 2, 0] + a \cdot (1, -1, 1) \in \mathcal{A}_3 \mid a \in \mathbb{R}\}, \\ q &= \{[0, 9, -2] + b \cdot (1, 0, 0) \in \mathcal{A}_3 \mid b \in \mathbb{R}\} \end{aligned}$$

takovou, že přímka jí určená prochází bodem $[1, -7, 4]$.

Řešení. Označme $A = [1, 2, 0]$, $B = [0, 9, -2]$ a $C = [1, -7, 4]$; $\mathbf{u} = (1, -1, 1)$ a standardně $\mathbf{e}_1 = (1, 0, 0)$. Příčka bude jistě obsažena v rovině ρ určené přímkou p a bodem C . Rovinu ρ můžeme zadat parametricky pomocí bodu a směrového vektoru p a druhého vektoru $\overrightarrow{AC}$.

$$\rho = \{A + a \cdot \mathbf{u} + c \cdot \overrightarrow{AC} \in \mathcal{A}_3 \mid a, c \in \mathbb{R}\}$$

Chceme najít implicitní zadání ρ . Vektor $\overrightarrow{AC}$ je $(0, -9, 4)$. Je zřejmé, že vektory $(x_1, 4, 9)$ na něj budou kolmé. První složku získáme pomocí skalárního součinu s $\mathbf{u}$. Máme tak $\mathbf{n} = (-5, 4, 9)$. Dosazením bodu A získáme rovnici zadávající ρ .

$$-5x_1 + 4x_2 + 9x_3 = 3 \quad (2.13)$$

Dosazením bodů přímky q do (2.13) získáme rovnici pro b , kterou vyřešíme.

$$\begin{aligned} -5b + 9 \cdot 9 - 9 \cdot 2 &= 3 \\ -5b + 18 &= 3 \\ -5b &= -15 \\ b &= 3 \end{aligned}$$

Průsečíkem ρ a q bude bod $Q = [3, 9, -2]$. Přímka r tak bude určena body C a Q . Máme její parametrické vyjádření.

$$\begin{aligned} r &= \{C + t \cdot \overrightarrow{CQ} \in \mathcal{A}_3 \mid t \in \mathbb{R}\} \\ &= \{[1, -7, 4] + t \cdot (2, 15, -6) \in \mathcal{A}_3 \mid t \in \mathbb{R}\} \end{aligned}$$

Průnik $P := p \cap r \neq \emptyset$, protože $r \subseteq \rho \supseteq p$ a jejich směrové vektory jsou lineárně nezávislé. Chceme-li zjistit pouze přímku r , jsme hotovi. Příčkou mimoběžek však někdy rozumíme pouze úsečku spojující jejich některé body. Pokud chceme nalézt tuto úsečku, musíme zjistit P . Postupujeme stejně jako u Q . Přímka r je průsečnicí roviny ρ a roviny σ , zadané bodem C a směrovými vektory $\mathbf{e}_1$ a $\overrightarrow{BC} = (1, -16, 6)$. Za normálový vektor můžeme vzít například $(0, 3, 8)$ a rovnici zadávající σ získáme dosazením C .

$$3x_2 + 8x_3 = 11 \quad (2.14)$$

Dosazením parametrizace p do (2.14) dostaneme rovnici pro a .

$$\begin{aligned} 3(2 - a) + 8a &= 11 \\ 5a &= 5 \\ a &= 1 \end{aligned}$$

Vidíme, že pak $P = [2, 1, 1]$ a máme parametrizaci příčky mimoběžek jako úsečky. Rozdíl je jen v tom, že parametr bereme jen z uzavřeného intervalu.

$$\{P + t \cdot \overrightarrow{PQ} \mid t \in [0, 1]\} \quad \triangle$$

Poznámka. Jinou možností hledání průniku je použít vyjádření vektorů pomocí báze. Průnik musí být vyjádřitelný jak pomocí parametrů roviny ρ , tak pomocí těch pro q . Musí tedy platit

$$A + a \cdot \mathbf{u} + c \cdot \overrightarrow{AC} = B + b \cdot \mathbf{e}_1$$

pro nějaké (jednoznačně určené) hodnoty a , b a c . Převedením dostaneme vektorovou rovnici

$$a \cdot \mathbf{u} + c \cdot \overrightarrow{AC} - b \cdot \mathbf{e}_1 = B - A =: \overrightarrow{AB}.$$

Po složkách dostaneme soustavu tří rovnic o třech neznámých. Řešením obdržíme konkrétní hodnoty a , b a c . Řešením bychom obdrželi rovnou hodnoty a a b , tedy bychom rovnou zjistili P a Q a odtud parametrizaci příčky, ať jako přímky či jako úsečky.

Příklad 2.3.7. Osa dvou mimoběžných přímek p a q v afinním prostoru $\mathcal{A}_3$ je přímka, která obě přímky protíná a je na ně kolmá. Najděte osu mimoběžek

$$\begin{aligned} p &= \{[1, 2, 3] + a \cdot (1, 2, -1) \in \mathcal{A}_3 \mid a \in \mathbb{R}\} \\ q &= \{[2, -3, 4] + b \cdot (2, -1, -2) \in \mathcal{A}_3 \mid b \in \mathbb{R}\} \end{aligned}$$

a body $P \in p$ a $Q \in q$, ve kterých tyto přímky protíná.

Řešení. Označme $A = [1, 2, 3]$, $B = [2, -3, 4]$, $\mathbf{u} = (1, 2, -1)$ a $\mathbf{v} = (2, -1, -2)$. Osa bude určena body $P \in p$ a $Q \in q$. Ty budou mít souřadnice

$$P = [1 + a, 2 + 2a, 3 - a] \quad Q = [2 + 2b, -3 - b, 4 - 2b] \quad (2.15)$$

pro nějaká a a b . Směrový vektor osy bude

$$\overrightarrow{PQ} = (1 + 2b - a, -5 - b - 2a, 1 - 2b + a). \quad (2.16)$$

Hodnoty a , b určíme z podmínek $\overrightarrow{PQ} \perp \mathbf{u}$ a $\overrightarrow{PQ} \perp \mathbf{v}$, což zajistíme pomocí skalárního součinu s těmito vektory, které položíme nule. Dostaneme soustavu lineárních rovnic pro a a b .

$$\begin{aligned} 1 \cdot (1 + 2b - a) + 2 \cdot (-5 - b - 2a) - 1 \cdot (1 - 2b + a) &= 0 \\ 2 \cdot (1 + 2b - a) - 1 \cdot (-5 - b - 2a) - 2 \cdot (1 - 2b + a) &= 0 \end{aligned}$$

Po roznásobení a sečtení výrazů a převedení absolutních členů na druhou stranu dostaneme následující soustavu.

$$\begin{aligned} -6a + 2b &= 10 \\ -2a + 9b &= -5 \end{aligned}$$

Tu řešíme s užitím maticového zápisu Gaußovou eliminací s výběrem pivotu.

$$\left(\begin{array}{cc|c} -3 & 1 & 5 \\ -2 & 9 & -5 \end{array} \right) \sim \left(\begin{array}{cc|c} -3 & 1 & 5 \\ 25 & 0 & -50 \end{array} \right) \sim \left(\begin{array}{cc|c} 0 & 1 & -1 \\ 1 & 0 & -2 \end{array} \right)$$

Máme tedy výsledek: $a = -2$ a $b = -1$. Dosazením do (2.16) dostaneme složky vektoru $\overrightarrow{PQ} = (1, 0, 1)$, dosazením do (2.15) pak souřadnice bodů $P = [-1, -2, 5]$ a $Q = [0, -2, 6]$. Máme i parametrické vyjádření osy.

$$\{[-1, -2, 5] + t \cdot (1, 0, 1) \in \mathcal{A}_3 \mid t \in \mathbb{R}\} \quad \triangle$$

Příklad 2.3.8. Pomocí determinantu určete obsah trojúhelníka $\triangle ABC$ v $\mathcal{A}_2$, kde $A = [1, 3]$, $B = [-2, 101]$, $C = [-8, 11]$. Zjistěte, které ze stran tohoto trojúhelníka jsou vidět z bodu $D = [200, -300]$.

Řešení. Determinant matice, jejímiž sloupci (nebo řádky) budou složky vektorů $\overrightarrow{AB}$, $\overrightarrow{AC}$, bude orientovaným obsahem rovnoběžnostěnu zadaného body A , B , $A + \overrightarrow{AB} + \overrightarrow{AC}$ a C . Znaménko odpovídá pouze orientaci. Polovina absolutní hodnoty tohoto determinantu tak bude odpovídat ploše trojúhelníka. Máme $\overrightarrow{AB} = (-3, 98)$ a $\overrightarrow{AC} = (-9, 8)$. Máme tak i obsah.

$$S_{\triangle ABC} = \frac{1}{2} \cdot \left| \det \begin{pmatrix} -3 & -9 \\ 98 & 8 \end{pmatrix} \right| = \frac{1}{2} \cdot |-3 \cdot 8 + 9 \cdot 98| = \frac{1}{2} \cdot 858 = 429$$

Strana AB je viditelná z D právě tehdy, když báze $\overrightarrow{AB}$, $\overrightarrow{AC}$ je opačně orientovaná než báze $\overrightarrow{AB}$, $\overrightarrow{AD}$. Orientaci poznáme podle znaménka determinantu matice, jejíž sloupce budou složky vektorů. Báze $\overrightarrow{AB}$, $\overrightarrow{AC}$ je kladně orientovaná. Máme vektor $\overrightarrow{AD} = (199, -303)$.

$$\det \begin{pmatrix} -3 & 199 \\ 98 & -303 \end{pmatrix} = 303 \cdot 3 - 199 \cdot 98 = -18\,593$$

Báze $\overrightarrow{AB}$, $\overrightarrow{AD}$ je záporně orientovaná, proto strana AB je z D vidět. Báze $\overrightarrow{AC}$, $\overrightarrow{AB}$ je orientovaná opačně než $\overrightarrow{AB}$, $\overrightarrow{AC}$, tedy záporně. Zjistíme orientaci báze $\overrightarrow{AC}$, $\overrightarrow{AD}$.

$$\det \begin{pmatrix} -9 & 199 \\ 8 & -303 \end{pmatrix} = 9 \cdot 303 - 8 \cdot 199 = 1\,135$$

Báze $\overrightarrow{AC}$, $\overrightarrow{AD}$ je orientována kladně. Proto je i strana AC z bodu D vidět. Strana BC tak být vidět nemůže, protože v rovině lze z jednoho bodu pozorovat maximálně dvě strany trojúhelníka. $\triangle$

2.4 Eukleidovská geometrie

Příklad 2.4.1. V $\mathbb{R}^3$ najděte ortogonální doplněk podprostoru $M = \text{Span}((1, 2, -1), (1, -2, 5))$.

Řešení. Máme podle (2.9)

$$M^\perp = \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid (x_1, x_2, x_3) \perp (1, 2, -1), (x_1, x_2, x_3) \perp (1, -2, 5)\}.$$

Kolmost spočítáme pomocí skalárního součnu (2.5). Dostaneme soustavu rovnic.

$$\begin{array}{rrrrrcl} x_1 & + & 2x_2 & - & x_3 & = & 0 \\ x_1 & - & 2x_2 & + & 5x_3 & = & 0 \end{array}$$

Tuto řešíme pomocí maticového zápisu.

$$\begin{pmatrix} 1 & 2 & -1 \\ 1 & -2 & 5 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & -1 \\ 0 & -4 & 6 \end{pmatrix} \sim \begin{pmatrix} 2 & 4 & -2 \\ 0 & -4 & 6 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 4 \\ 0 & 2 & -3 \end{pmatrix}$$

Máme $x_3 = 2t$, $x_2 = 3t$, $x_1 = -4t$, $t \in \mathbb{R}$. Vidíme, že

$$M^\perp = \text{Span}((-4, 3, 2)). \quad \triangle$$

Příklad 2.4.2. Spočítejte kolmou projekci vektoru $\mathbf{u} = (7, -16, 9)$ do podprostoru M a jeho ortogonálního doplňku $M^\perp$ z předchozího příkladu 2.4.1.

Řešení. Víme, že $M = \text{Span}((1, 2, -1), (1, -2, 5))$ a $M^\perp = \text{Span}((-4, 3, 2))$. Vyjádříme si $\mathbf{u}$ jako lineární kombinaci vektorů $(1, 2, -1)$, $(1, -2, 5)$ a $(-4, 3, 2)$. Dostaneme soustavu rovnic pro koeficienty.

$$\begin{array}{rrrrcl} k_1 & + & k_2 & - & 4k_3 & = & 7 \\ 2k_1 & - & 2k_2 & + & 3k_3 & = & -16 \\ -k_1 & + & 5k_2 & + & 2k_3 & = & 9 \end{array}$$

Tu řešíme v maticovém zápisu Gaußovou eliminací s výběrem pivotu.

$$\begin{pmatrix} 1 & 1 & -4 & | & 7 \\ 2 & -2 & 3 & | & -16 \\ -1 & 5 & 2 & | & 9 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & -4 & | & 7 \\ 0 & -4 & 11 & | & -30 \\ 0 & 6 & -2 & | & 16 \end{pmatrix} \sim \begin{pmatrix} 1 & -11 & 0 & | & -25 \\ 0 & 29 & 0 & | & 58 \\ 0 & -3 & 1 & | & -8 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & | & -3 \\ 0 & 1 & 0 & | & 2 \\ 0 & 0 & 1 & | & -2 \end{pmatrix}$$

Vidíme, že

$$\mathbf{u} = \underbrace{-3 \cdot (1, 2, -1) + 2 \cdot (1, -2, 5)}_{P_M(\mathbf{u})} + \underbrace{(-2) \cdot (-4, 3, 2)}_{P_{M^\perp}(\mathbf{u})}$$

a $P_M(\mathbf{u}) = (-1, -10, 13)$ a $P_{M^\perp}(\mathbf{u}) = (8, -6, -4)$. $\triangle$

Příklad 2.4.3. Necht $\varphi: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ je kolmá projekce na rovinu ρ , zadanou implicitně rovnicí

$$2x_1 - x_2 + 2x_3 = 0.$$

Najděte matici A tvaru 3×3 takovou, že v souřadnicích standardní báze je

$$\varphi(\mathbf{x}) = A \cdot \mathbf{x}.$$

Řešení. Normálový vektor roviny ρ je $\mathbf{n} = (2, -1, 2)$. Za směrové vektory můžeme vzít například $\mathbf{u} = (1, 2, 0)$ a $\mathbf{v} = (0, 2, 1)$. V bázi α tvořené vektory $\mathbf{u}$, $\mathbf{v}$ a $\mathbf{n}$ má φ matici

$$\varphi_{\alpha,\alpha} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Hledáme matici $A = \varphi_{\epsilon,\epsilon}$. Matice přechodu od α k ϵ je

$$P_{\epsilon,\alpha} = \begin{pmatrix} 1 & 0 & 2 \\ 2 & 2 & -1 \\ 0 & 1 & 2 \end{pmatrix}.$$

Opačná matice přechodu $P_{\alpha,\epsilon}$ je matice k ní inverzní. Inverzi spočítáme pomocí determinantů.

