LINEÁRNÍ ALGEBRA

LIBOR BARTO A JIŘÍ TŮMA

barto@karlin.mff.cuni.cz, tuma@karlin.mff.cuni.cz

Toto jsou průběžně vznikající zápisky z přednášky Lineární algebra a geometrie 1. Pokud naleznete jakoukoliv chybu, dejte nám určitě vědět!

---

1. Předpoklady

1.1. **Komplexní čísla.**

1.2. **Teorie čísel.** GCD, Bezout, inverzy modulo p, gcd a Bezout pro polynomy

1.3. **Zobrazení.** Zobrazení $f : A \to B$ má vždy definiční obor A (ne jak v analýze, nebo úvodním kurzu).
Bijekce právě když má inverz.
Zobrazení je prosté právě když má levý inverz, je na právě když má pravý inverz.

Cvičení

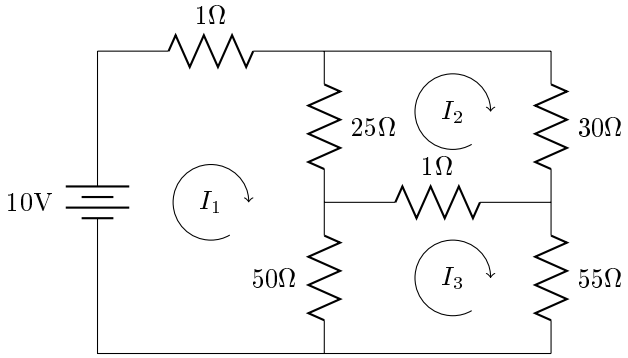
1. Předpokládejme, že $f : A \to B$ je bijekce a $g : B \to A$ je zobrazení zprava inverzní k f. Dokažte, že g je bijekce (a tím pádem $g = f^{-1}$).

2. Řešení soustav lineárních rovnic

Cíl. *Naučíme se řešit soustavy lineárních rovnic Gaussovou eliminační metodou.*

2.1. **Aplikace.**
Na řešení soustavy lineárních rovnic vede celá řada praktických i teoretických úloh. Pro ilustraci uvedeme čtyři příklady.

2.1.1. *Elektrické obvody.* U elektrického obvodu na obrázku chceme určit proudy protékající jednotlivými větvemi.



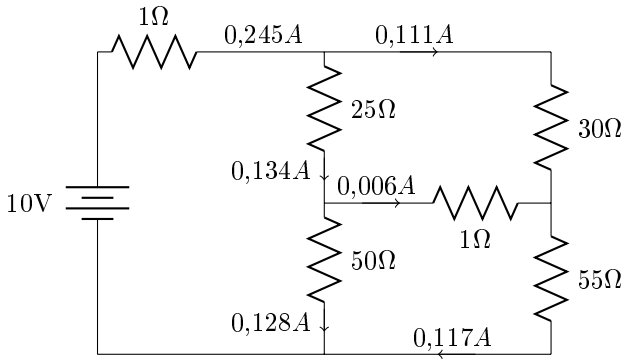
Obrázek 1. Elektrický obvod z části 2.1.1

Date: 30. ledna 2013.

Použijeme metodu smyček. Proudy protékající jednotlivými elementárními smyčkami jsou označeny I_1, I_2, I_3 podle obrázku. Aplikací druhého Kirchhoffova zákona získáme pro každou smyčku jednu rovnici:

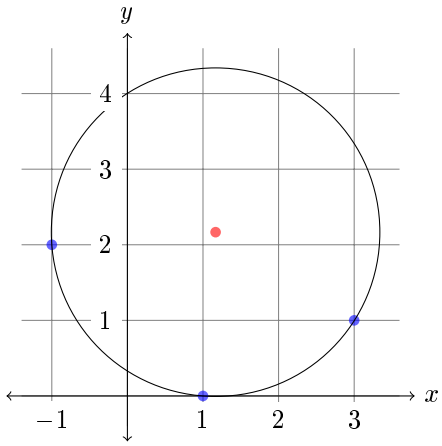
$$1I_1 + 25(I_1 - I_2) + 50(I_1 - I_3) = 10$$
$$25(I_2 - I_1) + 30I_2 + 1(I_2 - I_3) = 0$$
$$50(I_3 - I_1) + 1(I_3 - I_2) + 55I_3 = 0$$

Zjednodušením dostaneme soustavu třech lineárních rovnic o třech neznámých, která má právě jedno řešení $(I_1, I_2, I_3) = (0{,}245,\ 0{,}111,\ 0{,}117)$. Z toho dopočteme proudy pro jednotlivé větve.



Obrázek 2. Proudy v elektrickém obvodu z části 2.1.1

2.1.2. *Prokládání kružnice danými body.* Chceme najít kružnici v rovině procházející body $(1, 0)$, $(-1, 2)$, $(3, 1)$. (Například víme, že se nějaký objekt pohybuje po kruhové dráze, máme změřeny tři polohy a chceme určit střed obíhání.)



Obrázek 3. Kružnice procházející danými třemi body

Rovnice kružnice v rovině má tvar

$$x^2 + y^2 + ax + by + c = 0.$$

Dosazením daných třech bodů získáme soustavu lineárních rovnic

$$1 + a + c = 0,$$
$$5 - a + 2b + c = 0,$$
$$10 + 3a + b + c = 0.$$

Soustava má právě jedno řešení $(a, b, c) = (-7/3, -13/3, 4/3)$, takže hledaná kružnice má rovnici

$$x^2 + y^2 - \frac{7}{3}x - \frac{13}{3}y + \frac{4}{3} = 0.$$

Chceme-li znát střed a poloměr, rovnici můžeme upravit na tvar

$$\left(x-\frac{7}{6}\right)^2+\left(y-\frac{13}{6}\right)^2=\frac{85}{18},$$

z kterého vidíme, že hledaná kružnice má střed $(7/6, 13/6)$ a poloměr $\sqrt{85/18}$.

2.1.3. *Vyčíslování chemické rovnice.* Uvažujme chemickou reakci toluenu a kyseliny dusičné, při které vznikná TNT a voda:

$$C_7H_8+HNO_3\longrightarrow C_7H_5O_6N_3+H_2O.$$

Vyčíslení chemické rovnice znamená nalezení poměrů jednotlivých molekul, aby počet atomů každého prvku byl na obou stranách stejný.

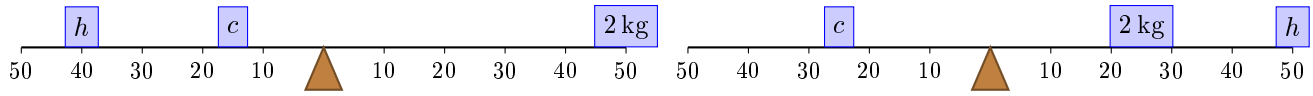
$$xC_7H_8+yHNO_3\longrightarrow zC_7H_5O_6N_3+vH_2O.$$

Chceme tedy najít hodnoty x, y, z, v, které splňují soustavu rovnic To vede na rovnice

$$\begin{aligned}7x&=7z,\\8x+y&=5z+2v,\\y&=3z,\\3y&=6z+w.\end{aligned}$$

Vzhledem k výbušné povaze tohoto příkladu nebudeme na tomto místě raději uvádět řešení.

2.1.4. *Neznámá závaží.* Máme tři závaží. První váží $2kg$, ale hmotnost dalších dvou bohužel neznáme. Podařilo se nám však najít dvě rovnovážné polohy:



Obrázek 4. Neznámá závaží

Z těchto informací můžeme hmotnosti určit. Provnáním momentů totiž dostaneme soustavu lineárních rovnic

$$\begin{aligned}40h+15c&=50\cdot 2\\25c&=25\cdot 2+50h,\end{aligned}$$

kterou snadno vyřešíme.

2.2. **Geometrická interpretace.** Jedno řešení soustavy lineárních rovnic o n neznámých budeme zapisovat jako uspořádanou n-tici čísel. To předpokládá nějaké pevné uspořádání proměnných. Z kontextu bude toho uspořádání zřejmé, proměnné jsou většinou značeny $x_1, \dots, x_n$. Uspořádanou n-tici čísel nazýváme *n-složkový aritmetický vektor*:

Definice 2.1. *Aritmetickým vektorem nad $\mathbb{R}$ s n složkami* rozumíme uspořádanou n-tici reálných čísel.

V této kapitole budeme často místo „aritmetický vektor nad $\mathbb{R}$“ říkat pouze „aritmetický vektor“, nebo jen „vektor“, protože jiné druhy vektorů nebudeme používat.

Vektory budeme psát sloupcově, například

$$\mathbf{v}=\begin{pmatrix}1\\-33\\5\end{pmatrix}.$$

Pro úsporu místa vektor často napíšeme řádkově a přidáme exponent T, například

$$\mathbf{v}=(1,-33,5)^T.$$

Znak T bude zaveden v kapitole **??** obecněji pro transponování matic.

Aritmetické vektory si pro $n=2$ (resp. $n=3$) můžeme představovat jako šipky v rovině (resp. prostoru) s danou velikostí a směrem.

OBRAZEK

Každý bod má svůj *polohový vektor*, což je vektor určený počátkem a tímto bodem. Takto si vzájemně jednoznačně odpovídají body a vektory a můžeme mezi těmito pojmy libovolně přecházet. Například množinu řešení soustavy lineárních rovnic můžeme chápat jako množinu bodů, nebo jako množinu polohových vektorů těchto bodů.

2.2.1. *Jedna rovnice o dvou neznámých.* Množinou řešení rovnice $a_1x_1 + a_2x_2 = b_1$, kde $a_1, a_2, b_1 \in \mathbb{R}$ jsou zvolená čísla a x_1, x_2 jsou neznámé, je přímka v rovině, kromě triviálního případu, že $a_1 = a_2 = 0$, kdy je množinou řešením buď celá rovina (v případě $b_1 = 0$) nebo prázdná množina (v případě $b_1 \neq 0$). Kolmostí a skalárním součinem se budeme detailněji zabývat v kapitole **??**, teď jen připomeňme, že $(a_1, a_2)^T$ je normálový vektor této přímky, tj. vektor kolmý na její směr.

OBRAZEK

Každá přímka může být také vyjádřena parametricky. K tomu připomeneme operace sčítání vektorů a násobení vektorů reálným číslem.

Definice 2.2. Jsou-li $\mathbf{u} = (u_1, u_2 \ldots, u_n)^T$ a $\mathbf{v} = (v_1, v_2, \ldots, v_n)^T$ dva n-složkové aritmetické vektory nad $\mathbb{R}$, pak jejich součtem rozumíme aritmetický vektor

$$\mathbf{u} + \mathbf{v} = \begin{pmatrix} u_1 + v_1 \\ u_2 + v_2 \\ \vdots \\ u_n + v_n \end{pmatrix} .$$

Je-li $\mathbf{u} = (u_1, \ldots, u_n)$ aritmetický vektor nad $\mathbb{R}$ a $t \in \mathbb{R}$ reálné číslo, pak t-násobkem vektoru $\mathbf{u}$ rozumíme vektor

$$t \cdot \mathbf{u} = t\mathbf{u} = \begin{pmatrix} tu_1 \\ tu_2 \\ \vdots \\ tu_n \end{pmatrix} .$$

Pro dva n-složkové vektory $\mathbf{u}, \mathbf{v}$ definujeme

$$-\mathbf{u} = (-1) \cdot \mathbf{u} \quad \text{a} \quad \mathbf{u} - \mathbf{v} = \mathbf{u} + (-\mathbf{v}) .$$

OBRAZEK

Příklad 2.3.

$$2 \cdot \begin{pmatrix} 1 \\ 3 \\ 7 \end{pmatrix} - \begin{pmatrix} 5 \\ 2 \\ -2 \end{pmatrix} = \begin{pmatrix} 2 \\ 6 \\ 14 \end{pmatrix} + \begin{pmatrix} -5 \\ -2 \\ 2 \end{pmatrix} = \begin{pmatrix} -3 \\ 4 \\ 16 \end{pmatrix} .$$

Parametrické vyjádření přímky v rovině je zápis tvaru

$$\{\mathbf{u} + t\mathbf{v} : t \in \mathbb{R}\} ,$$

kde $\mathbf{u}$ a $\mathbf{v}$ jsou 2-složkové vektory. Vektor $\mathbf{u}$ je polohovým vektorem bodu ležícího na přímce a vektor $\mathbf{v}$ určuje směr.

OBRAZEK

V prostoru má parametrické vyjádření přímky stejný tvar, akorát vektory $\mathbf{u}, \mathbf{v}$ mají tři složky.

2.2.2. *Více rovnic o dvou neznámých.* Uvažujme libovolnou soustavu lineárních rovnic o dvou neznámých x_1, x_2. Každá (netriviální) rovnice určuje přímku v rovině a my se snažíme najít dvojice (x_1, x_2), které vyhovují všem rovnicím. Řešením je tedy průnik přímek daných našimi rovnicemi. Z toho je intuitivně jasné jak může vypadat množina všech řešení:

- Celá rovina. To se stane v případě, že všechny rovnice mají triviální tvar $0x_1 + 0x_2 = 0$.
- Přímka. To se stane v případě, že všechny (netriviální) rovnice popisují tutéž přímku, neboli všechny rovnice jsou násobkem jedné z rovnic.
- Bod. Nastane v případě, že soustavy popisují alespoň dvě různé přímky a všechny tyto přímky procházejí jedním bodem.

  OBRAZEK
- Prázdná množina. Nastane v případě, že dvě rovnice určují rovnoběžné přímky, nebo rovnice určují tři přímky neprocházející jedním bodem, nebo jedna z rovnic je triviálně nesplnitelná, například $0x_1 + 0x_2 = 123$.

  OBRAZEK

2.2.3. *Tři neznámé.* Množina řešení jedné lineární rovnice o třech neznámých tvaru $a_1x_1 + a_2x_2 + a_3x_3 = b$ geometricky odpovídá rovině v $\mathbb{R}^3$, kromě triviálního případu $a_1 = a_2 = a_3 = 0$. Vektor $(a_1, a_2, a_3)^T$ je normálovým vektorem roviny. Parametricky lze rovinu zapsat ve tvaru

$$\{\mathbf{u} + s\mathbf{v} + t\mathbf{w} : s, t \in \mathbb{R}\} \ ,$$

kde $\mathbf{u}, \mathbf{v}, \mathbf{w}$ jsou vhodné (trojsložkové) vektory.

OBRAZEK

Řešíme-li tedy soustavu lineárních rovnic o třech neznámých, hledáme průnik rovin. Řešením může být:

- Celý prostor. To nastane v triviálním případě.
- Rovina.
- Přímka. OBRAZEK
- Bod. OBRAZEK
- Prázdná množina. OBRAZEK

2.2.4. *Více než tři neznámé.* Pro více proměnných je vizuální představa obtížná, ne-li nemožná. Stále ale platí, že jedna netriviální rovnice určuje „rovný útvar“ s dimenzí o jedna menší než je počet neznámých, tzv. *nadrovinu.* (Dimenzi sice budeme definovat později, ale pro malé dimenze definice souhlasí s intuicí.) Řešení soustavy pak lze chápat jako hledání průniku nadrovin. Výsledkem bude „rovný útvar“ nějaké dimenze (bod, přímka, rovina, ...).

2.3. **Příklady.** Princip řešení soustav lineárních rovnic Gaussovou eliminační metodou předvedeme nejprve na několika příkladech. V další části pak shrneme obecný postup.

2.3.1. *Soustava s jedním řešením.* Začneme s přímočarým příkladem soustavy třech rovnic o třech neznámých x_1, x_2, x_3.

$$\begin{aligned} 2x_1 + 6x_2 + 5x_3 &= 0 \\ 3x_1 + 5x_2 + 18x_3 &= 33 \\ 2x_1 + 4x_2 + 10x_3 &= 16 \end{aligned}$$

Principem eliminační metody je převést soustavu ekvivalentními úpravami (tj. úpravami, které nemění množinu řešení) do tvaru, ze kterého se řešení snadno dopočítá. Ekvivalentními úpravami jsou například prohození dvou rovnic, vynásobení některé rovnic nenulovým číslem a přičtení několikanásobku jedné rovnice k jiné. Tvar, o který se snažíme, je tzv. *odstupňovaný tvar.* Přesně bude definován později, ale principem je, že v každé další rovnici je na začátku více nulových koeficientů.