Je-li $B = (b_{i,j})_{i,j=1}^n$ invertibilní matice, pak definujeme *matici algebraických doplňků*⁴ $\tilde{B} = (\tilde{b}_{i,j})_{i,j=1}^n$, kde

$$\tilde{b}_{i,j} = (-1)^{i+j} \det B_{i,j},$$

je *algebraický doplněk* $b_{i,j}$ a $\det B_{i,j}$ je determinant matice vzniklé z B vynecháním i -tého řádku a j -tého sloupce. Platí, že

$$B^{-1} = \frac{1}{\det B} \cdot \tilde{B}^T.$$

(Součin i -tého řádku B a j -tého sloupce $\tilde{B}$ dává Laplaceův rozvoj determinantu podle j -tého řádku matice vzniklé z B nahrazením j -tého řádku i -tým. Vidíme, že dostaneme $\det B$ pro $i = j$ a 0 jinak.)

Pomocí Sarrusova pravidla spočítáme $\det P_{\epsilon,\alpha} = 4 + 4 + 0 - 0 - 0 - (-1) = 9$. Pak získáme adjungovanou matici.

$$\tilde{P}_{\epsilon,\alpha} = \begin{pmatrix} 5 & -4 & 2 \\ 2 & 2 & -1 \\ -4 & 5 & 2 \end{pmatrix}$$

Inverze tedy je

$$P_{\alpha,\epsilon} = \frac{1}{9} \cdot \tilde{P}_{\epsilon,\alpha}^T = \frac{1}{9} \cdot \begin{pmatrix} 5 & 2 & -4 \\ -4 & 2 & 5 \\ 2 & -1 & 2 \end{pmatrix}.$$

Pak jednoduše spočítáme $A = \varphi_{\epsilon,\epsilon} = P_{\epsilon,\alpha} \cdot \varphi_{\alpha,\alpha} \cdot P_{\alpha,\epsilon}$.

$$A = \frac{1}{9} \cdot \begin{pmatrix} 5 & -4 & 2 \\ 2 & 2 & -1 \\ -4 & 5 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 5 & 2 & -4 \\ -4 & 2 & 5 \\ 2 & -1 & 2 \end{pmatrix} = \frac{1}{9} \cdot \begin{pmatrix} 5 & 2 & -4 \\ 2 & 8 & 2 \\ -4 & 2 & 5 \end{pmatrix} \quad \triangle$$

⁴Též zvaná *adjungovaná matice*.

Příklad 2.4.4. V $\mathcal{E}_3$ spočítejte vzdálenost bodu $A = [5, 7, 1]$ od roviny ρ zadané implicitně rovnicí

$$x_1 + 3x_2 - 2x_3 + 4 = 0. \quad (2.17)$$

Současně najděte bod $C \in \rho$ takový, že $\text{dist}(A, C) = \text{dist}(A, \rho)$.

Analytické řešení. Zjistíme parametrické vyjádření roviny ρ . Máme normálový vektor $(1, 3, -2)$ a z něj zjistíme směrové vektory, například $(3, -1, 0)$ a $(2, 0, 1)$. Body ρ tedy lze vyjádřit jako

$$X(t, s) = [-4, 0, 0] + t \cdot (3, -1, 0) + s \cdot (2, 0, 1) = [-4 + 3t + 2s, -t, s]$$

pro $t, s \in \mathbb{R}$. Vektory z bodu A do ρ pak lze parametrizovat pomocí

$$\overrightarrow{X(t, s)A} = (9 - 3t - 2s, 7 + t, 1 - s).$$

Snažíme se minimalizovat reálnou funkci $\|\overrightarrow{X(t, s)A}\|$ reálných proměnných t a s . Protože je druhá mocnina rostoucí bijekcí $[0, \infty)$ do sebe, bude se velikost vektoru minimalizovat právě tehdy, když se bude minimalizovat její druhá mocnina. Máme

$$\|\overrightarrow{X(t, s)A}\|^2 = (9 - 3t - 2s)^2 + (7 + t)^2 + (1 - s)^2. \quad (2.18)$$

Zjistíme stacionární body. Derivací (2.18) podle t máme

$$\frac{\partial \|\overrightarrow{X(t, s)A}\|^2}{\partial t} = 2(9 - 3t - 2s)(-3) + 2(7 + t) = 20t + 12s - 40, \quad (2.19)$$

derivací podle s pak

$$\frac{\partial \|\overrightarrow{X(t, s)A}\|^2}{\partial s} = 2(9 - 3t - 2s)(-2) + 2(1 - s)(-1) = 12t + 10s - 38. \quad (2.20)$$

Položíme obě derivace nule. Pak získáme soustavu dvou lineárních rovnic o dvou neznámých, kterou řešíme pomocí maticového zápisu.

$$\begin{aligned} \left(\begin{array}{cc|c} 20 & 12 & 40 \\ 12 & 10 & 38 \end{array} \right) &\sim \left(\begin{array}{cc|c} 5 & 3 & 10 \\ 6 & 5 & 19 \end{array} \right) \sim \left(\begin{array}{cc|c} 5 & 3 & 10 \\ 1 & 2 & 9 \end{array} \right) \sim \\ &\sim \left(\begin{array}{cc|c} 0 & -7 & -35 \\ 1 & 2 & 9 \end{array} \right) \sim \left(\begin{array}{cc|c} 0 & 1 & 5 \\ 1 & 2 & 9 \end{array} \right) \sim \left(\begin{array}{cc|c} 0 & 1 & 5 \\ 1 & 0 & -1 \end{array} \right) \end{aligned}$$

Máme jediný stacionární bod. Zjistíme druhé derivace (2.18) pomocí derivování (2.19) a (2.20).

$$\frac{\partial^2 \|\overrightarrow{X(t, s)A}\|^2}{\partial t^2} = 20$$

$$\frac{\partial^2 \|\overrightarrow{X(t,s)A}\|^2}{\partial t \partial s} = 12$$

$$\frac{\partial^2 \|\overrightarrow{X(t,s)A}\|^2}{\partial s^2} = 10$$

Matice druhých derivací je

$$\begin{pmatrix} 20 & 12 \\ 12 & 10 \end{pmatrix}$$

Její hlavní minory jsou 20 a $20 \cdot 10 - 12^2 = 200 - 144 = 56$, oba kladné, takže je matice pozitivně definitní a ve stacionárním bodě máme lokální minimum. Vzdálenost se tak minimalizuje v bodě

$$X(-1, 5) = [3, 1, 5]$$

a je rovna $\|\overrightarrow{X(-1,5)A}\| = \sqrt{(3-5)^2 + (1-7)^2 + 4^2} = \sqrt{56} = 2\sqrt{14}$. $\triangle$

Poznámka. Jinou možností analytického řešení je vzít obecný bod $X(x_1, x_2, x_3) = [x_1, x_2, x_3]$ a minimalizovat funkci $\|\overrightarrow{AX(x_1, x_2, x_3)}\|$ za podmínky $x_1 + 3x_2 - 2x_3 + 4 = 0$ například metodou Lagrangeových multiplikátorů.

Geometrické řešení. Vzdálenost se minimalizuje v bodě P , který je kolmou projekcí bodu A na rovinu ρ . Normálový vektor roviny je $\mathbf{n} = (1, 3, -2)$. P bude průnikem přímky

$$p = \{A + t \cdot \mathbf{n} \in \mathcal{E}_3 \mid t \in \mathbb{R}\} \quad (2.21)$$

a roviny ρ , tedy bude tvaru (2.21) a bude vyhovovat rovnici (2.17). Dosazením získáme rovnici pro t , kterou vyřešíme.

$$\begin{aligned} (5+t) + 3(7+3t) - 2(1-2t) + 4 &= 0 \\ 5+t + 21+9t - 2+4t &= -4 \\ 14t &= -28 \\ t &= -2 \end{aligned}$$

Máme $P = [3, 1, 5]$ a

$$\text{dist}(A, \rho) = \|\overrightarrow{AP}\| = \sqrt{(3-5)^2 + (1-7)^2 + 4^2} = \sqrt{56} = 2\sqrt{14}. \quad \triangle$$

Příklad 2.4.5. V $\mathcal{E}_3$ spočítejte vzdálenost přímek p a q .

$$\begin{aligned} p &= \{[4, 4, 4] + a \cdot (2, 1, -1) \in \mathcal{E}_3 \mid a \in \mathbb{R}\} \\ q &= \{[1, 15, 12] + b \cdot (1, -2, 1) \in \mathcal{E}_3 \mid b \in \mathbb{R}\}. \end{aligned}$$

Dále najděte body $K \in p$ a $L \in q$, v nichž se vzdálenost přímek realizuje, tj. platí $\text{dist}(K, L) = \text{dist}(p, q)$.

Poznámka. Samozřejmě bychom mohli řešit situaci analyticky. Parametrizovali bychom si body obou přímk a pak minimalizovali vzdálenost jako funkci obou parametrů pomocí hledání stacionárních bodů podobně jako v příkladu 2.4.4. Příklad 2.4.5 již však budeme řešit pouze geometricky.

Řešení. Vzdálenost se bude realizovat na ose mimoběžek. Hledáme ji tedy podobně jako v příkladu 2.3.7. Parametrizujeme si body obou přímk.

$$P = [4 + 2a, 4 + a, 4 - a] \quad Q = [1 + b, 15 - 2b, 12 + b]$$

Máme vektor $\overrightarrow{PQ} = (-3 + b - 2a, 1 - 2b - a, 8 + b + a)$. Vektor $\overrightarrow{PQ}$ musí být kolmý na obě přímky. Skalárním součinem s jejich směrovými vektory získáme rovnice pro parametry a, b .

$$\begin{aligned} 2(-3 + b - 2a) + 11 - 2b - a - 8 - b - a &= 0 \\ -3 + b - 2a - 2(11 - 2b - a) + 8 + b + a &= 0 \end{aligned}$$

Úpravou výrazů získáme následující soustavu.

$$\begin{aligned} a + 6b &= 17 \\ 6a + b &= -3 \end{aligned}$$

Soustavu řešíme pomocí maticového zápisu.

$$\left(\begin{array}{cc|c} 1 & 6 & 17 \\ 6 & 1 & -3 \end{array} \right) \sim \left(\begin{array}{cc|c} -35 & 0 & 35 \\ 6 & 1 & -3 \end{array} \right) \sim \left(\begin{array}{cc|c} 1 & 0 & -1 \\ 0 & 1 & 3 \end{array} \right)$$

Máme tedy $P = [2, 3, 5]$, $Q = [4, 9, 15]$, $\overrightarrow{PQ} = (2, 6, 10)$ a

$$\text{dist}(p, q) = \|\overrightarrow{PQ}\| = \sqrt{4 + 36 + 100} = \sqrt{140} = 2\sqrt{35}. \quad \triangle$$

Příklad 2.4.6. V $\mathcal{E}_3$ určete odchylku roviny ρ od přímky p .

$$\begin{aligned} \rho &= \{[1, 3, 5] + a \cdot (1, 1, 1) + b \cdot (1, 3, 2) \in \mathcal{E}_3 \mid a, b \in \mathbb{R}\} \\ p &= \{[-3, 1, 7] + c \cdot (1, 0, -1) \in \mathcal{E}_3 \mid c \in \mathbb{R}\} \end{aligned}$$

Řešení. Zjistíme si normálový vektor roviny ρ . Musí být kolmý na $(1, 1, 1)$ a $(1, 3, 2)$.

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

Vidíme, že můžeme brát například $\mathbf{n} = (1, 1, -2)$ za normálový vektor. Z obrázku 2.3 vidíme, že stačí počítat odchylku směrového vektoru p a $\mathbf{n}$ a místo arkuskosinu vzít arkussinus (nebo dopočítat do $\frac{\pi}{4}$). Máme

$$\langle \mathbf{n}, (1, 0, -1) \rangle = 1 \cdot 1 + (-1) \cdot (-2) = 3,$$

dále

$$\|\mathbf{n}\| = \sqrt{6}$$

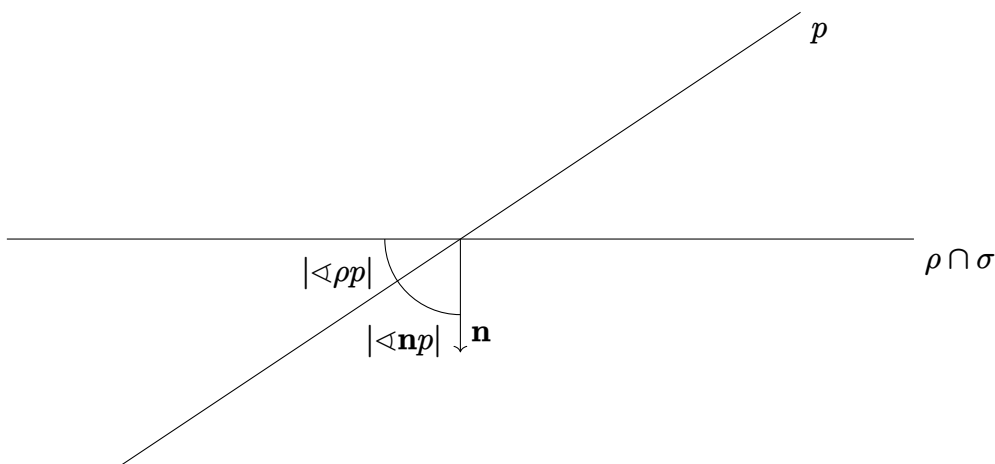
$$\|(1, 0, -1)\| = \sqrt{2}.$$

Pak vidíme, že

$$\sin |\angle \rho p| = \left| \frac{3}{\sqrt{12}} \right| = \frac{3}{2\sqrt{3}} = \frac{\sqrt{3}}{2}$$

a odchylka je $\arcsin \frac{\sqrt{3}}{2} = \frac{\pi}{3}$.

△



Obrázek 2.3: Nákres obrázku v rovině σ kolmé na ρ a obsahující p . Vidíme, že $|\angle \rho p| = \frac{\pi}{4} - |\angle np|$. Proto $\cos |\angle \rho p| = \sin |\angle np|$.

Poznámka. Jinou možností by bylo spočítat si kolmou projekci přímky p do roviny ρ , následně počítat odchylku těchto přímek.