Nejprve docílíme toho, že ve všech rovnicích kromě první bude nulový koeficient u x_1. Tomuto procesu se také říká eliminace proměnné x_1. V našem případě bychom mohli $(-3/2)$-násobek první rovnice přičíst k druhé a (-1)-násobek první rovnice přičíst ke třetí. Aby nám však vycházely hezčí koeficienty, vynásobíme třetí rovnici jednou polovinou a prohodíme ji s první rovnicí.

$$\begin{aligned} x_1 + 2x_2 + 5x_3 &= 8 \\ 3x_1 + 5x_2 + 18x_3 &= 33 \\ 2x_1 + 6x_2 + 5x_3 &= 0 \end{aligned}$$

Jsme připraveni k eliminaci proměnné x_1: Přičteme (-3)-násobek první rovnice ke druhé a (-2)-násobek první rovnice ke třetí.

$$\begin{aligned} x_1 + 2x_2 + 5x_3 &= 8 \\ -x_2 + 3x_3 &= 9 \\ +2x_2 - 5x_3 &= -16 \end{aligned}$$

Po eliminaci jedné proměnné již první řádek nebudeme měnit a budeme se zabývat pouze zbylými řádky. V našem případě již zbývají pouze dva a k eliminaci proměnné x_2 stačí přičíst 2-násobek druhé rovnice ke třetí.

$$\begin{aligned} x_1 + 2x_2 + 5x_3 &= 8 \\ -x_2 + 3x_3 &= 9 \\ x_3 &= 2 \end{aligned}$$

Nyní již můžeme dopočítat řešení tzv. *zpětnou substitucí*, kdy postupujeme od poslední rovnice k první a postupně dosazováním získáváme hodnoty proměnných. V našem případě dostáváme $x_3 = 2$, $x_2 = -3$, $x_1 = 4$. Původní soustava má právě jedno řešení, a to aritmetický vektor $(4, -3, 2)^T$.

2.3.2. *Maticový zápis.* Pro zkrácení zápisu budeme místo soustavy psát její *rozšířenou matici.* Nejprve zavedeme pojem matice:

Definice 2.4. *Maticí* (nad $\mathbb{R}$) typu $m \times n$ rozumíme obdélníkové schéma reálných čísel s m řádky a n sloupci.

Zápis $A = (a_{ij})_{m\times n}$ znamená, že A je matice typu $m \times n$, která má na pozici (i, j) (tedy v i-tém řádku a j-tém sloupci) číslo a_{ij}.

Pozor na pořadí indexů – první číslo označuje řádek, druhé sloupec.

Definice 2.5. *Maticí soustavy*

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1\\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2\\ &\cdots\\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m \end{aligned}$$

rozumíme matici

$$A = (a_{ij})_{m\times n} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n}\\ a_{21} & a_{22} & \dots & a_{2n}\\ \vdots & \vdots & \ddots & \vdots\\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

Vektor pravých stran je vektor $\mathbf{b} = (b_1, b_2, \dots, b_m)^T$ a *rozšířená matice soustavy* je matice

$$(A \mid \mathbf{b}) = \left(\begin{array}{cccc|c} a_{11} & a_{12} & \dots & a_{1n} & b_1\\ a_{21} & a_{22} & \dots & a_{2n} & b_2\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{array}\right).$$

Rozšířená matice soustavy tedy vznikne tak, že do i-tého řádku zapíšeme koeficienty v i-té rovnici u proměnných $x_1, \dots, x_n$ a nakonec napíšeme pravou stranu. Pro přehlednost se pravé strany oddělují svislou čarou. Rozšířená matice se tímto rozdělí na dva bloky. V levém je matice soustavy a v pravém je sloupec pravých stran.

Pro soustavu rovnic z předchozího příkladu

$$\begin{aligned} 2x_1 + 6x_2 + 5x_3 &= 0\\ 3x_1 + 5x_2 + 18x_3 &= 33\\ 2x_1 + 4x_2 + 10x_3 &= 16 \end{aligned}$$

jsou její matice, sloupec pravých stran a rozšířená matice

$$A = \begin{pmatrix} 2 & 6 & 5\\ 3 & 5 & 18\\ 2 & 4 & 10 \end{pmatrix},\ \mathbf{b} = \begin{pmatrix} 0\\ 33\\ 16 \end{pmatrix},\ (A \mid \mathbf{b}) = \left(\begin{array}{ccc|c} 2 & 6 & 5 & 0\\ 3 & 5 & 18 & 33\\ 2 & 4 & 10 & 16 \end{array}\right).$$

Prohození dvou rovnic se v rozšířené matici projeví prohozením dvou řádků, vynásobení i-té rovnice číslem t odpovídá vynásobení i-tého řádku matice číslem t a podobně přičtení t-násobku i-té rovnice k j-té se projeví odpovídá přičtení t-násobku i-tého řádku k j-tému. Pro vyznačení, že rozšířená matice vznikla z předchozí ekvivalentní úpravou používáme symbol $\sim$. Úpravy provedené u naší soustavy tedy zapíšeme takto:

$$\left(\begin{array}{ccc|c} 2 & 6 & 5 & 0\\ 3 & 5 & 18 & 33\\ 2 & 4 & 10 & 16 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 2 & 5 & 8\\ 3 & 5 & 18 & 33\\ 2 & 6 & 5 & 0 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|c} 1 & 2 & 5 & 8\\ 0 & -1 & 3 & 9\\ 0 & 2 & -5 & -16 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 2 & 5 & 8\\ 0 & -1 & 3 & 9\\ 0 & 0 & 1 & 2 \end{array}\right)$$

Zápis úprav se tímto značně zkrátí a zpřehlední.

Místo „soustava rovnic s rozšířenou maticí $(A \mid \mathbf{b})$“ budeme někdy stručně říkat „soustava $(A \mid \mathbf{b})$“.

Poznamenejme ještě, že užitím násobení matic z kapitoly **??** lze řešení soustavy rovnic s rozšířenou maticí $(A \mid \mathbf{b})$ zapsat jako hledání všech vektorů $\mathbf{x}$ takových, že $A\mathbf{x} = \mathbf{b}$. Maticový popis se hodí nejen ke zkrácení a zpřehlednění, je výhodnější i pro teoretické úvahy. Po zavedení všech pojmů již vlastně jiný zápis ani nebudeme používat.

2.3.3. *Jeden parametr.* Podívejme se na příklad soustavy rovnic o třech neznámých, kdy řešením je přímka. Používáme rovnou maticový zápis.

$$\left(\begin{array}{ccc|c} 1 & 4 & 3 & 11 \\ 1 & 4 & 5 & 15 \\ 2 & 8 & 3 & 16 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 4 & 3 & 11 \\ 0 & 0 & 2 & 4 \\ 0 & 0 & -3 & -6 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|c} 1 & 4 & 3 & 11 \\ 0 & 0 & 2 & 4 \\ 0 & 0 & 0 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 4 & 3 & 11 \\ 0 & 0 & 2 & 4 \end{array}\right).$$

V první úpravě jsme přičetli (-1)-násobek prvního řádku k druhému a (-2)-násobek prvního řádku k třetímu. V druhé úpravě jsme $(3/2)$-násobek druhého řádku přičetli k třetímu. Nakonec jsme jen vynechali poslední řádek, který odpovídá rovnici $0x_1 + 0x_2 + 0x_3 = 0$, která množinu řešení nemění. Vzniklá soustava rovnic je v nematicovém zápisu

$$\begin{aligned} x_1 + 4x_2 + 3x_3 &= 11 \\ 2x_3 &= 4 \ . \end{aligned}$$

Z poslední rovnice umíme spočítat $x_3 = 2$ a z první rovnice x_1, známe-li ovšem x_2. Proměnnou x_2 lze volit libovolně a budeme jí říkat *parametr*. Parametr označíme $t = x_2$ a vyjde $x_1 = 5 - 4t$. Množina všech řešení je tedy

$$\left\{ \begin{pmatrix} 5-4t \\ t \\ 2 \end{pmatrix} : t \in \mathbb{R} \right\} \ .$$

V našem konkrétním případě lze za parametr zvolit proměnnou $x_1 = s$, dopočítat $x_2 = 5/4 - s/4$ a získat množinu řešení ve tvaru $\{(s, 5/4 - s/4, 2)^T : s \in \mathbb{R}\}$. Nevýhodou této volby je, že by nefungovala, pokud by byl koeficient u x_2 v první rovnici roven nule. Volba parametrů, která funguje vždy bude diskutována u následujícího příkladu a pak v plné obecnosti v části 2.4.

Vraťme se ale k množině řešení $\{(5 - 4t, t, 2)^T : t \in \mathbb{R}\}$. Vektor $(5 - 4t, t, 2)^T$ lze pomocí sčítání a násobení skalárem vyjádřit také jako

$$\begin{pmatrix} 5-4t \\ t \\ 2 \end{pmatrix} = \begin{pmatrix} 5-4t \\ 0+t \\ 2+0t \end{pmatrix} = \begin{pmatrix} 5 \\ 0 \\ 2 \end{pmatrix} + \begin{pmatrix} -4t \\ t \\ 0t \end{pmatrix} = \begin{pmatrix} 5 \\ 0 \\ 2 \end{pmatrix} + t \begin{pmatrix} -4 \\ 1 \\ 0 \end{pmatrix} \ .$$

Takže množinu všech řešení lze napsat ve tvaru

$$\left\{ \begin{pmatrix} 5 \\ 0 \\ 2 \end{pmatrix} + t \begin{pmatrix} -4 \\ 1 \\ 0 \end{pmatrix} : t \in \mathbb{R} \right\} \ .$$

Tento tvar je lepší než předchozí. Vidíme z něj totiž, že řešením je přímka procházející bodem $(5, 0, 2)^T$ se směrovým vektorem $(-4, 1, 0)^T$.

Uvedený postup na hledání řešení soustavy nebudeme používat. Vektory $(5, 0, 2)^T$ a $(-4, 1, 0)^T$ lze totiž spočítat jednodušším způsobem, který teď popíšeme. Budeme potřebovat pojem *homogenní soustava rovnic*:

Definice 2.6. Soustava rovnic se nazývá *homogenní*, pokud všechny pravé strany jsou rovny nule.

Máme-li soustavu rovnic s rozšířenou maticí $(A \mid \mathbf{b})$, pak *příslušnou homogenní soustavou* rozumíme homogenní soustavu s maticí $(A \mid \mathbf{o})$, kde $\mathbf{o} = (0, 0, \ldots, 0)^T$ je *nulový vektor*.

Vraťme se ke tvaru rovnic po úpravách, čili

$$\left(\begin{array}{ccc|c} 1 & 4 & 3 & 11 \\ 0 & 0 & 2 & 4 \end{array}\right) \qquad \text{neboli} \qquad \begin{aligned} x_1 + 4x_2 + 3x_3 &= 11 \\ 2x_3 &= 4 \end{aligned}$$

Začneme určením parametrů. Je jeden, totiž proměnná x_2 (více k tomuto tématu níže). Množinu řešení budeme hledat ve tvaru $\{\mathbf{u} + t\mathbf{v} : t \in \mathbb{R}\}$. Vektor $\mathbf{u}$ určíme jako libovolné (tzv. *partikulární*) řešení soustavy. Většinou bývá nejjednoduší zvolit za parametr(y) nulu a zpětnou substitucí dopočítat zbylé proměnné. Vektor $\mathbf{v}$ je řešení **příslušné homogenní soustavy** při volbě parametru $t = 1$, spočítáme jej opět zpětnou substitucí. Prakticky můžeme postupovat tak, že napíšeme množinu všech řešení s doplněnými zvolenými parametry

$$\left\{ \begin{pmatrix} \cdot \\ 0 \\ \cdot \end{pmatrix} + t \begin{pmatrix} \cdot \\ 1 \\ \cdot \end{pmatrix} : t \in \mathbb{R} \right\}$$

a na prázdná místa doplňujeme odzadu zpětnou substitucí dopočtené hodnoty. Pozor na nejčastější chybu, totiž, že se při počítání druhého vektoru zapomene vynulovat pravá strana!

V našem případě dostaneme množinu řešení

$$\left\{ \begin{pmatrix} 5 \\ 0 \\ 2 \end{pmatrix} + t \begin{pmatrix} -4 \\ 1 \\ 0 \end{pmatrix} : t \in \mathbb{R} \right\} \ .$$

Vyšel nám stejný tvar výsledku jako předchozím postupem (není to náhoda). Nová metoda je daleko přehlednější a rychlejší, zejména máme-li větší soustavu.

Nakonec si ukážeme, že nalezená množina $S = \{(5,0,2)^T + t(-4,1,0)^T : t \in \mathbb{R}\}$ je skutečně rovná množině R všech řešení soustavy (aniž bychom porovnávali výsledek ze starším postupem).

- $S \subseteq R$. Je potřeba ukázat, že každý vektor v S je řešením soustavy. Podíváme se například na první rovnici. Vektor $\mathbf{u} = (u_1, u_2, u_3)^T = (5,0,2)^T$ byl zvolen jako řešení původní soustavy, tj.

(1) $$u_1 + 4u_2 + 3u_3 = 11 \ .$$

  Vektor $\mathbf{v} = (v_1, v_2, v_3)^T = (-4,1,0)^T$ je řešením příslušné homogenní soustavy, tj.

(2) $$v_1 + 4v_2 + 3v_3 = 0 \ .$$

  Vynásobením rovnice (2) číslem t a přičtením k (1) dostaneme

$$(u_1 + tv_1) + 4(u_2 + tv_2) + 3(u_3 + tv_3) = 11 \ ,$$

  neboli vektor $\mathbf{u} + t\mathbf{v}$ je řešením první rovnice. Je vidět, že důkaz nezávisí na volbě rovnice (a ani na volbě konkrétní soustavy).
- $R \subseteq S$. Nejprve si všimneme, že prvky množiny R jsou jednoznačně určeny hodnotou parametru (tedy druhou složkou vektoru). Skutečně, druhá rovnice (v odstupňovaném tvaru) určuje x_3 a první rovnice určuje x_1.

  Uvažujme nyní libovolné řešení $\mathbf{w} = (w_1, w_2, w_3)^T \in R$. V S rovněž existuje vektor, jehož druhá složka (odpovídající parametru) je w_2, totiž $\mathbf{w}' = (5,0,2)^T + w_2(-4,1,0)^T$. Již víme, že $S \subseteq R$, tedy $\mathbf{w}' \in R$. Druhé složky vektorů $\mathbf{w}$ a $\mathbf{w}'$ se rovnají, takže z poznámky v předchozím odstavci vyplývá, že $\mathbf{w} = \mathbf{w}'$. Protože $\mathbf{w}' \in S$, máme $\mathbf{w} \in S$, což jsme chtěli.

2.3.4. *Více parametrů.* Podíváme se na soustavu s více parametry, ze které již snad bude vidět obecný postup. Soustava bude mít pět neznámých $x_1, \ldots, x_5$, takže vizuální představa je stěží možná.

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

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

V první úpravě jsme prohodili řádky, aby byl na prvním místě v prvním řádku nenulový prvek. V druhé úpravě jsme (-2)-násobek prvního řádku přičetli ke druhému. Ve třetí úpravě jsme (-1)-násobek druhého řádku přičetli ke třetímu.

Soustava je teď v odstupňovaném tvaru. K volbě parametrů nejprve určíme *pivoty*, to jsou první nenulové prvky v každém řádku. Proměnné odpovídající sloupcům s pivotem se nazývají *bázové proměnné*. V našem případě jsou jimi x_1 a x_3. Zbylé proměnné jsou tzv. *volné proměnné*, v našem případě x_2, x_4, x_5. Volným proměnným také říkáme *parametry*. Protože máme tři volné proměnné, množina všech řešení bude tvaru

$$\{\mathbf{u} + t^{(2)}\mathbf{v}^{(2)} + t^{(4)}\mathbf{v}^{(4)} + t^{(5)}\mathbf{v}^{(5)} : t^{(2)}, t^{(4)}, t^{(5)} \in \mathbb{R}\} \ .$$

Vektor $\mathbf{u}$ (partikulární řešení) najdeme jako libovolné řešení soustavy, nejjednodušší bude zvolit za volné proměnné nuly. Vektory $\mathbf{v}^{(2)}, \mathbf{v}^{(4)}, \mathbf{v}^{(5)}$ budou řešení příslušné homogenní soustavy. Vektor $\mathbf{v}^{(2)}$ získáme volbou $(x_2, x_4, x_5) = (1,0,0)$, vektor $\mathbf{v}^{(4)}$ volbou $(x_2, x_4, x_5) = (0,1,0)$ a vektor $\mathbf{v}^{(5)}$ volbou $(x_2, x_4, x_5) = (0,0,1)$. Množinu všech řešení tedy hledáme ve tvaru

$$\left\{ \begin{pmatrix} \cdot \\ 0 \\ \cdot \\ 0 \\ 0 \end{pmatrix} + t^{(2)} \begin{pmatrix} \cdot \\ 1 \\ \cdot \\ 0 \\ 0 \end{pmatrix} + t^{(4)} \begin{pmatrix} \cdot \\ 0 \\ \cdot \\ 1 \\ 0 \end{pmatrix} + t^{(5)} \begin{pmatrix} \cdot \\ 0 \\ \cdot \\ 0 \\ 1 \end{pmatrix} : t^{(2)}, t^{(4)}, t^{(5)} \in \mathbb{R} \right\} \ .$$

Každý ze čtyřech vektorů dopočítáme zpětnou substitucí. Vyjde

$$\left\{ \begin{pmatrix} -1 \\ 0 \\ -3 \\ 0 \\ 0 \end{pmatrix} + t^{(2)} \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + t^{(4)} \begin{pmatrix} -3 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + t^{(5)} \begin{pmatrix} -2 \\ 0 \\ -2 \\ 0 \\ 1 \end{pmatrix} : t^{(2)}, t^{(4)}, t^{(5)} \in \mathbb{R} \right\} .$$

Důkaz, že nalezená množina je množinou všech řešení dané soustavy, by byl obdobný jako u předchozího případu. V druhé části bychom ukázali, že pro libovolné $\mathbf{w} = (w_1, w_2, \ldots, w_5)^T \in R$ existuje v S vektor, jenž se s $\mathbf{w}$ shoduje na druhé, čtvrté a páté pozici, totiž vektor $\mathbf{u} + w_2\mathbf{v}^{(2)} + w_4\mathbf{v}^{(4)} + w_5\mathbf{v}^{(5)}$. Proto byly hodnoty volných proměnných voleny uvedeným způsobem.