Příklad 2.4.7. V $\mathcal{E}_3$ určete odchylku rovin ρ a σ , kde ρ je zadána implicitně

$$\rho = \{[2, 3, 4] + a \cdot (2, 2, 1) + b \cdot (3, 3, -2) \in \mathcal{E}_3 \mid a, b \in \mathbb{R}\}$$

a σ je zadána rovnicí

$$x_1 - 2x_2 + x_3 = 4.$$

Řešení. Můžeme najít nějakou rovinu kolmou na obě roviny a pak počítat odchylky průsečnic. Otočíme-li celou situaci o $\frac{\pi}{4}$, úloha se převede na odchylku normál. Máme normálový vektor $\mathbf{s} = (1, -2, 1)$ roviny σ . Zjistíme normálový vektor $\mathbf{r}$ roviny ρ , který je kolmý na oba směrové vektory.

$$\begin{pmatrix} 2 & 2 & 1 \\ 3 & 3 & -2 \end{pmatrix} \sim \begin{pmatrix} 2 & 2 & 1 \\ 7 & 7 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

Můžeme brát například $\mathbf{r} = (1, -1, 0)$. Máme

$$\langle \mathbf{r}, \mathbf{s} \rangle = 1 \cdot 1 + (-1) \cdot (-2) = 3,$$

$$\begin{aligned}\|\mathbf{r}\| &= \sqrt{2}, \\ \|\mathbf{s}\| &= \sqrt{6},\end{aligned}$$

takže

$$\cos |\angle \rho \sigma| = \frac{3}{\sqrt{12}} = \frac{\sqrt{3}}{2}$$

$$\text{a } |\angle \rho \sigma| = \arccos \frac{\sqrt{3}}{2} = \frac{\pi}{6}. \quad \triangle$$

Příklad 2.4.8. V $\mathbb{R}^3$ spočtěte velikosti a vzájemnou odchylku vektorů $\mathbf{u} = (2, 2, -1)$ a $\mathbf{v} = (-2, 0, 2)$. Spočtěte vzájemnou odchylku přímk generovaných těmito vektory.

Řešení. Máme vektory $\mathbf{u} = (2, 2, -1)$ a $\mathbf{v} = (-2, 0, 2)$. Spočítáme jejich skalární součin

$$\langle \mathbf{u}, \mathbf{v} \rangle = 2 \cdot (-2) + 2 \cdot 0 - 1 \cdot 2 = -6,$$

a jejich velikosti.

$$\|\mathbf{u}\| = \sqrt{2^2 + 2^2 + 1^2} = \sqrt{9} = 3 \quad \|\mathbf{v}\| = \sqrt{2^2 + 0^2 + 2^2} = \sqrt{8} = 2\sqrt{2}$$

Pak máme vztah pro odchylku.

$$\cos |\angle \mathbf{u} \mathbf{v}| = \frac{-6}{6\sqrt{2}} = -\frac{1}{\sqrt{2}} = -\frac{\sqrt{2}}{2}$$

Kosinus odchylky je záporný, proto $|\angle \mathbf{u} \mathbf{v}| \in \left(\frac{\pi}{2}, \pi\right]$ a vidíme, že řešením je $|\angle \mathbf{u} \mathbf{v}| = \frac{3\pi}{4}$.

Ptáme-li se na odchylku přímk, víme, že berem *menší z úhlů*. Toho docílíme tak, že ve vztahu (2.7) dáme do čitatele absolutní hodnotu. (Druhou možností je spočítat odchylku směrových vektorů a je-li víc než $\frac{\pi}{2}$ odpočítat od π .) V našem případě vyjde kosinus odchylky přímk $\frac{\sqrt{2}}{2}$ a úhel $\frac{\pi}{4}$. $\triangle$

Kapitola 3

Teorie čísel

3.1 Počítání v $\mathbb{Z}_m$

Příklad 3.1.1. Najděte inverzní prvek k číslu 157 modulo 2 475, a to

- a) pomocí Bezoutovy věty,
- b) pomocí soustavy kongruencí, která vychází z rozkladu $2\,475 = 9 \cdot 11 \cdot 25$,
- c) pomocí Eulerovy věty.

Řešení. Část a) jsme vyřešili již v příkladu 1.2.7. Máme spočítané koeficienty Bézoutovy rovnosti. Víme, že

$$268 \cdot 157 - 17 \cdot 2\,475 = 1$$

a inverze je tedy 268. Počítejme proto část b). Hledáme inverzi x takovou, že $157x \equiv 1 \pmod{2\,475}$. Tato kongruence musí platit i modulo děliteli 2 475, takže zejména

$$\begin{aligned} 157x &\equiv 1 \pmod{9}, \\ 157x &\equiv 1 \pmod{11}, \\ 157x &\equiv 1 \pmod{25}. \end{aligned}$$

Vyřešíme jednotlivé kongruence. Protože $157 \equiv 4 \pmod{9}$, $157 \equiv 3 \pmod{11}$ a $157 \equiv 7 \pmod{25}$, máme postupně

$$\begin{aligned} 4x &\equiv 1 \pmod{9}, \\ 3x &\equiv 1 \pmod{11}, \\ 7x &\equiv 1 \pmod{25}. \end{aligned}$$

Nyní můžeme zjistit řešení jednotlivých kongruencí. Některá lze díky malým modulům uhádnout. Prvně $4 \cdot 2 = 8 \equiv -1$, proto $4 \cdot (-2) \equiv 1 \pmod{9}$. Dále $4 \cdot 3 = 12 \equiv 1 \pmod{11}$ a nakonec $7 \cdot 7 = 49 \equiv -1$, tudíž $7 \cdot (-7) \equiv 1 \pmod{25}$. Máme tedy soustavu

$$x \equiv -2 \pmod{9},$$

$$\begin{aligned}x &\equiv 4 \pmod{11}, \\x &\equiv -7 \pmod{25}.\end{aligned}$$

Platí, že soustava má jediné řešení modulo $9 \cdot 11 \cdot 25 = 2475$, protože čísla 9, 11 a 25 jsou nesoudělná. Soustavu vyřešíme dosazovací metodou. Protože $x \equiv -2 \pmod{9}$, musí být $x = 9t - 2$. Dosazením do druhé kongruence řešíme následující kongruenci pro t pomocí ekvivalentních úprav.

$$\begin{aligned}9t - 2 &\equiv 4 \pmod{11} \\-2t &\equiv 6 \pmod{11} \\t &\equiv -3 \pmod{11}\end{aligned}$$

V posledním kroku jsme mohli vydělit dvěma, protože 2 a 11 jsou nesoudělná. Máme tedy $t = 11s - 3$, takže

$$x = 9t - 2 = 9 \cdot (11s - 3) - 2 = 99s - 29.$$

Dosazením do třetí kongruence řešíme pro s .

$$\begin{aligned}99s - 29 &\equiv -7 \pmod{25} \\-s &\equiv 22 \equiv -3 \pmod{25} \\s &\equiv 3 \pmod{25}\end{aligned}$$

Vidíme, že $s = 25k + 3$. Pak

$$x = 99s - 29 = 99 \cdot (25k + 3) - 29 = 2475k + 268.$$

Dostáváme (nepřekvapivě) stejný výsledek jako v a). Nyní vyřešíme c). Čísla 157 a 2475 jsou nesoudělná (například proto, že 157 je prvočíslo). Můžeme tedy použít Eulerovu větu. Víme, že pokud $(a, m) = 1$, pak

$$a^{\varphi(m)} \equiv 1 \pmod{m} \tag{3.1}$$

kde $\varphi(m)$ je hodnota Eulerovy funkce v m . Tato funkce udává počet čísel menších než m s m nesoudělných. Pro její výpočet použijeme následující pravidla:

- pro m a n nesoudělná je $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$;
- je-li p prvočíslo a k přirozené číslo (ne nula), pak $\varphi(p^k) = p^{k-1} \cdot (p - 1)$.

Vidíme že $2475 = 9 \cdot 11 \cdot 25 = 3^2 \cdot 11 \cdot 5^2$. Pak

$$\varphi(2475) = \varphi(3^2) \cdot \varphi(11) \cdot \varphi(5^2) = (3 \cdot 2) \cdot 10 \cdot (5 \cdot 4) = 1200.$$

Vidíme, že $157^{1200} \equiv 1 \pmod{2475}$, takže modulární inverzí bude 157^{1199} , což spočítáme pomocí softwaru jako 268. $\triangle$

Příklad 3.1.2. Pomocí malé Fermatovy věty najděte zbytek po dělení čísla $2^{97^{99}}$ číslem 26.

Řešení. Máme rozklad $26 = 2 \cdot 13$. Číslo $2^{97^{99}}$ je sudé, zbytek modulo 2 bude nula. Zbývá najít zbytek modulo 13. Protože 13 je prvočíslo, lze použít *malou Fermatovu větu*. Je-li p prvočíslo a a číslo s ním nesoudělné, pak

$$a^{p-1} \equiv 1 \pmod{p}.$$

Vidíme, že $\varphi(p) = p - 1$. , Jedná se tak vlastně o speciální případ Eulerovy věty (3.1). Máme $\varphi(13) = 12$. Chceme najít zbytek čísla $2^{97^{99}}$ po dělení 12. Protože však $96 = 12 \cdot 8$, je $97 \equiv 1 \pmod{12}$, tudíž $97^{99} \equiv 1 \pmod{12}$. Potom vidíme, že

$$2^{97^{99}} \equiv 2^1 = 2 \pmod{13}.$$

Dohromady existuje jediné řešení soustavy kongruencí $x \equiv 0 \pmod{2}$ a $x \equiv 2 \pmod{13}$ modulo 26, a to $x \equiv 2 \pmod{26}$. Celkem tak máme

$$2^{97^{99}} \equiv 2 \pmod{26}. \quad \triangle$$

Příklad 3.1.3. Najděte poslední dvě cifry čísla $3^{97^{99}}$. Hledáme zbytek po dělení 4 a pomocí Eulerovy věty zbytek po dělení 25.

Řešení. Protože $3 \equiv -1 \pmod{4}$ a exponent je lichý, máme rovnou

$$3^{97^{99}} \equiv (-1)^{97^{99}} = -1 \equiv 3 \pmod{4}.$$

Spočítáme $\varphi(25) = \varphi(5^2) = 5 \cdot 4 = 20$. Hledáme zbytek 97^{99} po dělení 20. Nejprve si všimneme, že $97 \equiv -3$, proto $97^{99} \equiv (-3)^{99} \pmod{20}$. Dále opakujeme stejný postup s Eulerovou funkcí – $\varphi(20) = \varphi(2^2 \cdot 5) = 2 \cdot 1 \cdot 4 = 8$. Hledáme zbytek po dělení 99 osmi. Protože $12 \cdot 8 = 96$, máme $99 \equiv 3 \pmod{8}$, odtud

$$97^{99} \equiv (-3)^{99} \equiv (-3)^3 = -27 \equiv -7 \equiv 13 \pmod{20}.$$

Nyní máme dvě možnosti: buď zjistíme inverzi ke třem modulo 25 (vyjde -8) a tu umocníme na sedmou, nebo přímo trojku umocníme na $13 = 8 + 4 + 1$. Máme $3^2 = 9$, $3^4 = 9^2 = 81 \equiv 6$, $3^8 \equiv 6^2 = 36 \equiv 11 \pmod{25}$. Pak

$$3^{97^{99}} \equiv 3^{13} = 3^{8+4+1} \equiv 11 \cdot 6 \cdot 3 = 66 \cdot 3 \equiv 16 \cdot 3 = 48 \equiv -2 \pmod{25}.$$

Řešíme soustavu $x \equiv -1 \pmod{4}$, $x \equiv -2 \pmod{25}$. Z druhé kongruence máme $x = 25k - 2$, dosazením do první získáme k .

$$25k - 2 \equiv -1 \pmod{4}$$

$$k \equiv 1 \pmod{4}$$

Pak máme $k = 4\ell + 1$, tedy $x = 25 \cdot (4\ell + 1) - 2 = 100\ell + 23$ a poslední dvě cifry čísla $3^{97^{99}}$ jsou 23. $\triangle$

Příklad 3.1.4. Najděte všechny primitivní kořeny modulo 26.

Řešení. Zopakujme si definici primitivních kořenů. *Primitivní kořen modulo n* je g takové, že pro každé b nesoudělné s n existuje k takové, že $g^k \equiv b \pmod{n}$. Platí, že primitivní kořeny modulo prvočísla existují, naopak je-li n dělitelné dvěma *lichými* prvočísky, primitivní kořeny neexistují. Obecnou podmínku však nemáme. Číslo r nazveme *řádem a modulo n* (bereme nesoudělná a a n), jestliže r je nejmenší takové, že

$$a^r \equiv 1 \pmod{p}.$$

Platí, že r dělí $\varphi(n)$ (Lagrangeova věta). Primitivní kořeny modulo n budou ty prvky, jejichž řád je právě $\varphi(n)$. V našem případě máme $26 = 2 \cdot 13$, $\varphi(26) = 1 \cdot 12 = 12$. Máme 12 čísel menších než 26 s ním nesoudělných. Hledáme prvek řádu 12. Stačí ověřovat, že a^4 a a^6 nejsou kongruentní 1. (To jsou maximální dělitelé 12, kteří nejsou 12. Pokud by některá menší mocnina a byla 1, pak by jistě i některá z těchto mocnin byla 1.) Zkoušejme postupně čísla nesoudělná s 26:

- $3^3 = 27 \equiv 1 \pmod{26}$, tedy 3 není primitivní kořen;
- $5^2 = 25 \equiv -1$, proto $5^4 \equiv (-1)^2 = 1 \pmod{26}$, ani 5 není primitivní kořen;
- $7^2 = 49 \equiv -3$, proto $7^4 \equiv (-3)^2 = 9 \not\equiv 1 \pmod{26}$; $7^6 \equiv (-3)^3 = -27 \equiv -1 \not\equiv 1 \pmod{26}$, tedy 7 je primitivní kořen modulo 26.

Pokud známe jeden primitivní kořen modulo n , umíme popsat všechny. Budou to ty jeho mocniny, jejichž exponent je nesoudělný s $\varphi(n)$, jejich počet tedy bude $\varphi(\varphi(n))$. V našem případě budou 4, což je $\varphi(12)$. Exponenty budou 1, 5, 7 a 11, primitivní kořeny budou $7^1 = 7$, $7^5 \equiv 9 \cdot 7 = 63 \equiv 11$, $7^7 \equiv -7 \equiv 19$ a $7^{11} \equiv -11 \equiv 15 \pmod{26}$. $\triangle$

3.2 Šifrování

Příklad 3.2.1. Šifrou RSA s veřejným klíčem $n = 95$ a $e = 49$ bylo posláno číslo $Z = 42$. Šifru prolomte a určete zaslanou zprávu $M \in \{1, 2, \dots, 94\}$.

Řešení. Zopakujeme si šifru RSA. Pro generování klíčů zvolí účastník dvě *velká* prvočísla p a q , spočítá $n = p \cdot q$, $\varphi(n) = (p - 1)(q - 1)$, dále zvolí e nesoudělné s $\varphi(n)$ a spočítá (například pomocí Eukleidova algoritmu) modulární inverzi d , tedy $d \cdot e \equiv 1 \pmod{\varphi(n)}$. Veřejným klíčem je pak dvojice (n, e) , soukromým klíčem je $S = d$. Při šifrování zprávy M spočítáme $C \equiv M^e \pmod{n}$. Při dešifrování šifrované zprávy C pak účastník spočítá $M \equiv C^d \pmod{n}$.

Hledáme rozklad 95 na prvočinitele. Vidíme, že $95 = 5 \cdot 19$, tedy $\varphi(95) = 4 \cdot 18 = 72$. Hledáme inverzi k 49 modulo 72. Řešíme následující soustavu ekvivalentními úpravami.¹

$$49d \equiv 1 \pmod{72}$$

¹Samozřejmě bychom mohli také počítat pomocí rozkladu $72 = 8 \cdot 9$ jako v příkladu 3.1.1, což by bylo i jednodušší.

$$\begin{aligned}
72d &\equiv 0 & (\text{mod } 72) \\
49d &\equiv 1 & (\text{mod } 72) \\
23d &\equiv -1 & (\text{mod } 72) \\
3d &\equiv 3 & (\text{mod } 72) \\
23d &\equiv -1 & (\text{mod } 72) \\
3d &\equiv 3 & (\text{mod } 72) \\
-d &\equiv -25 & (\text{mod } 72) \\
0d &\equiv 72 & (\text{mod } 72) \\
d &\equiv 25 & (\text{mod } 72)
\end{aligned}$$

Vidíme, že $d = 25$. Spočítáme 42^{25} modulo 95. Víme, že $42 \equiv 4 \pmod{19}$ a $25 \equiv 7 \pmod{18}$, takže chceme spočítat 4^7 modulo 19 s tím, že $7 = 4 + 2 + 1$. Víme, že $4^2 = 16 \equiv -3$, odtud $4^4 \equiv (-3)^2 = 9$ a výsledně $4^7 \equiv -3 \cdot 9 \cdot 4 = -3 \cdot 36 \equiv -3 \cdot -2 = 6 \pmod{19}$. Obdobně $42 \equiv 2 \pmod{5}$ a $25 \equiv 1 \pmod{4}$, tedy $42^{25} \equiv 2^1 = 2 \pmod{5}$. Hledáme M takové, že $M \equiv 6 \pmod{19}$ a $M \equiv 2 \pmod{5}$. Z první kongruence máme $M = 19k + 6$, dosazením do druhé zjistíme k .

$$\begin{aligned}
19k + 6 &\equiv 2 & (\text{mod } 5) \\
-k &\equiv -4 & (\text{mod } 5) \\
k &\equiv -1 & (\text{mod } 5)k &= 5\ell - 1
\end{aligned}$$

Tedy $M = 19k + 6 = 19 \cdot (5\ell - 1) + 6 = 95\ell - 19 + 6 = 95\ell - 13$, z čísel mezi 1 a 94 rovnici vyhovuje 82. $\triangle$

Příklad 3.2.2. V šifrovacím systému RSA s veřejným klíčem skládajícím se z modulu $n = 2021$ a exponentu $e = 11$ došlo k prozrazení faktorizace $n = p \cdot q = 43 \cdot 47$. S její pomocí dešifrujte zprávu $c = 21$. Při výpočtu mocniny c^d mod 2021 počítejte zvlášť modulo 43 a modulo 47 a tyto mezivýsledky pak dejte dohromady.

Řešení. Umíme spočítat $\varphi(2021) = 42 \cdot 46 = 1932 = 4 \cdot 3 \cdot 7 \cdot 23$. Hledáme inverzi k 11 modulo 1932. Jednou možností je použít Eulerovu větu. Máme

$$\varphi(1932) = \varphi(2^2 \cdot 3 \cdot 7 \cdot 23) = (2 \cdot 1) \cdot 2 \cdot 6 \cdot 22 = 528,$$

takže inverzí bude 11^{527} , což spočítáme na počítači. Pokud chceme počítat ručně, počítáme inverzi modulo 4, 3, 7 a 23. tj. řešíme následující soustavu.

$$\begin{aligned}
11d &\equiv 1 & (\text{mod } 4) \\
11d &\equiv 1 & (\text{mod } 3) \\
11d &\equiv 1 & (\text{mod } 7)
\end{aligned}$$

$$11d \equiv 1 \pmod{23}$$

Protože $11 \equiv -1 \pmod{4}$, máme $d \equiv -1 \pmod{4}$. Stejná kongruence platí i modulo 3. Tudíž musí být $d \equiv -1$ i modulo $12 = 3 \cdot 4$. $11 \cdot 2 = 22 \equiv 1 \pmod{7}$, tedy $d \equiv 2 \pmod{7}$. Nakonec $11 \cdot (-2) = -22 \equiv 1 \pmod{23}$. Řešíme tak následující soustavu.

$$d \equiv -1 \pmod{12}$$

$$d \equiv 2 \pmod{7}$$

$$d \equiv -2 \pmod{23}$$

Z první kongruence máme $d = 12t - 1$. Dosazením do druhé kongruence zjistíme t .

$$12t - 1 \equiv 2 \pmod{7}$$

$$-2t \equiv 3 \pmod{7}$$

$$t \equiv -12 \equiv 2 \pmod{7}$$

Máme $t = 7s + 2$, tedy $d = 12 \cdot (7s + 2) - 1 = 84s + 23$. Dosadíme do třetí kongruence a spočítáme s .

$$84s + 23 \equiv -2 \pmod{23}$$

$$15s \equiv -2 \pmod{23}$$

Vynásobením -3 dostaneme na levé straně $-45 \equiv 1 \pmod{23}$.

$$s \equiv 6 \pmod{23}$$

Tudíž $s = 23k + 6$ a $d = 84 \cdot (23k + 6) + 23 = 1932k + 527$. Vidíme, že $d = 527$ a náhodou vyšlo $11^{527} \equiv 527 \pmod{1932}$.

Nyní zjistíme 21^{527} modulo 2021. Nejprve modulo 43. Protože $527 \equiv 23 \pmod{42}$, počítáme 7^{23} a $3^{23} \pmod{43}$. Vidíme, že $7^1 = 7$, $7^2 = 49 \equiv 6 \pmod{43}$, $7^3 \equiv 6 \cdot 7 = 42 \equiv -1$, tudíž $7^6 \equiv 1 \equiv 7^{18} \pmod{43}$. Nakonec $7^{23} \equiv 7^5 \equiv 6 \cdot (-1) = -6 \pmod{43}$. Dále $3^4 = 81 \equiv -5$, $3^5 \equiv -15$, $3^6 \equiv -45 \equiv -2$, $3^{18} \equiv -8$, takže $3^{23} \equiv -15 \cdot (-8) \equiv -9 \pmod{43}$. Nakonec

$$c^d \equiv -6 \cdot -9 \equiv 11 \pmod{43}.$$

Obdobně modulo 47. Protože $527 \equiv 21 \pmod{46}$, stačí počítat 7^{21} a 3^{21} . Vidíme, že $7^2 = 49 \equiv 2 \pmod{47}$, takže $7^8 \equiv 2^4 = 16$ a $7^{12} \equiv 2^6 = 64 \equiv 17 \pmod{47}$, tudíž $7^{21} \equiv 17 \cdot 16 \cdot 7 \equiv -10 \cdot 7 = -70 \equiv 24 \pmod{47}$. Dále $3^4 = 81 \equiv -13$, tedy $3^5 \equiv -39 \equiv 8 \pmod{47}$, $3^{10} \equiv 64 \equiv 17$, $3^{20} \equiv 17^2 \equiv 7$, tedy $3^{21} \equiv 21 \pmod{47}$. Celkem

$$c^d \equiv 21 \cdot 24 = 504 \equiv 34 \pmod{34}.$$

Řešíme soustavu kongruencí pro $M \equiv c^d \pmod{2021}$.

$$M \equiv 11 \pmod{43}$$

$$M \equiv 34 \pmod{47}$$

Vyjádřením $M = 47t + 34$ a dosazením řešíme pro t .

$$47t + 34 \equiv 11 \pmod{43}$$

$$4t \equiv -23 \equiv 20 \pmod{43}$$

$$t \equiv 5 \pmod{43}$$

Takže $t = 43s + 5$ a $M = 2021s + 249$.

△

Příklad 3.2.3. V ElGamalově šifrovacím systému si Alice zvolila veřejný klíč sestávající z prvočísla $p = 997$, primitivního kořene $g = 11$ a jeho mocniny g^x (kde exponent $x = 23$ je soukromý). Bartoloměj si pro komunikaci s Alicí zvolil soukromý klíč $y = 25$ a poslal jí svůj veřejný klíč g^y . Pomocí společného soukromého klíče g^{xy} pak zašifroval zprávu m a výslednou zprávu $c = 20$ poslal Alici. Jak ji bude Alice dešifrovat?

Řešení. Připomeneme si ElGamalovu šifru, která vychází z DH protokolu pro výměnu klíčů pro symetrickou kryptografii, kde obě strany komunikace se dohodnou na prvočísle p a primitivním kořenu g modulo p . Každý z účastníků vybere a , respektive b , a pošle druhé straně g^a , resp. g^b modulo p . Společným klíčem pro komunikaci je pak $g^{ab} = (g^a)^b = (g^b)^a$, kterýžto mohou oba účastníci spočítat bez toho, aby jej mohl zjistit kdokoli jiný.

Při použití ElGamalovy šifry účastník zvolí prvočíslo p , primitivní kořen g modulo p , náhodné a a spočítá $h \equiv g^a \pmod{p}$. Veřejným klíčem pak je trojice (p, g, h) a soukromým klíčem je a . Při šifrování zprávy M zvolíme náhodné b a spočítáme $C_1 \equiv g^b \pmod{p}$ a $C_2 \equiv M \cdot h^b \pmod{p}$; následně pošleme $C = (C_1, C_2)$. Pro dešifrování pak účastník spočítá $M \equiv C_2 / C_1^a \pmod{p}$.

V našem příkladu bude společným klíčem $11^{23 \cdot 25} \pmod{997}$. Počítáme $11^{575} \pmod{997}$. Pomocí počítače spočítáme, že je to $950 \equiv -47 \pmod{997}$. Alicin veřejný klíč bude $11^{23} \equiv 659 \pmod{997}$. Naopak Bartolomějův veřejný klíč bude $11^{25} \equiv 976 \equiv -21 \pmod{997}$. Jak Alice tak Bartoloměj jsou schopni zjistit soukromý klíč jako

$$950 \equiv 659^{25} \equiv 976^{23} \pmod{997}.$$

Protože jsme zprávu zašifrovali (modulárním) násobením společným klíčem, pro dešifrování budeme modulárně dělit, tj. násobit modulární inverzí společného klíče. Tu zjistíme jako $950^{995} \equiv 700 \pmod{997}$, takže původní zpráva byla $700 \cdot 20 = 14\,000 \equiv 42 \pmod{997}$. △

Kapitola 4

Aplikace

4.1 Rekurentní posloupnosti

Příklad 4.1.1. Najděte explicitní vyjádření členů posloupnosti splňující rekurentní vztah

$$x_{n+1} = x_n + 6x_{n-1}$$

s počátečními členy $x_0 = 5$, $x_1 = 0$.

Řešení pomocí vlastních čísel. Přidejme si k rekurenci ještě druhou triviální rovnici.

$$x_n = x_n$$

Dostaneme následující soustavu rovnic, která je lineární.

$$\begin{aligned} x_{n+1} &= x_n + 6x_{n-1} \\ x_n &= x_n \end{aligned} \tag{4.1}$$

Pišme sloupcový vektor $(x_{n+1}, x_n)^T$ dvou po sobě následujících členů posloupnosti. S pomocí tohoto zápisu můžeme psát (4.1) ve vektorovém tvaru.

$$\begin{pmatrix} x_{n+1} \\ x_n \end{pmatrix} = \begin{pmatrix} 1 & 6 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} x_n \\ x_{n-1} \end{pmatrix} \tag{4.2}$$

Označme matici z (4.2) P . Pak můžeme s pomocí (4.2) psát rekurenci následujícím způsobem.

$$\begin{pmatrix} x_{n+1} \\ x_n \end{pmatrix} = P \cdot \begin{pmatrix} x_n \\ x_{n-1} \end{pmatrix} = P^2 \cdot \begin{pmatrix} x_{n-1} \\ x_{n-2} \end{pmatrix} = \dots = P^n \cdot \begin{pmatrix} x_1 \\ x_0 \end{pmatrix} \tag{4.3}$$

Nyní nalezneme vlastní čísla a vektory k matici P . Vůči nim se totiž P chová jako násobení vlastním číslem, a tudíž P^n bude mít stejné vlastní vektory a vlastní čísla n -té mocniny vlastních čísel matice P .

$$\det(P - \lambda E) = \det \begin{pmatrix} 1 - \lambda & 6 \\ 1 & -\lambda \end{pmatrix} = \lambda^2 - \lambda - 6 = (\lambda - 3)(\lambda + 2)$$

Máme vlastní číslo $\lambda_1 = 3$, spočítáme k němu příslušný vlastní vektor.

$$P - 3E = \begin{pmatrix} -2 & 6 \\ 1 & -3 \end{pmatrix} \sim \begin{pmatrix} 1 & -3 \\ 0 & 0 \end{pmatrix}$$

Máme vlastní vektor $\mathbf{v}_1 = (3, 1)^T$. Druhým vlastním číslem je $\lambda_2 = -2$, spočítáme jeho vlastní vektor.

$$P + 2E = \begin{pmatrix} 3 & 6 \\ 1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}$$

Druhým vlastním vektorem je $\mathbf{v}_2 = (-2, 1)^T$. Všimněte si, že první složku vlastních vektorů jsme stejně jako dané vlastní číslo a pak druhá složka vyšla 1. To plyne z (4.2).