Při výpočtu na papíře je vhodné nalezené vektory zkontrolovat dosazením **do původních rovnic**.

2.4. **Řešení obecné soustavy rovnic Gaussovou eliminací.** Nyní představíme metodu řešení soustav lineárních rovnic ukázanou na předchozích příkladech v obecném případě.

2.4.1. *Odstupňovaný tvar.*

Definice 2.7. *Ekvivalentní úpravou* soustavy lineárních rovnic rozumíme úpravu, která nemění množinu všech řešení.

Při řešení soustav lineárních rovnic vystačíme s jednoduchými úpravami tří typů. Úpravy ve skutečnosti provádíme s řádky rozšířené matice soustavy, proto jim říkáme *elementární řádkové úpravy.*

Definice 2.8. *Elementárními řádkovými úpravami* soustavy lineárních rovnic (resp. její rozšířené matice) rozumíme následující tři typy úprav.

(i) prohození dvou rovnic (resp. řádků matice),
(ii) vynásobení jedné z rovnic (resp. jednoho z řádků) nenulovým číslem,
(iii) přičtení několikanásobku jedné rovnice (resp. jednoho řádku) k jiné rovnici (resp. k jinému řádku).

Tyto úpravy skutečně nemění množinu řešení:

Tvrzení 2.9. *Každá elementární řádková úprava soustavy lineárních rovnic je ekvivalentní úpravou.*

Důkaz. Označme S_1 resp. S_2 množinu všech řešení původní resp. nové soustavy. Je zřejmé, že každé řešení původní soustavy je řešením nové soustavy, neboli platí $S_1 \subseteq S_2$. K důkazu opačné inkluze si stačí uvědomit, že lze efekt úprav vrátit, tj. z nové soustavy jde dostat původní elementárními řádkovými úpravami. V případě (i) prohodíme stejné řádky, v případě (ii) vynásobíme stejnou rovnici inverzním číslem a přičtení t-násobku i-tého řádku k j-tému lze vrátit přičtením $(-t)$-násobku i-tého řádku k j-tému. □

Úpravu (i), tedy prohození dvou rovnic, lze docílit posloupností zbylých dvou úprav, viz cvičení.

Gaussova eliminační metoda na řešení soustav lineárních rovnic je založená na převodu soustavy na řádkově odstupňovaný tvar.

Definice 2.10. Matice $C = (c_{ij})_{m\times n}$ je v *řádkově odstupňovaném tvaru*, pokud existuje celé číslo $r \in \{0, 1, \ldots, m\}$ takové, že řádky $r+1, \ldots, m$ jsou nulové, řádky $1, \ldots, r$ jsou nenulové, a platí $k_1 < k_2 < \cdots < k_r$, kde k_i značí sloupec, ve kterém je první nenulové číslo v i-tém řádku (tedy platí $c_{i1} = c_{i2} = \cdots = c_{i,k_i-1} = 0$ a $c_{i,k_i} \neq 0$; ještě jinak, $k_i = \min\{l : c_{il} \neq 0\}$).

Prvkům c_{i,k_i}, $i = 1, 2, \ldots, r$ říkáme *pivoty.*

Soustava lineárních rovnic je v *řádkově odstupňovaném tvaru*, pokud její rozšířená matice je v řádkově odstupňovaném tvaru.

Jinak řečeno, nenulové řádky jsou na začátku (jejich počet je v definici označen r) a v každém nenulovém řádku (kromě prvního) je na začátku více nul než v předchozím.

OBRAZEK

Příklad 2.11. Matice

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 7 & 2 \\ 0 & 3 & 1 \\ 0 & 0 & 7 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 & 3 & 4 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 4 & 2 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 10 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

jsou v odstupňovaném tvaru. Matice

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 7 & 2 \\ 0 & 0 & 1 \\ 0 & 0 & 7 \end{pmatrix}, \begin{pmatrix} 2 & 3 & 1 \\ 0 & 3 & 1 \\ 0 & 2 & 0 \end{pmatrix}$$

v odstupňovaném tvaru nejsou.

Gaussova eliminace převede každou soustavu lineárních rovnic do odstupňovaného tvaru posloupností elementárních řádkových úprav. Algoritmus budeme raději předvádět na rozšířené matici soustavy. Nechť $C = (A \mid \mathbf{b})$ je rozšířená matice soustavy m rovnic o n neznámých, $C = (c_{ij})$.

Eliminace jednoho sloupce (jedné proměnné) proběhne následovně.

1. Najdeme první sloupec l, který není celý nulový. Pokud takový neexistuje, jsme hotovi.
2. Pokud je $c_{1l} = 0$, prohodíme první řádek s libovolným řádkem i, pro který $c_{il} \neq 0$.
3. Pro každé $k = 2, 3, \ldots, m$ přičteme $(-c_{kl}/c_{1l})$-násobek prvního řádku ke k-tému řádku.

(Všimněte si, že po provedení kroku 3 máme $c_{2l} = c_{3l} = \cdots = c_{ml} = 0$.) Dále postupujeme tak, jako bychom eliminovali matici bez prvního řádku. V dalším kroku tedy najdeme sloupec l', pro který je alespoň jedno z čísel $c_{2l'}, \ldots, c_{ml'}$ nenulové, řekněme $c_{ij} \neq 0, i \geq 2$. Prohodíme druhý a i-tý řádek a pak pro každé $k = 3, 4, \ldots, m$ přičteme $(-c_{kl'}/c_{2l'})$-násobek prvního řádku ke k-tému řádku. Gaussova eliminace končí buď v bodě 1, nebo ve chvíli, kdy dojdou řádky.

Věta 2.12. *Gaussova eliminace převede každou soustavu lineárních rovnic do odstupňovaného tvaru.*

Důkaz. Důkaz provedeme indukcí podle počtu rovnic. Předpokládejme tedy, že věta platí, pokud má soustava méně než m rovnic, a vezměme soustavu s m rovnicemi. Pokud tvoří rozšířenou matici soustavy samé nuly, pak se eliminace zastaví v bodě 1. a věta platí. Předpokládejme tedy, že tomu tak není.

Označme C rozšířenou matici soustavy po provedení eliminace jednoho sloupce, $D = (d_{ij})$ rozšířenou matici po provedení celé Gaussovy eliminace a C' (resp. $D' = (d'_{ij})$) matici, která vznikne z C (resp. D) vynecháním prvního řádku. Z algoritmu je patrné, že D' je matice, která vznikne z C' Gaussovou eliminací.

Podle indukčního předpokladu je D' v odstupňovaném tvaru. Podle definice tedy existuje r' takové, že D' má řádky $r'+1, \ldots, m-1$ nulové, řádky $1, \ldots, r'$ nenulové a $k'_1 < \cdots < k'_{r'}$, kde $k'_i = \min\{j : d'_{ij} \neq 0\}$. Položíme $r = r'+1$ a ověříme, že takové r splňuje definici odstupňovaného tvaru matice D. Nechť l je číslo prvního nenulového sloupce matice C nalezené v kroku 1. Protože $c_{1l} = d_{1l} \neq 0$, je první řádek matice D nenulový. Takže řádky $1, \ldots, r$ matice D jsou skutečně nenulové a řádky $r+1, \ldots, m$ nulové. Označme $k_i = \min\{j : d_{ij} \neq 0\}, i = 1, \ldots, r$. Potřebujeme ověřit, že $k_1 < \cdots < k_r$. Protože pro $i = 2, \ldots, r$ je $k_i = k'_{i-1}$, platí $k_2 < \cdots < k_r$. Zbylá nerovnost plyne z toho, že v matici C a tím pádem i D máme prvních $l-1$ sloupců nulových a pro l-tý sloupec platí $d_{1l} \neq 0$ a $d_{2l} = \cdots = d_{ml} = 0$. Je tedy $k_1 = l$ a $k_2, \ldots, k_r > l$. □

2.4.2. *Dopočítání řešení.* Mějme nyní soustavu m lineárních rovnic o n neznámých $x_1, \ldots, x_n$ s rozšířenou maticí $C = (A \mid \mathbf{b})$ v odstupňovaném tvaru. Nechť r, $k_1, \ldots, k_r$ jsou čísla z definice 2.10, tj. číslo r udává počet nenulových řádků a čísla $k_1, \ldots, k_r$ pozice pivotů.