Chceme si vektor $(x_1, x_0)^T$ vyjádřit v souřadnicích báze $\alpha = (\mathbf{v}_1, \mathbf{v}_2)$. Matici přechodu od standardní báze ϵ k bázi α tvoří po sloupcích složky vektorů α .

$$P_{\epsilon, \alpha} = \begin{pmatrix} 3 & -2 \\ 1 & 1 \end{pmatrix}$$

Opačná matice přechodu (od ϵ k α) bude matice inverzní, kterou můžeme spočítat pomocí determinantů, viz příklad 2.4.3. V případě matice 2×2 inverzní matici spočítáme tak, že prvky na hlavní diagonále prohodíme, na antidiagonále (vedlejší diagonále) změnímme znaménko a výsledek vydělíme determinantem.

$$P_{\alpha, \epsilon} = P_{\epsilon, \alpha}^{-1} = \frac{1}{5} \cdot \begin{pmatrix} 1 & 2 \\ -1 & 3 \end{pmatrix}$$

Následně máme vyjádření $(x_1, x_0)^T = x_1 \mathbf{e}_1 + x_0 \mathbf{e}_0$.

$$\begin{pmatrix} x_1 \\ x_0 \end{pmatrix} = x_1 \mathbf{e}_1 + x_0 \mathbf{e}_2 = \frac{2x_0 + x_1}{5} \mathbf{v}_1 + \frac{3x_0 - x_1}{5} \mathbf{v}_2 \quad (4.4)$$

Nyní můžeme dosadit (4.4) do (4.3) a získáme následující vztah.

$$\begin{aligned} \begin{pmatrix} x_{n+1} \\ x_n \end{pmatrix} &= P^n \cdot \left[\frac{2x_0 + x_1}{5} \mathbf{v}_1 + \frac{3x_0 - x_1}{5} \mathbf{v}_2 \right] \\ &= \frac{2x_0 + x_1}{5} P^n \cdot \mathbf{v}_1 + \frac{3x_0 - x_1}{5} P^n \cdot \mathbf{v}_2 \\ &= \frac{2x_0 + x_1}{5} 3^n \mathbf{v}_1 + \frac{3x_0 - x_1}{5} (-2)^n \mathbf{v}_2 \end{aligned}$$

Porovnáním druhých složek vektorů na obou stranách získáme vzorec pro n -tý člen posloupnosti.

$$x_n = \frac{2x_0 + x_1}{5} 3^n + \frac{3x_0 - x_1}{5} (-2)^n \quad (4.5)$$

Vzhledem k tomu, jak jsme volili vlastní vektory, získáme porovnáním prvních složek vektorů vzorec pro n plus první člen, který bude souhlasit s (4.5). Vidíme, že posloupnost zadaná rekurencí závisí na počátečních podmínkách, tedy na tom, jak zadáme x_0 a x_1 . V našem případě je $x_0 = 5$ a $x_1 = 0$, tedy z (4.5) máme řešení.

$$x_n = 2 \cdot 3^n + 3 \cdot (-2)^n \quad \triangle$$

Jiné řešení. Rekurence je lineární s konstantními koeficienty. Jejím řešením bude proto lineární kombinace posloupností tvaru λ^n . Pro ně má platit

$$\lambda^{n+1} = \lambda^n + 6\lambda^{n-1}$$

pro všechna n . Po vydělení λ^{n-1} a přesunutí členů na levou stranu dostaneme kvadratickou rovnici.

$$\lambda^2 - \lambda - 6 = 0$$

(Všimněte si, že rovnice odpovídá charakteristickému polynomu matice P z předchozího řešení úlohy.) Vidíme, že řešeními jsou $\lambda_1 = 3$ a $\lambda_2 = -2$. Obecně pak bude

$$x_n = a \cdot 3^n + b \cdot (-2)^n$$

pro nějaká $a, b \in \mathbb{R}$. Dosazením $n = 0$ dostaneme $x_0 = a + b$, ze zadání máme $x_0 = 5$. Obdobně pro $n = 1$ máme z rovnice $x_1 = 3a - 2b$ a ze zadání $x_1 = 0$. Máme tedy soustavu dvou rovnic pro dvě neznámé a, b , kterou vyřešíme klasicky.

$$\left(\begin{array}{cc|c} 1 & 1 & 5 \\ 3 & -2 & 0 \end{array} \right) \sim \left(\begin{array}{cc|c} 1 & 1 & 5 \\ 0 & -5 & -15 \end{array} \right) \sim \left(\begin{array}{cc|c} 1 & 0 & 2 \\ 0 & 1 & 3 \end{array} \right)$$

Vidíme, že $a = 2$, $b = 3$ a $x_n = 2 \cdot 3^n + 3 \cdot (-2)^n$. △

Příklad 4.1.2. Určete explicitní vyjádření členů posloupnosti vyhovující rekurentní rovnici

$$x_{n+2} = 2x_{n+1} - 2x_n$$

se členy $x_1 = 2$, $x_2 = 2$.

Řešení. Rekurence je lineární s konstantními koeficienty. Hledáme řešení tvaru λ^n , která musejí splňovat

$$\lambda^{n+2} = 2\lambda^{n+1} - 2\lambda^n.$$

Po vydělení λ^n a převedení dostaneme rovnici

$$\lambda^2 - 2\lambda + 2 = 0$$

s diskriminantem $D = 4 - 8 = -4$ a kořeny $\lambda_{1,2} = \frac{2 \pm 2i}{2} = 1 \pm i$. Musí tedy platit

$$x_n = a \cdot (1 + i)^n + b \cdot (1 - i)^n.$$

Dosazením $n = 1$ máme $x_1 = (1 + i)a + (1 - i)b = 2$ s pravou stranou ze zadání. Protože $(1 \pm i)^2 = 1 \pm 2i - 1 = \pm 2i$, máme pro $n = 2$ ze zadání $x_2 = 2 = 2ia - 2ib$. Celkem tak máme následující soustavu rovnic.

$$\begin{array}{rcl} (1+i)a & + & (1-i)b = 2 \\ 2ia & - & 2ib = 2 \end{array}$$

Tuto soustavu řešíme v maticovém tvaru. Druhý řádek matice vydělíme dvěma. Následně jej vynásobíme $-i$ s tím, že $-i \cdot i = -(-1) = 1$ a $(-i)^2 = -1$.

$$\left(\begin{array}{cc|c} 1+i & 1-i & 2 \\ i & -i & 1 \end{array} \right) \sim \left(\begin{array}{cc|c} 1+i & 1-i & 2 \\ 1 & -1 & -i \end{array} \right)$$

Od prvního řádku odečítáme $(1+i)$ -násobek druhého. V prvním sloupci máme 0, ve druhém $1-i+(1+i)=2$ a ve třetím $2+i(1+i)=2+i-1=1+i$.

$$\sim \left(\begin{array}{cc|c} 0 & 2 & 1+i \\ 1 & -1 & -i \end{array} \right)$$

Nový první řádek vydělíme dvěma.

$$\sim \left(\begin{array}{cc|c} 0 & 1 & \frac{1+i}{2} \\ 1 & -1 & -i \end{array} \right)$$

Nakonec přičteme první řádek ke druhému. Na pravé straně máme $-i+\frac{1+i}{2}=\frac{-2i+1+i}{2}=\frac{1-i}{2}$.

$$\sim \left(\begin{array}{cc|c} 0 & 1 & \frac{1+i}{2} \\ 1 & 0 & \frac{1-i}{2} \end{array} \right)$$

Vidíme, že $a = \frac{1-i}{2}$ a $b = \frac{1+i}{2}$. Máme tak vztah

$$x_n = \frac{1-i}{2} \cdot (1+i)^n + \frac{1-i}{2} \cdot (1-i)^n.$$

Zajímavé je, že ač máme ve vyjádření komplexní čísla, výsledek bude nejen reálný, ale dokonce celočíselný. Podívejme se, proč. Nejprve si koeficienty i mocněnce převedeme do goniometrického tvaru. Vidíme, že $|1 \pm i| = \sqrt{2}$ a že argument mají $\pm \frac{\pi}{4}$, což je zřejmé z obrázku. Máme tak

$$\begin{aligned} x_n &= \frac{\sqrt{2}^{n+1}}{2} \cdot \left(\cos\left(-\frac{\pi}{4}\right) + i \sin\left(-\frac{\pi}{4}\right) \right) \cdot \left(\cos\frac{n\pi}{4} + i \sin\frac{n\pi}{4} \right) + \\ &\quad + \frac{\sqrt{2}^{n+1}}{2} \cdot \left(\cos\frac{\pi}{4} + i \sin\frac{\pi}{4} \right) \cdot \left(\cos\left(-\frac{n\pi}{4}\right) + i \sin\left(-\frac{n\pi}{4}\right) \right) \\ &= \frac{\sqrt{2}^{n+1}}{2} \cdot \left[\cos\frac{(n-1)\pi}{4} + i \sin\frac{(n-1)\pi}{4} + \cos\frac{(1-n)\pi}{4} + i \sin\frac{(1-n)\pi}{4} \right] \end{aligned}$$

což, protože je sinus lichá a kosinus sudá funkce, dává

$$= \sqrt{2}^{n+1} \cos\left(\frac{n\pi}{4} - \frac{\pi}{4}\right)$$

následně s použitím součtového vzorce $\cos(x - y) = \cos x \cos y + \sin x \sin y$ a faktu, že $\cos \frac{\pi}{4} = \sin \frac{\pi}{4} = \frac{1}{\sqrt{2}}$ dostáváme

$$= \sqrt{2}^n \cdot \left(\cos \frac{n\pi}{4} + \sin \frac{n\pi}{4} \right).$$

Podíváme se na hodnoty kosinu a sinu. Protože jsou funkce 2π -periodické, budou se hodnoty opakovat pro n modulo 8. Máme

- $n \equiv 0 \pmod{8}$: sinus vyjde 0 a kosinus 1, v součtu 1;
- $n \equiv 1 \pmod{8}$: sinus i kosinus vyjdou $\frac{\sqrt{2}}{2}$, v součtu $\sqrt{2}$;
- $n \equiv 2 \pmod{8}$: sinus vyjde 1 a kosinus 0, v součtu 1;
- $n \equiv 3 \pmod{8}$: sinus vyjde $\frac{\sqrt{2}}{2}$ a kosinus $-\frac{\sqrt{2}}{2}$, v součtu 0;
- $n \equiv 4 \pmod{8}$: sinus vyjde 0 a kosinus -1 , v součtu -1 ;
- $n \equiv 5 \pmod{8}$: sinus i kosinus vyjdou $-\frac{\sqrt{2}}{2}$, v součtu $-\sqrt{2}$;
- $n \equiv 6 \pmod{8}$: sinus vyjde -1 a kosinus 0, v součtu -1 ;
- $n \equiv 7 \pmod{8}$: sinus vyjde $-\frac{\sqrt{2}}{2}$ a kosinus $\frac{\sqrt{2}}{2}$, v součtu 0.

Pro $n \equiv 3 \pmod{4}$ dostaneme 0, pro n sudá až na znaménko sudou mocninu $\sqrt{2}$, tedy nějakou mocninu 2. Pokud $n \equiv 1 \pmod{4}$, pak dostáváme $\sqrt{2}^{4k+1} \cdot \sqrt{2} = \sqrt{2}^{4k+2}$, tedy opět (až na znaménko) mocninu 2. $\triangle$

4.2 Markovské procesy

Příklad 4.2.1. Roční Albertek Einsteinů staví se 4 kostkami věž. Ta mu ale každou chvíli spadne. Když ji má čerstvě spadlou, vezme nějakou kostku a snaží se ji postavit na některou jinou, což se mu podaří s pravděpodobností $\frac{1}{2}$. Když má věž ze dvou nebo tří kostek, snaží se postavit další kostku na její vrchol, což se mu opět s pravděpodobností $\frac{1}{2}$ podaří. Pokud se mu to nepodaří, věž spadne a Albertek začne znovu. Pokud má věž ze čtyř kostek, radostně zatleská a věž zboří. Takto pokračuje pořád dokola. Maminka se na něj po dostatečně dlouhé době přijde podívat. Jaká je pravděpodobnost, že uvidí stát věž o čtyřech kostkách?

Řešení. Věž se může skládat z jedné, dvou, tří nebo čtyř kostek. Označme tyto stavy čísly 1 až 4. Podívejme se nyní na možné přechody mezi stavy.

1. Můžeme přejít do stavu 2 nebo 1, obojí s pravděpodobností $\frac{1}{2}$.
2. Můžeme přejít do stavu 3 nebo 1, obojí s pravděpodobností $\frac{1}{2}$.
3. Můžeme přejít do stavu 4 nebo 1, obojí s pravděpodobností $\frac{1}{2}$.

4. Jistě přejdeme do stavu 1.

Mějme přechodovou matici $P = (p_{i,j})_{i,j=1}^4$, kde $p_{i,j}$ značí pravděpodobnost přechodu z j -tého stavu do i -tého. (Sloupce odpovídají vstupním hodnotám, řádky výstupním. To je proto, že vektory uvažujeme sloupcové a maticemi je násobíme zleva.)

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

Ta má automaticky dominantní vlastní číslo 1, nebudeme to ověřovat. Spočítáme k němu vlastní vektor.

$$2(P - E) = \begin{pmatrix} -1 & 1 & 1 & 2 \\ 1 & -2 & 0 & 0 \\ 0 & 1 & -2 & 0 \\ 0 & 0 & 1 & -2 \end{pmatrix} \sim \begin{pmatrix} -1 & 1 & 1 & 2 \\ 0 & -1 & 1 & 2 \\ 0 & 0 & -1 & 2 \\ 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} -1 & 0 & 0 & 8 \\ 0 & -1 & 0 & 4 \\ 0 & 0 & -1 & 2 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Máme pravděpodobnostní vlastní vektor $\mathbf{p} = (\frac{8}{15}, \frac{4}{15}, \frac{2}{15}, \frac{1}{15})$. Pravděpodobnost, že maminka uvidí věž se čtyřmi kostkami je $\frac{1}{15}$.

Můžeme také spočítat střední výšku věže. To bude průměr všech možných výšek vážených pravděpodobnostmi jejich výskytu.

$$E = \frac{8}{15} \cdot 1 + \frac{4}{15} \cdot 2 + \frac{2}{15} \cdot 3 + \frac{1}{15} \cdot 4 = \frac{28}{15} = 1,8\bar{6} \approx 1,87 \quad \triangle$$

Poznámka. Řešení by šlo rozšířit na úlohu o n kostkách. Přechodová matice měla rozměry $n \times n$ a byla definována podobně jako v úloze. Její pravděpodobnostní vlastní vektor by byl

$$\left(\frac{2^{n-1}}{2^n - 1}, \frac{2^{n-2}}{2^n - 1}, \dots, \frac{1}{2^n - 1} \right).$$

Nyní chceme spočítat střední výšku věže. Jistě platí, že pravděpodobnost výskytu věže výšky k je $\frac{2^{n-k}}{2^n - 1}$. Potom počítáme střední výšku věže.

$$E = \sum_{k=1}^n \frac{2^{n-k} \cdot k}{2^n - 1} = \frac{2^{n-1}}{2^n - 1} \cdot \sum_{k=1}^n \frac{k}{2^{k-1}}$$

Po vytknutí konstanty získáme napravo částečný součet aritmeticko-geometrické řady s kvocienem $\frac{1}{2}$. Podívejme se, jak ji sečíst. Máme

$$S = 1 + 2q + 3q^2 + \dots + nq^{n-1}$$

Po vynásobení q dostaneme druhou rovnici.

$$q \cdot S = q + 2q^2 + \dots + (n-1)q^{n-1} + nq^n$$

Odečtením získáme částečný součet geometrické řady.

$$\begin{aligned}(1-q)S &= 1 + q + q^2 + \cdots + q^{n-1} - nq^n \\ &= \frac{1-q^n}{1-q} - nq^n\end{aligned}$$

Odtud již získáme potřebný vzorec.

$$\begin{aligned}S &= \frac{1-q^n}{(1-q)^2} - \frac{nq^n}{1-q} \\ &= \frac{1-(n+1)q^n + nq^{n+1}}{(1-q)^n}\end{aligned}$$

V našem případě je $q = \frac{1}{2} = 2^{-1}$. Dosazením do vzorce tedy spočítáme střední hodnotu.

$$\begin{aligned}E &= \frac{2^{n-1}}{2^n - 1} \cdot \frac{1 - (n+1)2^{-n} + n2^{-n-1}}{\left(1 - \frac{1}{2}\right)^2} \\ &= \frac{2^{n+1} \cdot (1 - 2 \cdot 2^{-n-1} - 2n \cdot 2^{-n-1} + n \cdot 2^{-n-1})}{2^n - 1} \\ &= \frac{2^{n+1} - n - 2}{2^n - 1}\end{aligned}$$

Zajímavostí je, že při limitním přechodu $n \rightarrow \infty$ bychom dostali pravděpodobnostní vektor

$$\left(\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \dots\right)$$

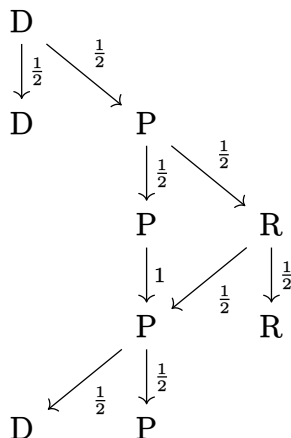
a střední hodnota výšky věže budou 2 kostky.