Pokud $k_r = n+1$, jinými slovy, pokud poslední nenulový řádek rozšířené matice soustavy je tvaru $(0\ 0\ \ldots 0|b_r)$, kde $b_r \neq 0$, pak soustava $(A \mid \mathbf{b})$ nemá žádné řešení: tato rovnice říká $0x_1 + 0x_2 + \ldots, 0x_n = b_r \neq 0$, což zřejmě nejde.

Předpokládejme odteď, že $k_r < n+1$. Ukážeme, že soustava $(A \mid \mathbf{b})$ má alespoň jedno řešení, a ukážeme, jak všechna řešení popsat.

Označme P množinu těch sloupců od 1 do n, které neobsahují pivot, tj.

$$P = \{1, 2, \ldots, n\} \setminus \{k_1, \ldots, k_r\} \ .$$

Proměnným $x_p, p \in P$ říkáme volné proměnné (nebo též parametry). Ostatní proměnné, tj. proměnné $x_{k_1}, x_{k_2}, \ldots, x_{k_r}$ jsou bázové.

Nyní nahlédneme, že každá volba hodnot volných proměnných dává právě jedno řešení soustavy $(A \mid \mathbf{b})$. Soustava je tvaru

$$\begin{aligned} a_{1,k_1}x_{k_1} + a_{1,k_1+1}x_{k_1+1} + \cdots + a_{1,n}x_n &= b_1 \\ a_{2,k_2}x_{k_2} + a_{2,k_2+1}x_{k_2+1} + \cdots + a_{2,n}x_n &= b_2 \\ &\vdots \\ a_{r,k_r}x_{k_r} + a_{r,k_r+1}x_{k_r+1} + \cdots + a_{r,n}x_n &= b_r \ , \end{aligned}$$

což je ekvivalentní soustavě rovnic

$$\begin{aligned} x_{k_1} &= a_{1,k_1}^{-1}(b_1 - a_{1,k_1+1}x_{k_1+1} - \ldots - a_{1,n}x_n) \\ x_{k_2} &= a_{2,k_2}^{-1}(b_2 - a_{2,k_2+1}x_{k_2+1} - \ldots - a_{2,n}x_n) \\ &\vdots \\ x_{k_r} &= a_{r,k_r}^{-1}(b_r - a_{r,k_r+1}x_{k_r+1} - \ldots - a_{r,n}x_n) \ . \end{aligned}$$

Poslední rovnice jednoznačně určuje x_{k_r}, předposlední rovnice jednoznačně určuje $x_{k_{r-1}}$, atd. Tomuto dopočítávání hodnot říkáme zpětná substituce. Stejnou úvahu lze provést pro libovolný vektor pravých stran $\mathbf{c}$. Dokázali jsme následující pozorování.

Pozorování 2.13. *Pro libovolný vektor pravých stran* $\mathbf{c}$ *a libovolná reálná čísla* $x_p \in \mathbb{R}$, $p \in P$ *existují jednoznačně určená reálná čísla* $x_{k_1}, x_{k_2}, \ldots, x_{k_r} \in \mathbb{R}$ *taková, že aritmetický vektor* $(x_1, x_2, \ldots, x_n)$ *je řešením soustavy* $(A \mid \mathbf{c})$.

Jsme připraveni najít množinu všech řešení. Najdeme libovolné řešení $\mathbf{u}$ soustavy $(A \mid \mathbf{b})$ a pro každé $p \in P$ najdeme řešení $\mathbf{v}^{(p)} = (v_1^{(p)}, v_2^{(p)}, \ldots, v_n^{(p)})$ příslušné homogenní soustavy (tj. soustavy $(A \mid \mathbf{o})$), pro které platí $v_p^p = 1$ a $v_q^p = 0$ pro každé $q \in P, q \neq p$. Vektory $\mathbf{u}, \mathbf{v}^{(p)}, p \in P$ získáme zpětnou substitucí.

Věta 2.14. *Množina všech řešení soustavy* $(A \mid \mathbf{b})$ *je rovná množině*

$$S = \left\{ \mathbf{u} + \sum_{p \in P} t^{(p)}\mathbf{v}^{(p)} : (\forall p \in P)\ t^{(p)} \in \mathbb{R} \right\} \ .$$

Důkaz. Nejprve ukážeme, že množina

$$S_0 = \left\{ \sum_{p \in P} t^{(p)}\mathbf{v}^{(p)} : (\forall p \in P)\ t^{(p)} \in \mathbb{R} \right\}$$

je rovná množině R_0 všech řešení příslušné homogenní soustavy $(A \mid \mathbf{o})$. Budeme používat následující jednoduchá pozorování, jejichž důkazy přenecháme čtenáři jako cvičení.

(p1) Je-li vektor $\mathbf{w}$ řešením soustavy $(A \mid \mathbf{o})$ a $t \in \mathbf{R}$, pak je vektor $t\mathbf{w}$ řešením soustavy $(A \mid \mathbf{o})$.
(p2) Jsou-li vektory $\mathbf{w}, \mathbf{z}$ řešením soustavy $(A \mid \mathbf{o})$, pak je vektor $\mathbf{w} + \mathbf{z}$ řešením soustavy $(A \mid \mathbf{o})$.

Dokážeme inkluze $S_0 \subseteq R_0$ a $R_0 \subseteq S_0$.

- $S_0 \subset R_0$. Musíme dokázat, že pro libovolná čísla $t^{(p)}$ je vektor $\sum_{p \in P} t^{(p)}\mathbf{v}^{(p)}$ řešením soustavy $(A \mid \mathbf{o})$. Nechť tedy $t^{(p)} \in \mathbb{R}$ jsou libovolná čísla. Pro každé $p \in P$ je vektor $\mathbf{v}^{(p)}$ řešením $(A \mid \mathbf{o})$, takže je řešením této soustavy také vektor $t^{(p)}\mathbf{v}^{(p)}$ (podle (p1)) a proto je řešením také vektor $\sum_{p \in P} t^{(p)}\mathbf{v}^{(p)}$ (to plyne několikanásobnou aplikací (p2)).
- $R_0 \subseteq S_0$. Vezmeme libovolný vektor $\mathbf{w} = (w_1, w_2, \ldots, w_n)^T \in R$ a ukážeme, že leží v množině S_0. Uvažujme vektor

  $$\mathbf{w}' = \sum_{p \in P} w_p\mathbf{v}^{(p)} \ .$$

  Vektor $\mathbf{w}' = (w_1', w_2', \ldots, w_n')^T$ leží v S_0 podle definice této množiny. V předchozí části důkazu jsme ukázali, že $S_0 \subseteq R_0$, tedy $\mathbf{w}'$ leží také v R_0. Nyní si uvědomíme, že pro každé $q \in P$ platí $w_q' = w_q$. Skutečně:

  $$w_q' = \sum_{p \in P} w_p v_q^{(p)} = w_q v_q^{(q)} + \sum_{p \in P \setminus \{q\}} w_p v_q^{(p)} =$$

  $$= w_q \cdot 1 + \sum_{p \in P \setminus \{q\}} w_p \cdot 0 = w_q \ .$$

  Z toho podle pozorování 2.13 vyplývá $\mathbf{w} = \mathbf{w}'$. Protože $\mathbf{w}' \in S_0$, je také $\mathbf{w} \in S_0$ a jsme hotovi.

Přejdeme k samotnému důkazu, že množina S je rovná množině R všech řešení soustavy $(A \mid \mathbf{b})$. K důkazu opět využijeme dvě snadná pozorování.

(p3) Pokud je vektor $\mathbf{w}$ řešením soustavy $(A \mid \mathbf{b})$ a vektor $\mathbf{z}$ řešením soustavy $(A \mid \mathbf{o})$, pak je vektor $\mathbf{w} + \mathbf{z}$ řešením soustavy $(A \mid \mathbf{b})$.
(p4) Pokud jsou vektory $\mathbf{w}, \mathbf{z}$ řešením soustavy $(A \mid \mathbf{b})$, pak je vektor $\mathbf{w} - \mathbf{z}$ řešením soustavy $(A \mid \mathbf{o})$.

Dokážeme, že $S \subseteq R$ a $R \subseteq S$.