Příklad 4.2.2. Roztržitý profesor s sebou nosí deštník, ale s pravděpodobností $\frac{1}{2}$ jej zapomene tam, odkud zrovna odchází. Ráno odchází do práce. V poledne chodí z práce do restaurace, z ní se vrací zpět do práce a večer jde domů. Pro jednoduchost uvažujeme, že nikam jinam po dlouhou dobu nechodí a že v restauraci zůstává deštník na místě odkud si ho příště může zase vzít. Uvažujte tuto situaci jako Markovův proces a napište jeho matici. Jaká je pravděpodobnost, že po mnoha dnech bude deštník po ránu nalézat v restauraci? (Uvažujte časovou jednotku jeden den – od rána do rána.)

Řešení. Označme si stavy postupně D (deštník se nachází doma), P (v práci) a R (v restauraci). Rozdělme si den na podúseky určenými místy, mezi kterými se profesor pohybuje. Platí, že pokud se deštník na jeho začátku nachází na stejném místě jako profesor, se stejnou pravděpodobností odejde na následující místo nebo zde zůstane. Nachází-li se deštník na jiném místě než profesor, setrvá zde s jistotou.

Uvažujme nejprve, že je deštník ráno doma. Nakresleme si graf, kde jednotlivé úrovně představují shora dolů denní doby – ráno před odchodem do práce, před obědem, po obědě,

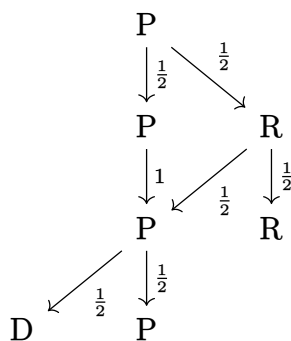
před odchodem domů a po příchodu domů. Šipky v grafu pak odpovídají přechodům mezi stavy, jejich popisky pak pravděpodobnostem.



Pravděpodobnost přechodu po dané cestě je součinem ohodnocení jednotlivých šipek. Pravděpodobnost, že deštník skončí na daném místě je rovna součtu pravděpodobností cest v onom místě končících. Máme tedy pravděpodobnosti

- $D \rightarrow D: \frac{1}{2} + \frac{1}{8} + \frac{1}{16} = \frac{11}{16};$
- $D \rightarrow P: \frac{1}{8} + \frac{1}{16} = \frac{3}{16};$
- $D \rightarrow R: \frac{1}{8}.$

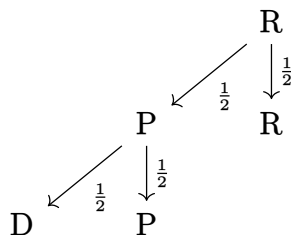
Obdobné grafy si můžeme kreslit i pro stavy, kdy je deštník ráno v práci. Protože však musí být v práci minimálně do profesora odchodu na oběd, stav ráno v grafu vynecháme.



Stejně si napíšeme i pravděpodobnosti přechodů.

- $P \rightarrow D: \frac{1}{8} + \frac{1}{4} = \frac{3}{8}$
- $P \rightarrow P: \frac{1}{4} + \frac{1}{8} = \frac{3}{8}$
- $P \rightarrow R: \frac{1}{4}$

Nakonec si situaci rozeptšíme pro pŕípad, kdy je deštník ráno v restauraci, kde musí zůstat nejméně do profesora odchodu z restaurace.¹



Máme také pravděpodobnosti přechodů: $R \rightarrow D$ i $R \rightarrow P$ s pravděpodobností $\frac{1}{4}$ a $R \rightarrow R$ s pravděpodobností $\frac{1}{2}$. Celkem tedy můžeme psát matici přechodu. Stavy máme seřazené 1. D, 2. P a 3. R a (i, j) -tá složka odpovídá pravděpodobnosti přechodu z j -tého stavu do i -tého.

$$P = \begin{pmatrix} \frac{11}{16} & \frac{3}{8} & \frac{1}{4} \\ \frac{3}{16} & \frac{3}{8} & \frac{1}{4} \\ \frac{1}{8} & \frac{1}{4} & \frac{1}{2} \end{pmatrix}$$

Pro nalezení vlastního vektoru příslušného jedničky řádkově upravujeme matici $16(P - E)$.

$$\begin{aligned} 16(P - E) &= \begin{pmatrix} -5 & 6 & 4 \\ 3 & -10 & 4 \\ 2 & 4 & -8 \end{pmatrix} \sim \begin{pmatrix} 1 & -14 & 12 \\ 3 & -10 & 4 \\ 2 & 4 & -8 \end{pmatrix} \sim \\ &\sim \begin{pmatrix} 1 & -14 & 12 \\ 0 & 32 & -32 \\ 0 & 32 & -32 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{pmatrix} \end{aligned}$$

Pravděpodobnostní vlastní vektor je $\mathbf{p} = \left(\frac{1}{2}, \frac{1}{4}, \frac{1}{4}\right)$, deštník se tedy ráno nachází doma s pravděpodobností $\frac{1}{2}$, v práci respektive v restauraci pak s pravděpodobností $\frac{1}{4}$. $\triangle$

Příklad 4.2.3. Rodina Novákova každoročně jezdí na celý srpen na dovolenou. Buď naloží auto kempingovým vybavením a cestuje po Evropě, nebo naloží kola a jedou k babičce na Vysočinu. Každý rok se rozhodují podle toho, jak trávili dovolenou poslední dva roky, a to částečně náhodně za použití klasické kostky. Rozhodují se podle následujících pravidel.

- Pokud byli poslední dva roky kempovat po Evropě, jedou na Vysočinu.
- Pokud byli poslední dva roky na Vysočině, tak jedou po Evropě.
- Pokud byli loni kempovat po Evropě a předloni u babičky, pak hází kostkou, a když padne liché číslo, tak jedou po Evropě, a když sudé číslo, tak jedou na Vysočinu.
- Pokud byli loni na Vysočině a předloni po Evropě, pak hází kostkou. Když padne 1 nebo 2, pak jedou na Vysočinu, jinak jedou po Evropě.

¹Samořejmě jsme mohli psát všechny případy do jednoho grafu, ale tento postup je přehlednější.

Tímto způsobem se o dovolené rozhodují celý život. V srpnu letošního roku je přijel do místa jejich bydliště navštívit kamarád, s kterým se neviděli po mnoho let. Soused, který věděl, že jsou buď na Vysočině nebo cestují po Evropě, ale nevěděl, kde byli poslední roky, jej poslal na Vysočinu. Určete, jaká je pravděpodobnost, že tam rodinu Novákovu najde.

Řešení. Označme si E stav, že Novákovi jedou kempovat po Evropě a V stav, že pojedou k babičce na Vysočinu. Díky tomu, že se Novákovi rozhodují podle předchozích dvou let, musíme uvažovat uspořádané dvojice těchto stavů. Zjistíme si přechodovou matici.

- Ze stavu EE přejdeme jistě do stavu EV (tedy napřed jeli kempovat a poté na Vysočinu).
- Ze stavu VV jistě přejdeme do stavu VE.
- Ze stavu EV jedou se stejnou pravděpodobností $\frac{1}{2}$ (pro sudá a lichá čísla na kostce) do stavu buď VE nebo VV.
- Ze stavu VE přecházejí do stavu EV s pravděpodobností $\frac{1}{3}$ (na kostce padla 1 nebo 2) nebo do stavu EE s pravděpodobností $\frac{2}{3}$.

Stavy si seřadíme EE, EV, VE, VV. Pak máme matici přechodu.

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

Protože je proces Markovský, má matice přechodu dominantní vlastní číslo 1. Spočítejme k němu vlastní vektor. (Při první úpravě si vynásobíme první dva řádky dvěma a druhé dva třemi.)

$$\begin{aligned} P - E &\sim \begin{pmatrix} -2 & 0 & 1 & 0 \\ 2 & -2 & 1 & 0 \\ 0 & 2 & -3 & 3 \\ 0 & 1 & 0 & -3 \end{pmatrix} \sim \begin{pmatrix} -2 & 0 & 1 & 0 \\ 0 & -2 & 2 & 0 \\ 0 & 2 & -3 & 3 \\ 0 & 1 & 0 & -3 \end{pmatrix} \sim \\ &\sim \begin{pmatrix} -2 & 0 & 1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 3 \\ 0 & 0 & 1 & -3 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 0 & -3 \\ 0 & 1 & 0 & -3 \\ 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 0 \end{pmatrix} \end{aligned}$$

Jako (celočíslný) vlastní vektor můžeme vzít například $\mathbf{v} = (3, 6, 6, 2)^T$, pravděpodobnostní vektor pak bude $\mathbf{p} = \frac{1}{17} \mathbf{v}$. Pravděpodobnost, že pojedou na vysoučinu pak bude součtem pravděpodobností, že jedou na Vysočinu za předpokladu, že loni jeli také na Vysočinu, a za předpokladu, že loni jeli kempovat po Evropě, tedy součtem pravděpodobností stavů EV a VV, což je $\frac{6}{17} + \frac{2}{17} = \frac{8}{17}$. $\triangle$

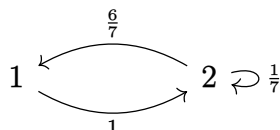
Příklad 4.2.4. Které z matic jsou primitivní, tj. některá její mocnina obsahuje pouze kladné členy?

$$A = \begin{pmatrix} 0 & \frac{1}{7} \\ 1 & \frac{6}{7} \end{pmatrix} \quad B = \begin{pmatrix} \frac{1}{2} & 0 & \frac{1}{3} \\ 0 & 1 & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{6} \end{pmatrix} \quad C = \begin{pmatrix} 0 & 1 & 0 \\ \frac{1}{4} & 0 & \frac{1}{2} \\ \frac{3}{4} & 0 & \frac{1}{2} \end{pmatrix}$$

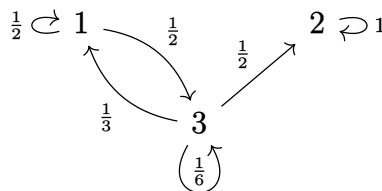
Řešení. Spočítejme si A^2 .

$$A^2 = \begin{pmatrix} 0 & \frac{1}{7} \\ 1 & \frac{6}{7} \end{pmatrix} \cdot \begin{pmatrix} 0 & \frac{1}{7} \\ 1 & \frac{6}{7} \end{pmatrix} = \begin{pmatrix} \frac{1}{7} & \frac{6}{49} \\ \frac{6}{7} & \frac{43}{49} \end{pmatrix}$$

Matice A je tedy primitivní. Jak to ale poznat obecněji? Představme si matici M typu $n \times n$, která popisuje Markovský proces na n stavech, které si označíme 1 až n . Matici M můžeme přiřadit ohodnocený orientovaný graf G_M , jehož vrcholy budou stavy 1 až n , a hrana z i do j bude ohodnocena $m_{j,i}$. Hrany ohodnocené 0 pro přehlednost vynecháme. Cesta je pak ohodnocena součinem ohodnocení jednotlivých hran. Nyní si vzpomeneme na příklad 1.5.4. V matici M^k je prvek $m_{j,i}$ součtem ohodnocení všech cest délky k vedoucích z i do j . Platí, že toto číslo je nenulové právě tehdy, když nějaká taková cesta existuje. Pokud mezi každými dvěma vrcholy grafu existuje orientovaná cesta, nazýváme takový graf silně souvislý. Dále máme následující tvrzení: *Matice M je primitivní právě tehdy, když G_M je silně souvislý a délky orientovaných kružnic jsou nesoudělné.*² Ukážeme si to pro případ matice A .



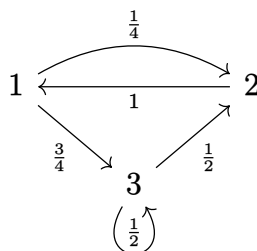
Vidíme, že mezi libovolnými dvěma vrcholy existují cesty a cykly mají délky 1 a 2, matice A je proto primitivní. Nyní můžeme přejít k matici B , která zadává následující graf.



Vidíme, že například ze stavu 2 neexistují cesty do stavů 1 a 3, matice B proto nemůže

²<https://www.sciencedirect.com/science/article/pii/S0024379514001062>

být primitivní. Nakonec vyřešme úlohu pro matici C .



Vidíme, že mezi každými dvěma vrcholy vede cesta a máme smyčku, tedy matice C je primitivní, což si můžeme ověřit počítáním.

$$C^2 = \begin{pmatrix} 0 & 1 & 0 \\ \frac{1}{4} & 0 & \frac{1}{2} \\ \frac{3}{4} & 0 & \frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 \\ \frac{1}{4} & 0 & \frac{1}{2} \\ \frac{3}{4} & 0 & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{4} & 0 & \frac{1}{2} \\ \frac{3}{8} & \frac{1}{4} & \frac{1}{4} \\ \frac{3}{8} & \frac{3}{4} & \frac{1}{4} \end{pmatrix}$$

$$C^3 = \begin{pmatrix} \frac{1}{4} & 0 & \frac{1}{2} \\ \frac{3}{8} & \frac{1}{4} & \frac{1}{4} \\ \frac{3}{8} & \frac{3}{4} & \frac{1}{4} \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 \\ \frac{1}{4} & 0 & \frac{1}{2} \\ \frac{3}{4} & 0 & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{3}{8} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{3}{8} & \frac{1}{4} \\ \frac{3}{8} & \frac{3}{8} & \frac{1}{2} \end{pmatrix} \quad \triangle$$

4.3 Leslieho populační model

Příklad 4.3.1. Farmář chová ovce. Jejich porodnost je dána pouze věkem a je průměrně 2 ovce na jednu ovci mezi jedním a dvěma lety věku, 4 ovce na jednu ovci mezi dvěma a třemi lety věku a 2 ovce na jednu ovci mezi třemi a čtyřmi roky věku. Ovce do jednoho roku nerodí. Z roku na rok umře vždy polovina ovcí a to rovnoměrně ve všech věkových skupinách. Po 4 letech posílá farmář ovce na jatka. Jakou část jehňátek může každý rok prodat, aby mu velikost stáda zůstávala stejná? V jakém věkovém poměru budou rozděleny počty ovcí v jednotlivých věkových skupinách?

Řešení. Máme stavy 0 až 3 podle toho, kolika let se již ovce dožily. Následně určíme matici přechodu. Ze stavů 0, 1 a 2 vždy přejde $\frac{1}{2}$ ovcí do stavu o jedna vyššího. Pro ovce ve stavech 1 a 3 vždy přibude jejich dvojnásobek do stavu 0, do stavu 0 také vždy přibude čtyřnásobek ovcí ve stavu 2. Navíc ještě chceme prodávat roční ovce řekněme $p \in [0, \frac{1}{2}]$ z celkového počtu tak, aby byl chov stabilní. (Hodnota p je shora ohraničena $\frac{1}{2}$, protože pouze tolik ovcí se dožije druhého věku.) To znamená, že ze stavu 0 do stavu 1 ve skutečnosti bude přecházet $\frac{1}{2} - p$ celkového počtu ovcí.

$$L = \begin{pmatrix} 0 & 2 & 4 & 2 \\ \frac{1}{2} - p & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 \end{pmatrix}$$

Populace bude stagnovat, bude-li mít Leslieho matice vlastní číslo 1. Musí tedy platit $\det(L - E) = 0$. Spočítejme tento determinant například Laplaceovým rozvojem podle posledního sloupce.

$$\begin{aligned}\det(L - E) &= \det \begin{pmatrix} -1 & 2 & 4 & 2 \\ \frac{1}{2} - p & -1 & 0 & 0 \\ 0 & \frac{1}{2} & -1 & 0 \\ 0 & 0 & \frac{1}{2} & -1 \end{pmatrix} \\ &= -2 \cdot \det \begin{pmatrix} \frac{1}{2} - p & -1 & 0 \\ 0 & \frac{1}{2} & -1 \\ 0 & 0 & \frac{1}{2} \end{pmatrix} - \det \begin{pmatrix} -1 & 2 & 4 \\ \frac{1}{2} - p & -1 & 0 \\ 0 & \frac{1}{2} & -1 \end{pmatrix}\end{aligned}$$

První matice je horní trojúhelníková. Pro determinant druhé matice použijeme opět Laplaceův rozvoj podle posledního sloupce.

$$\begin{aligned}&= -\frac{2}{4} \cdot \left(\frac{1}{2} - p\right) - 4 \cdot \det \begin{pmatrix} \frac{1}{2} - p & -1 \\ 0 & \frac{1}{2} \end{pmatrix} + \det \begin{pmatrix} -1 & 2 \\ \frac{1}{2} - p & -1 \end{pmatrix} \\ &= \frac{p}{2} - \frac{1}{4} - 1 + 2p + 1 - 1 + 2p = \frac{9}{2}p - \frac{5}{4} = 0\end{aligned}$$

Vidíme, že poslední rovnost nastane pro $p = \frac{5}{18}$, tedy farmář by měl prodávat $\frac{5}{18}$ ročních ovcí. $\triangle$

Příklad 4.3.2. Populační model je dán Leslieho maticí L .

$$L = \begin{pmatrix} 0 & 1 & 2 \\ \frac{1}{2} & 0 & 0 \\ 0 & a & 0 \end{pmatrix}$$

Pro která $a \in (0, 1]$ populace expanduje, pro která směřuje k vyhynutí a pro která se stabilizuje?

Řešení. Hledáme vlastní čísla matice L . Položíme tedy determinant matice $L - \lambda E$ roven nule. Počítáme například Laplaceovým rozvojem podle posledního sloupce.

$$\begin{aligned}\det(L - \lambda E) &= \det \begin{pmatrix} -\lambda & 1 & 2 \\ \frac{1}{2} & -\lambda & 0 \\ 0 & a & -\lambda \end{pmatrix} \\ &= 2 \det \begin{pmatrix} \frac{1}{2} & -\lambda \\ 0 & a \end{pmatrix} - \lambda \cdot \det \begin{pmatrix} -\lambda & 1 \\ \frac{1}{2} & -\lambda \end{pmatrix} \\ &= 2 \cdot \frac{a}{2} - \lambda \cdot \left(\lambda^2 - \frac{1}{2}\right) = -\lambda^3 + \frac{1}{2}\lambda + a = 0\end{aligned}$$

Průběh $\det(L - \lambda E)$ jako funkce λ v závislosti na parametru a je možné vidět například v souboru pro Geogebra.³ Odtud je vidět, že dominantní vlastní číslo bude pro $a \in (0, 1]$ kladné.

Vidíme, že má-li být $\det(L - \lambda E) = 0$, musí být samozřejmě $a = \lambda^3 - \frac{1}{2}\lambda$. Pokud populace stagnuje, je kořen $\lambda = 1$, tedy $a = \frac{1}{2}$. Pro $\lambda > 1$ populace roste a $a > \frac{1}{2}$. Jestliže populace klesá, je $\lambda < 1$ a $a < \frac{1}{2}$. Obrácené implikace platí také (například z analýzy protože derivace a jako funkce λ je na okolí 1 nenulová, nebo si stačí uvědomit, že pro $a > \frac{1}{2}$ stačí přírůstky na stagnaci a ještě máme něco navíc), můžeme tedy říci, že pro $a \in (0, \frac{1}{2})$ populace klesá, pro $a = \frac{1}{2}$ stagnuje a pro $a \in (\frac{1}{2}, 1]$ roste. $\triangle$

Příklad 4.3.3. V jezeru žije populace bílých ryb. Předpokládáme, že druhého roku se dožije 20 % plůdku a od tohoto věku jsou ryby schopné se reprodukovat. Z mladých ryb přežije do třetího roku do stadia velké ryby 60 %. Úmrtnost velkých ryb je zanedbatelná. Dále předpokládáme, že roční přírůstek ryb je trojnásobkem počtu ryb schopných reprodukce.

Tato populace by evidentně jezírko přeplnila. Rovnováhu chceme dosáhnout nasazením štik. Každá štika sní ročně 500 velkých ryb. Kolik štik máme do jezera nasadit, aby populace ryb stagnovala?

Řešení. Předpokládejme, že štiky jedí pouze velké ryby a že jejich populace bude konstantní. Stav si označíme P (plůdky), M (malé ryby) a V (velké ryby). Zjistíme Leslieho matici.

- Z P do M přejde $\frac{1}{5}$ populace.
- Z M do V přejdou $\frac{3}{5}$ populace a vytvoří se trojnásobek populace nových plůdků, tedy z M do P přejdou 3 populace.
- Z V štiky snědí neznámé množství, p , populace, do V tedy přejde $1 - p$ populace. Z V do P přejdou opět 3 populace.

Máme tak Leslieho matici.

$$L = \begin{pmatrix} 0 & 3 & 3 \\ \frac{1}{5} & 0 & 0 \\ 0 & \frac{3}{5} & 1 - p \end{pmatrix}$$

Chceme, aby měla vlastní číslo 1, tedy aby $\det(L - E) = 0$. Determinant spočítáme například Laplaceovým rozvojem podle posledního sloupce, který začíná kladným znaménkem.

$$\begin{aligned} \det(L - E) &= \begin{vmatrix} -1 & 3 & 3 \\ \frac{1}{5} & -1 & 0 \\ 0 & \frac{3}{5} & -p \end{vmatrix} \\ &= 3 \det \begin{pmatrix} \frac{1}{5} & -1 \\ 0 & \frac{3}{5} \end{pmatrix} - p \cdot \det \begin{pmatrix} -1 & 3 \\ \frac{1}{5} & -1 \end{pmatrix} \end{aligned}$$

³<https://math.muni.cz/~prochazka/vyuka/11.6.ggb>

$$= \frac{9}{25} - \frac{2}{5}p = 0$$

Vidíme, že musí platit $p = \frac{9}{10}$. Štiky tedy musí sníst každý rok 90 % velkých ryb. Jestliže jedna štika sní každý rok 500 velkých ryb, musíme nasadit jednu štikou na

$$\frac{10}{9} \cdot 500 = 555,5 \approx 556$$

velkých ryb.⁴

△

4.4 Lineární programování

Příklad 4.4.1. Firma plánuje reklamní kampaň, ve které chce použít inzerci v rádiu, televizi a novinách. Cena jednoho uvedení reklamy v rádiu je 10 000 Kč, v televizi 30 000 Kč, v novinách 20 000 Kč. Firma může za reklamní kampaň utratit nejvýše 350 000 Kč. Počet uvedení reklamy v televizi chce omezit na nejvýše 5. Dále firma chce, aby v novinách byla nejvýše čtvrtina z celkového počtu uvedení ve všech médiích. Počet lidí zasažených reklamou je následující: jedno uvedení reklamy v rádiu slyší 10 000 lidí, jedno uvedení reklamy v televizi vidí 60 000 lidí a jeden inzerát v novinách přečte 30 000 lidí. Firma předpokládá, že nikdo není reklamou zasažen vícekrát.

Při kolika uvedeních reklamy v rádiu, televizi a novinách maximalizuje firma počet lidí zasažených reklamou? Jaký tento počet bude? Zformulujte problém jako úlohu lineární optimalizace a pak úlohu vyřešte.

Řešení. Všechna čísla v zadání vydělíme 10 000. Počty uvedení postupně v radiu, televizi a novinách, označme postupně x_1 , x_2 a x_3 . V úloze jde o maximalizaci funkce

$$f(x_1, x_2, x_3) = x_1 + 6x_2 + 3x_3$$

za podmínek

$$x_1 + 3x_2 + 2x_3 \leq 35, \quad x_2 \leq 5, \quad x_3 \leq \frac{x_1 + x_2 + x_3}{4}.$$

Poslední podmínku můžeme pomocí vynásobení 4 a převedení na levou stranu přepsat do tvaru $4x_3 - x_1 - x_2 - x_3 = -x_1 - x_2 + 3x_3 \leq 0$. Přidáním nových proměnných $t_1, t_2, t_3 \geq 0$ můžeme podmínky přepsat do tvaru rovnic.

$$x_1 + 3x_2 + 2x_3 + t_1 = 35, \quad x_2 + t_2 = 5, \quad -x_1 - x_2 + 3x_3 + t_3 = 0.$$

Úlohu zapíšeme do simplexové tabulky, kde čísla odpovídají koeficientům u proměnných v rovnicích. V prvním řádku máme funkci, kterou minimalizujeme (tedy $-f$). Ostatní řádky

⁴Při tomto zaokrouhlování by populace mírně klesala. Pro korekce bychom museli nasadit jednu štikou na $556 > 555,5$ velkých ryb, ale jakmile by rozdíl přesáhl $555,5$, štikou bychom nenasadili, atd.

pak odpovídají rovnicím.

$$\begin{array}{cccccc|c} x_1 & x_2 & x_3 & t_1 & t_2 & t_3 & \\ \hline -1 & -6 & -3 & 0 & 0 & 0 & 0 \\ 1 & 3 & 2 & 1 & 0 & 0 & 35 \\ 0 & 1 & 0 & 0 & 1 & 0 & 5 \\ -1 & -1 & 3 & 0 & 0 & 1 & 0 \end{array}$$

Evidentně je možným řešením $x_1 = x_2 = x_3 = 0$, $t_1 = 35$, $t_2 = 5$ a $t_3 = 0$. Chceme najít řešení pomocí proměnných x_1 , x_2 a x_3 . Snažíme se postupně vynulovat záporná čísla v záhlaví prvních tří sloupců. Za vedoucí koeficient (pivot) v daném sloupci (postupujeme zleva doprava) určíme kladné číslo takové, že poměr posledního čísla jeho řádku a tohoto čísla je minimální (pokud bychom nemohli použít první sloupec, použili bychom následující). Pomocí řádku s pivotem vynulujeme řádkovými úpravami ostatní čísla v prvním sloupci. Takto pokračujeme s dalšími dvěma sloupci. Pivot je pro daný sloupec je označen červeně.

$$\begin{aligned} \left(\begin{array}{cccccc|c} -1 & -6 & -3 & 0 & 0 & 0 & 0 \\ \textcolor{red}{1} & 3 & 2 & 1 & 0 & 0 & 35 \\ 0 & 1 & 0 & 0 & 1 & 0 & 5 \\ -1 & -1 & 3 & 0 & 0 & 1 & 0 \end{array} \right) &\sim \left(\begin{array}{cccccc|c} 0 & -3 & -1 & 1 & 0 & 0 & 35 \\ 1 & 3 & 2 & 1 & 0 & 0 & 35 \\ 0 & \textcolor{red}{1} & 0 & 0 & 1 & 0 & 5 \\ 0 & 2 & 5 & 1 & 0 & 1 & 35 \end{array} \right) &\sim \\ &\sim \left(\begin{array}{cccccc|c} 0 & 0 & -1 & 1 & 3 & 0 & 50 \\ 1 & 0 & 2 & 1 & -3 & 0 & 20 \\ 0 & 1 & 0 & 0 & 1 & 0 & 5 \\ 0 & 0 & \textcolor{red}{5} & 1 & -2 & 1 & 25 \end{array} \right) &\sim \left(\begin{array}{cccccc|c} 0 & 0 & 0 & \frac{6}{5} & -\frac{2}{5} & \frac{1}{5} & 55 \\ 1 & 0 & 0 & \frac{3}{5} & 0 & 0 & 10 \\ 0 & 1 & 0 & 0 & 1 & 0 & 5 \\ 0 & 0 & 1 & \frac{1}{5} & -\frac{2}{5} & \frac{1}{5} & 5 \end{array} \right) \end{aligned}$$

Řešení je $x_1 = 10$, $x_2 = 5$, $x_3 = 5$. Maximální počet diváků zasažených reklamou je 550 000, tedy deseti tisíci násobek hodnoty funkce f . $\triangle$

Příklad 4.4.2. Květinářství odebírá každý týden květiny od dvou stálých dodavatelů Anny a Bořivoje. Pro tento týden má smysl brát nejvýše jednu dodávku od Anny a jednu od Bořivoje. Při jedné dodávce doveze Anna maximálně 50 svazků květin, přičemž nabízí dovoz růží a tulipánů. Také Bořivoj doveze při jedné dodávce nejvýše 50 svazků květin a nabízí rovněž růže a tulipány. Květinářství může uskladnit maximálně 70 svazků růží a 60 svazků tulipánů. Vedoucí ví, že prodá všechny dodané květiny. Zisk z jednoho svazku růží od Anny je 60 Kč, z jednoho svazku tulipánů od Anny 80 Kč, z jednoho svazku růží od Bořivoje je 100 Kč a z jednoho svazku tulipánů od Bořivoje 110 Kč.