- $S \subseteq R$. Již jsme dokázali (viz inkluzi $S_0 \subseteq R_0$), že pro libovolná čísla $t^{(p)} \in \mathbb{R}$ je vektor $\sum_{p\in P} t^{(p)}\mathbf{v}^{(p)}$ řešením soustavy $(A \mid \mathbf{o})$. Navíc vektor $\mathbf{u}$ řeší soustavu $(A \mid \mathbf{b})$, takže, podle (p3), je vektor $\mathbf{u}+\sum_{p\in P} t^{(p)}\mathbf{v}^{(p)}$ řešením soustavy $(A \mid \mathbf{b})$.
- $R \subseteq S$. Uvažujme libovolný vektor $\mathbf{w} \in R$. Podle (p4) je vektor $\mathbf{w} - \mathbf{u}$ řešením $(A \mid \mathbf{o})$, tedy patří do S_0. Protože $R_0 \subseteq S_0$, existují čísla $t^{(p)} \in \mathbb{R}$ taková, že $\mathbf{w} - \mathbf{u} = \sum_{p\in P} t^{(p)}\mathbf{v}^{(p)}$, z čehož po převodu $\mathbf{u}$ na pravou stranu dostáváme $\mathbf{w} \in S$.

□

2.4.3. *Shrnutí.* Obecnou soustavu lineárních rovnic o n neznámých lze vyřešit následujícím postupem.

1. Gaussovou eliminací převedeme soustavu na ekvivalentní soustavu v odstupňovaném tvaru.
2. Rozhodneme, zda soustava má řešení. Pokud ne, tj. existuje rovnice typu $0x_1 + 0x_2 + \cdots + 0x_n = b \neq 0$, skončíme.
3. Určíme volné proměnné (parametry) – proměnné odpovídající sloupcům, kde nejsou pivoty. Množinu těchto sloupců označíme P.
4. Množina všech řešení je
$$\left\{ \mathbf{u} + \sum_{p\in P} t^{(p)}\mathbf{v}^{(p)} : (\forall p \in P)\ t^{(p)} \in \mathbb{R} \right\} ,$$
kde $\mathbf{u}$ je libovolné řešení soustavy a $\mathbf{v}^{(p)}$ je řešení příslušné homogenní soustavy, kde za parametr odpovídající sloupci p volíme 1 a za zbylé parametry volíme 0. Každý z vektorů spočítáme zpětnou substitucí.

Všimněte si, že počet volných proměnných je roven číslu $n - r$, kde r je počet nenulových řádků v odstupňovaném tvaru. Zatím neumíme dokázat, že toto číslo nezávisí na tom, jaké ekvivalentní úpravy používáme k převodu na odstupňovaný tvar. Nicméně je tomu tak, toto číslo je rovné tzv. *hodnosti* (rozšířené) matice soustavy. Intuitivně to lze zdůvodnit tak, že v popisu množiny řešení máme $n-r$ parametrů, takže množina řešení je $(n-r)$-dimenzionální objekt, přičemž tato dimenze samozřejmě závisí jen na původní soustavě, nikoliv na konkrétním odstupňovaném tvaru.

Na popsaný postup na řešení rovnic se dá také dívat takto: Na začátku máme rovnicový popis „rovného útvaru“ v n-rozměrném prostoru, v bodě 1. nalezneme kompaktnější rovnicový popis stejného útvaru a v bodě 4. nalezneme jeho parametrický popis.

Příklad 2.15. Najděte všechna řešení soustavy lineárních rovnic s rozšířenou maticí

()

2.5. **Praktické problémy při řešení rovnic.**

2.5.1. *Numerická stabilita.* Při počítání soustav lineárních rovnic na počítači často reprezentujeme reálná čísla s nějakou předem určenou přesností. Problémem je, že Gaussova eliminace je obecně *numericky nestabilní*. To znamená, že malé zaokrouhlovací chyby mohou vést k výsledku, který se velmi liší od správného. Uvažujme například soustavu
$$\left(\begin{array}{cc|c} -10^{-4} & 1 & 1 \\ 1 & 1 & 2 \end{array}\right),$$
jejímž přesným řešením je
$$\left(\frac{1}{1{,}0001}, \frac{1{,}0002}{1{,}0001}\right)^T .$$
Pokud použijeme aritmetiku s třemi platnými ciframi, Gaussova eliminace nám dá
$$\left(\begin{array}{cc|c} -10^{-4} & 1 & 1 \\ 1 & 1 & 2 \end{array}\right) \sim \left(\begin{array}{cc|c} -10^{-4} & 1 & 1 \\ 0 & 10^4 & 10^4 \end{array}\right)$$
a zpětnou substitucí dostaneme řešení $(0, 1)^T$, které se od správného liší významně v první složce. Problémem je, že jsme při úpravě přičítali 10^4-násobek prvního řádku k druhému a číslo 10^4 je tak velké, že smaže pro danou soustavu podstatný rozdíl mezi 1 a 2 na pravých stranách. Tomuto problému lze předejít tak, že vždy před eliminací jedné proměnné prohodíme řádky tak, aby pivot byl co největší (v absolutní hodnotě). Tato tzv. *částečná pivotace* ale nezamezí všem problémům s numerickou stabilitou. Příkladem může být soustava
$$\left(\begin{array}{cc|c} -10 & 10^5 & 10^5 \\ 1 & 1 & 2 \end{array}\right),$$
která vznikne z předchozí vynásobením první rovnice číslem 10^5. Řešení při použití aritmetiky se třemi platnými ciframi vyjde opět $(0, 1)^T$ a částečná pivotace tomuto problému nezamezí (řádky jsou již od začátku ve správném

pořadí). U tohoto příkladu je problém ve značném rozdílu ve velikosti prvního řádku a druhého řádku. Těmto i dalším typům problémů lze zamezit *úplnou pivotací*, při níž prohodíme před eliminací řádky a sloupce tak, aby pivot byl co největší. Úplná pivotace je numericky stabilní v každém případě. Při prohození sloupců nesmíme zapomenout na to, že vlastně prohazujeme proměnné.

2.5.2. *Špatně podmíněné soustavy.* Jiný typ problémů ukážeme na soustavě

$$\left(\begin{array}{cc|c} 0{,}835 & 0{,}667 & 0{,}168 \\ 0{,}333 & 0{,}266 & 0{,}067 \end{array}\right),$$

jejíž řešením je $(1,-1)^T$. Pokud číslo $0{,}067$ jen nepatrně změníme na hodnotu $0{,}066$, řešení se změní na $(-666,\ 834)^T$. Důvodem tohoto drastického rozdílu je, že přímky určené rovnicemi jsou téměř rovnoběžné, takže malá změna jedné z nich může posunout průnik daleko od původního.

OBRAZEK

Soustavám, jejíž řešení je velmi citlivé na malou změnu koeficientů, říkáme *špatně podmíněné*. U špatně podmíněných soustav nám nepomůže ani numericky velmi stabilní algoritmus, protože koeficienty jsou v praxi většinou získány měřením, takže jsou zatíženy chybou. Je proto zapotřebí změnit model, navrhnout jiný experiment, apod., abychom se vyhnuli špatně podmíněným soustavám.

Cvičení

1. Dokažte, že prohození dvou rovnic lze docílit zbylými dvěmi elementárními řádkovými úpravami.

2. Dokažte pozorování (p1–4) z důkazu věty 2.14. Navrhněte zobecnění.

3. SLOZITOST

3. Tělesa

Cíl. *Studiem vlastností reálných čísel, které používáme při řešení soustav lineárních rovnic, dojdeme k pojmu tělesa. Ukážeme si několik důležitých příkladů těles.*

3.1. **Motivace.**

V minulé kapitole jsme řešili soustavy lineárních rovnic nad reálnými čísly. Zcela stejný postup lze využít pro řešení soustav lineárních rovnic nad jinými obory, například komplexními čísly. Obecně lze stejný postup použít nad libovolným *tělesem*. Těleso je tedy struktura, ve které jsou definované operace sčítání a násobení mající podobné vlastnosti jako reálná čísla, konkrétněji máme na mysli ty vlastnosti reálných čísel, které využíváme při řešení soustav lineárních rovnic.

Zamysleme se nejprve jaké vlastnosti reálných čísel využíváme při řešení rovnice $x + a = b$, konkrétně třeba

$$x + 11 = 18 \ .$$

Snažíme se odhlédnout od toho, že řešení okamžitě vidíme a že některé vlastnosti reálných čísel již používáme zcela automaticky.