Kolik a jakých svazků má vedoucí pro tento týden objednat, aby maximalizoval svůj zisk? A jaký tento zisk bude? Zformulujte problém jako úlohu lineární optimalizace a pak úlohu vyřešte.

Řešení. Částky můžeme vydělit deseti. Označme počty svazků růží, resp. tulipánů, od Anny a_1 , resp. a_2 . Obdobně pro Bořivoje máme b_1 a b_2 . Pak maximalizujeme funkci

$$f(a_1, a_2, b_1, b_2) = 6a_1 + 8a_2 + 10b_1 + 11b_2$$

(tedy minimalizujeme funkci $-f$) za podmínek

$$a_1 + a_2 \leq 50$$

$$b_1 + b_2 \leq 50$$

(pouze tolik mohou Anna i Bořivoj dodat)

$$a_1 + b_1 \leq 70$$

$$a_2 + b_2 \leq 60$$

(tolik svazků květin daného druhu může květinářství uskladnit). Přidáme si nové proměnné t_1, t_2, t_3 a $t_4 \geq 0$, abychom z nerovností v podmínkách dostali rovnosti. Nyní již můžeme postupovat jako v příkladu 4.4.1 simplexovou metodou, snažíme se vynulovat záporná čísla v prvním řádku. Pivot pro daný sloupec je opět označen červeně. (Všimněte si, že pivot pro první i druhý sloupce vyšel v téměř řádku, nejedná se tedy o klasickou Gaußovu eliminaci.)

$$\begin{aligned} & \left(\begin{array}{cccccccc|c} -6 & -8 & -10 & -11 & 0 & 0 & 0 & 0 & 0 \\ \textcolor{red}{1} & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 50 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 50 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 70 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 60 \end{array} \right) \sim \\ & \sim \left(\begin{array}{cccccccc|c} 0 & -2 & -10 & -11 & 6 & 0 & 0 & 0 & 300 \\ 1 & \textcolor{red}{1} & 0 & 0 & 1 & 0 & 0 & 0 & 50 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 50 \\ 0 & -1 & 1 & 0 & 0 & -1 & 1 & 0 & 20 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 60 \end{array} \right) \sim \\ & \sim \left(\begin{array}{cccccccc|c} 2 & 0 & -10 & -11 & 8 & 0 & 0 & 0 & 400 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 50 \\ 0 & 0 & \textcolor{red}{1} & 1 & 0 & 1 & 0 & 0 & 50 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 70 \\ -1 & 0 & 0 & 1 & -1 & 0 & 0 & 1 & 10 \end{array} \right) \sim \\ & \sim \left(\begin{array}{cccccccc|c} 2 & 0 & 0 & -1 & 8 & 0 & 0 & 0 & 900 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 50 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 50 \\ 1 & 0 & 0 & -1 & 0 & -1 & 1 & 0 & 20 \\ -1 & 0 & 0 & \textcolor{red}{1} & -1 & 0 & 0 & 1 & 10 \end{array} \right) \sim \\ & \sim \left(\begin{array}{cccccccc|c} 2 & 0 & 0 & 0 & 7 & 10 & 0 & 0 & 910 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 50 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & -1 & 40 \\ 0 & 0 & 0 & 0 & -1 & -1 & 1 & 1 & 30 \\ -1 & 0 & 0 & 1 & -1 & 0 & 0 & 1 & 10 \end{array} \right) \end{aligned}$$

V prvním řádku máme v prvním sloupci 2, proto $a_1 = 0$. Dále $a_2 = 50$, $b_1 = 40$ a $b_2 = 10$. Odebíráme tedy 50 tulipánů od Anny a 40 růží a 10 tulipánů od Bořivoje. Maximální zisk bude 9 100 Kč. $\triangle$

Příklad 4.4.3. Firma Defekt vyrábějící jízdní kola chce naplánovat optimální měsíční výrobu. Produkuje tři typy kol: silniční, horská a zimní. Výroba je rozdělená na montáž a testování kvality, přičemž firma má k dispozici 520 hodin provozu montážní linky a 100 hodin testovací laboratoře za jeden měsíc. Pro výrobu silničního kola jsou potřeba 4 hodiny montáže, pro výrobu jednoho horského kola 5 hodin montáže a pro výrobu jednoho zimního kola 6 hodin montáže. Pro každé kolo je potřeba 1 hodina testování. Firma chce, aby zimní kola tvořila maximálně polovinu měsíční produkce všech kol. Zisk z prodeje jednoho silničního kola je 4 000 Kč, z prodeje jednoho horského kola 6 000 Kč a z prodeje jednoho zimního kola 7 000 Kč. Firma vždy prodá všechna vyrobená kola.

Při jakém počtu vyrobených silničních, horských a zimních kol za jeden měsíc maximalizuje firma svůj zisk? A jaký tento zisk bude? Zformulujte problém jako úlohu lineární optimalizace a úlohu vyřešte.

Řešení. Částky vydělíme 1 000. Označíme si proměnné s (počet silničních kol), h (počet horských kol) a z (počet zimních kol). Maximalizujeme funkci

$$f(s, h, z) = 4s + 6h + 7z$$

(minimalizujeme $-f$). Máme omezení

$$4s + 5h + 6z \leq 520$$

$$s + h + z \leq 100$$

pro hodinovou dotaci na výrobu a testování a

$$z \leq \frac{s + h + z}{2}$$

aby zimní kola tvořila maximálně polovinu produkce. Poslední nerovnice je ekvivalentní $s - h + z \leq 0$. Přidáním pomocných proměnných t_1 , t_2 a $t_3 \geq 0$ docílíme toho, aby podmínky měly tvar rovnic. Nyní již můžeme postupovat simplexovou metodou pomocí tabulky. Pivota opět značíme červeně.

$$\begin{pmatrix} -4 & -6 & -7 & 0 & 0 & 0 & 0 \\ 4 & 5 & 6 & 1 & 0 & 0 & 520 \\ \textcolor{red}{1} & 1 & 1 & 0 & 1 & 0 & 100 \\ -1 & -1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & -2 & -3 & 0 & 4 & 0 & 400 \\ 0 & 1 & 2 & 1 & -4 & 0 & 120 \\ 1 & \textcolor{red}{1} & 1 & 0 & 1 & 0 & 100 \\ 0 & 0 & 2 & 0 & 1 & 1 & 100 \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 2 & 0 & -1 & 0 & 6 & 0 & 600 \\ -1 & 0 & \textcolor{red}{1} & 1 & -5 & 0 & 20 \\ 1 & 1 & 1 & 0 & 1 & 0 & 100 \\ 0 & 0 & 2 & 0 & 1 & 1 & 100 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 620 \\ -1 & 0 & 1 & 1 & -5 & 0 & 20 \\ 2 & 1 & 0 & -1 & 6 & 0 & 80 \\ 2 & 0 & 0 & -2 & 11 & 1 & 60 \end{pmatrix}$$

V prvním sloupci máme v prvním řádku kladné číslo, tedy $s = 0$. Dále $h = 80$ a $z = 20$, měsíčně tedy budeme vyrábět 80 horských kol a 20 zimních. Zisk pak bude 620 000 Kč za měsíc. $\triangle$

Příklad 4.4.4. Truhlářství vyrábí stoly, židle a poličky. Na výrobu jednoho stolu potřebuje 3 hodiny, jedné židle 2 hodiny a jedné poličky 1 hodinu. Výrobní kapacita truhlářství je 60 hodin a celkově lze vyrobit nejvýše 40 výrobků. Poliček vyrobí nejvýše tolik, kolik dohromady vyrobí stolů a židlí. Zisk z jednoho stolu je 1 000 Kč, z jedné židle 800 Kč a z jedné poličky 600 Kč.

Zformulujte problém jako úlohu lineárního programování. Určete optimální skladbu výroby a spočítejte maximální zisk simplexovou metodou.

Řešení. Částky vydělíme stem. Označme si s , z a p počty vyrobených stolů, židlí a polic. Maximalizujeme funkci

$$f(s, z, p) = 10s + 8z + 6p$$

za podmínek

$$3s + 2z + p \leq 60 \qquad s + z + p \leq 40 \qquad p \leq s + z$$

což si za pomoci pomocných nezáporných proměnných zapíšeme jako rovnice.

$$3s + 2z + p + t_1 = 60 \qquad s + z + p + t_2 = 40 \qquad -s - z + p + t_3 = 0$$

Následně řešíme úlohu pomocí simplexového algoritmu. Pivota značíme červeně.

$$\begin{aligned} \left(\begin{array}{cccccc|c} -10 & -8 & -6 & 0 & 0 & 0 & 0 \\ \textcolor{red}{3} & 2 & 1 & 1 & 0 & 0 & 60 \\ 1 & 1 & 1 & 0 & 1 & 0 & 40 \\ -1 & -1 & 1 & 0 & 0 & 1 & 0 \end{array} \right) &\sim \left(\begin{array}{cccccc|c} 0 & -\frac{4}{3} & -\frac{8}{3} & \frac{10}{3} & 0 & 0 & 200 \\ 3 & \textcolor{red}{2} & 1 & 1 & 0 & 0 & 60 \\ 0 & \frac{1}{3} & \frac{2}{3} & -\frac{1}{3} & 1 & 0 & 20 \\ 0 & -\frac{1}{3} & \frac{4}{3} & \frac{1}{3} & 0 & 1 & 20 \end{array} \right) &\sim \\ &\sim \left(\begin{array}{cccccc|c} 2 & 0 & -2 & 4 & 0 & 0 & 240 \\ 3 & 2 & 1 & 1 & 0 & 0 & 60 \\ -1 & 0 & \textcolor{red}{1} & -1 & 2 & 0 & 20 \\ 1 & 0 & \textcolor{blue}{3} & 1 & 0 & 2 & 60 \end{array} \right) &\sim \left(\begin{array}{cccccc|c} 0 & 0 & 0 & 2 & 0 & 0 & 280 \\ 4 & 2 & 0 & 2 & -2 & 0 & 40 \\ -1 & 0 & 1 & -1 & 2 & 0 & 20 \\ 4 & 0 & 0 & 4 & 0 & 2 & 0 \end{array} \right) &\sim \\ &\sim \left(\begin{array}{cccccc|c} 0 & 0 & 0 & 2 & 0 & 0 & 280 \\ 0 & 2 & 0 & -2 & -2 & -2 & 40 \\ 0 & 0 & 1 & 0 & 2 & \frac{1}{2} & 20 \\ 2 & 0 & 0 & 2 & 0 & 1 & 0 \end{array} \right) \end{aligned}$$

(Poslední krok je Gaußova eliminace pro skladbu výroby. To, že $s = 0$ vidíme již z předposledního kroku. Použili-li bychom modrého pivota, vyšlo by v prvním řádku v prvním sloupci kladné číslo.) Optimálně bychom neměli vyrábět žádné stoly a vyrábět po dvaceti židlích a policích. Zisk bude 28 000 Kč. $\triangle$

Příklad 4.4.5. Rádio vysílá hudbu, moderátora nebo pohádku a potřebuje zaplnit hodinu vysílacího času. Alespoň 50 % času musí být hudba, alespoň 10 minut pohádka. Náklady na minutu vysílání jsou u hudby 200 Kč, u moderátora 100 Kč, u pohádky 150 Kč. Zisk rádia za minutu vysílání je 300 Kč.

Zformulujte příklad jako úlohu lineárního programování. Užitím simplexového algoritmu určete optimální skladbu programu a celkový zisk.

Řešení. Hudba má zabírat nejméně polovinu programu, což je z 60 minut 30. Pohádka má zabírat minimálně 10 minut. Jediným jiným omezením je, že celkově vysíláme 60 minut (ticho nevysíláme). Čisté zisky za minutu vysílání zjistíme odečtením nákladů:

- $300 - 200 = 100$ Kč za hudbu;
- $300 - 150 = 150$ Kč za pohádku;
- $300 - 100 = 100$ Kč za moderátora.

Vzhledem k omezením bychom intuitivně odhadli, že nejvyšších zisků dosáhneme, když budeme vysílat 30 minut hudby a 10 minut pohádek (tedy předepsaná minima) a zbytek (20 minut) vyplníme moderátorem, jehož náklady jsou nejnižší. Pak výdělek za hodinu bude $30 \cdot 100 + 10 \cdot 150 + 20 \cdot 200 = 8\,500$ Kč.

Zjistíme, zda je náš odhad správný pomocí lineárního programování. Označme h , p a m počty minut vysílání hudby, pohádek a moderátora. Maximalizujeme funkci

$$f(h, p, m) = 100h + 150p + 200m$$

za omezení

$$h + p + m = 60$$

$$h \geq 30$$

$$p \geq 10$$

přičemž druhé dvě podmínky si změním na rovnice odečtením nových kladných proměnných.

$$h - t_1 = 30$$

$$p - t_2 = 10$$

Můžeme úlohu řešit pomocí simplexového algoritmu. Pivota značíme červeně.

$$\begin{aligned} \left(\begin{array}{ccccc|c} -100 & -150 & -200 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 60 \\ \textcolor{red}{1} & 0 & 0 & -1 & 0 & 30 \\ 0 & 1 & 0 & 0 & -1 & 10 \end{array} \right) &\sim \left(\begin{array}{ccccc|c} 0 & -150 & -200 & -100 & 0 & 3\,000 \\ 0 & 1 & 1 & 1 & 0 & 30 \\ 1 & 0 & 0 & -1 & 0 & 30 \\ 0 & \textcolor{red}{1} & 0 & 0 & -1 & 10 \end{array} \right) &\sim \\ &\sim \left(\begin{array}{ccccc|c} 0 & 0 & -200 & -100 & -150 & 4\,500 \\ 0 & 0 & \textcolor{red}{1} & 1 & 1 & 20 \\ 1 & 0 & 0 & -1 & 0 & 30 \\ 0 & 1 & 0 & 0 & -1 & 10 \end{array} \right) &\sim \left(\begin{array}{ccccc|c} 0 & 0 & 0 & 100 & 50 & 8\,500 \\ 0 & 0 & 1 & 1 & 1 & 20 \\ 1 & 0 & 0 & -1 & 0 & 30 \\ 0 & 1 & 0 & 0 & -1 & 10 \end{array} \right) \end{aligned}$$

Vidíme, že optimálního zisku za daných podmínek dosáhneme vysíláním 30 minut hudby, 10 minut pohádky a 20 minut moderátora a maximální zisk bude opravdu 8 500 Kč. $\triangle$