Většina z nás by na tomto místě navrhla odečíst od obou stran číslo 11. My se budeme snažit vystačit se dvěmi základními operacemi, sčítáním a násobením. Ostatní operace, jako odčítání a dělení, budeme považovat za odvozené. Proto k oboum stranám raději přičteme číslo -11. Protože jsme zapomněli na komutativitu sčítání, musíme se domluvit, z které strany přičítáme. V našem případě potřebujeme přičíst zprava. Dostáváme

$$(x + 11) + (-11) = 7 \ ,$$

přičemž na pravé straně jsme rovnou spočítali, že $18 + (-11) = 7$. Dalším krokem je přezávorkování levé strany:

$$x + (11 + (-11)) = 7 \ .$$

Teď můžeme závorku vypočítat:

$$x + 0 = 7 \ .$$

Nakonec využijeme skutečnosti, že $x + 0 = x$ a dostáváme

$$x = 7 \ .$$

(Teď bychom ještě buď ověřili, že 7 je opravdu řešením, případně nahlédli, že úpravy jsou vratné.)

Při řešení rovnic typu $x + a = b$ tedy využíváme asociativitu sčítání, existenci neutrálního prvku a existenci opačných prvků. Přesněji řečeno, využíváme následující vlastnosti:

(S1) („asociativita sčítání“) Pro libovolná čísla $a, b, c \in \mathbb{R}$ platí $(a + b) + c = a + (b + c)$.
(S2) („existence nulového prvku“) Existuje číslo $0 \in \mathbb{R}$ takové, že pro libovolné $a \in \mathbb{R}$ platí $0 + a = a + 0 = a$.
(S3) („existence opačného prvku“) Pro každé $a \in \mathbb{R}$ existuje $b \in \mathbb{R}$ takové, že $a + b = b + a = 0$. (Takové b značíme $-a$.)

Pointa je v tom, že kdykoliv máme na nějaké množině operaci $+$ s těmito vlastnostmi, pak můžeme na řešení rovnic typu $x + a = b$ (nebo $a + x = b$) použít zcela stejný postup. (Binární) operací na množině T se rozumí jakékoliv zobrazení, které každé dvojici prvků z T jednoznačně přiřadí prvek T. Formálně:

Definice 3.1. *Binární operací* na množině T rozumíme zobrazení z $T \times T$ do T.

Je-li $\oplus$ binární operace na T, pak její hodnotu na dvojici (a, b) zapisujeme většinou $a \oplus b$, místo $\oplus(a, b)$, nebo formálně ještě správnějšího $\oplus((a, b))$.

Všimněte si, že $a \oplus b$ musí být definované pro každou dvojici $a, b \in T$ a že výsledek operace je opět prvek T. Pokud má $\oplus$ vlastnost (S1), pak ve výrazech typu $a_1 \oplus a_2 \oplus \cdots \oplus a_n$ nemusíme psát závorky, protože každé smysluplné uzávorkování dá stejný výsledek (důkaz je technicky docela náročný, nebudeme jej provádět). Obecně však nemůžeme beztrestně prohazovat pořadí.

Příklady množin a operací splňující (S1), (S2), (S3) jsou

- $T = \mathbb{Z}$ a $+$ je běžné sčítání.
- Podobně $T = \mathbb{Q}$ (nebo $T = \mathbb{R}$, nebo $T = \mathbb{C}$) a $+$ je běžné sčítání.
- Větším příkladem je množina všech reálných funkcí reálné proměnné s operací sčítání funkcí.
- Naopak velmi malým příkladem je $T = \{0, 1\}$ s operací $\oplus$ definovanou $0 \oplus 0 = 1 \oplus 1 = 0$ a $0 \oplus 1 = 1 \oplus 0 = 1$.
- Zcela odlišným příkladem pak je množina všech permutací na nějaké pevné množině s operací $\circ$ skládání permutací. Tento příklad vybočuje tím, že operace není komutativní (tj. nesplňuje $a \circ b = b \circ a$).

Vraťme se nyní k problému, které vlastnosti reálných čísel využíváme při řešení soustav lineárních rovnic. Uvažujme rovnici typu $x \cdot a = b$, například $x \cdot 3 = 12$. Postup řešení je následující.

$$\begin{aligned} x \cdot 3 &= 12 \\ (x \cdot 3) \cdot 3^{-1} &= 4 \\ x \cdot (3 \cdot 3^{-1}) &= 4 \\ x \cdot 1 &= 4 \\ x &= 4 \end{aligned}$$

Všimněte si, že postup je velmi podobný postupu na řešení rovnice $x + a = b$. Rozdíl je v tom, že místo operace $+$ pracujeme s operací $\cdot$, místo 0 používáme prvek 1 a místo $-x$ používáme x^{-1}. Vlastnosti $\cdot$, které využíváme, jsou proto velmi podobné vlastnostem (S1), (S2), (S3) s jedním důležitým rozdílem – obdoba vlastnosti (S3), což je existence inverzního prvku, platí pouze pro nenulová čísla. Použité vlastnosti jsou následující.

(N1) („asociativita násobení“) Pro libovolná čísla $a, b, c \in \mathbb{R}$ platí $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
(N2) („existence jednotkového prvku“) Existuje číslo $1 \in \mathbb{R}$ takové, že pro libovolné $a \in \mathbb{R}$ platí $1 \cdot a = a \cdot 1 = x$.
(N3) („existence inverzního prvku“) Pro každé $a \in \mathbb{R}$ takové, že $a \neq 0$, existuje $b \in \mathbb{R}$ takové, že $a \cdot b = b \cdot a = 1$. (Takové b značíme a^{-1}.)

Při elementárních úpravách používáme ještě dvě další vlastnosti. Ty lze vidět například z úprav, které mlčky probíhají při přičítání 2-násobku rovnice $x + 3y = 10$ k rovnici $(-2)x + 4y = 15$. V úpravách již využíváme (S1) a (N1), takže nepíšeme závorky.

$$\begin{aligned} 2(x + 3y) + (-2)x + 4y &= 35 \\ 2x + 2 \cdot 3y + (-2)x + 4y &= 35 \\ 2x + 6y + (-2)x + 4y &= 35 \\ 2x + (-2)x + 6y + 4y &= 35 \\ (2 + (-2))x + (6 + 4)y &= 35 \\ 0x + 10y &= 35 \\ 0 + 10y &= 35 \\ 10y &= 35 \end{aligned}$$

Kromě již formulovaných vlastností jsme využili tyto:

(D) („oboustranná distributivita“) Pro libovolná čísla $a, b, c \in \mathbb{R}$ platí $a \cdot (b+c) = a \cdot b + a \cdot c$ a $(b+c) \cdot a = b \cdot a + c \cdot a$.
(S4) („komutativita sčítání“) Pro libovolná čísla $a, b \in \mathbb{R}$ platí $a + b = b + a$.

Ještě jsme využili, že $0 \cdot x = 0$. Později však ukážeme, že tento vztah plyne ze zbylých vlastností.

Shrneme-li všechny doposud zformulované vlastnosti, dostaneme pojem *nekomutativního tělesa*. Nikde jsme totiž nevyužili komutativitu násobení a soustavy lineárních rovnic lze Gaussovou eliminací řešit i nad nekomutativními tělesy, jen bychom se museli dohodnout, zda koeficienty v rovnicích budeme psát zleva nebo zprava. Rovnice $ax = b$ totiž může mít jiné řešení než rovnice $xa = b$. Důležitým příkladem nekomutativního těleso je těleso kvaternionů, viz níže.

My ale budeme pracovat s tělesy, kde násobení je komutativní, proto do definice tělesa tuto vlastnost přidáme. Tím pádem stačí vyžadovat jen jeden z distributivních zákonů a můžeme také zjednodušit vlastnosti (S2), (S3), (N2) a (N3). Ještě přidáme tzv. axiom netriviality, tj. požadavek že těleso má alespoň 2 prvky. Jednoprvkovou množinu totiž za těleso nechceme považovat.

3.2. **Definice tělesa.**

Definice 3.2. *Tělesem* **T** rozumíme množinu T spolu s dvěmi binárními operacemi $+, \cdot$ na T, které splňují následující axiomy.

(S1) („asociativita sčítání“) Pro libovolné prvky $a, b, c \in T$ platí $(a + b) + c = a + (b + c)$.
(S2) („existence nulového prvku“) Existuje prvek $0 \in T$ takový, že pro libovolné $a \in T$ platí $a + 0 = a$.
(S3) („existence opačného prvku“) Pro každé $a \in T$ existuje $-a \in T$ takové, že $a + (-a) = 0$.
(S4) („komutativita sčítání“) Pro libovolné prvky $a, b \in T$ platí $a + b = b + a$.
(N1) („asociativita násobení“) Pro libovolné prvky $a, b, c \in T$ platí $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
(N2) („existence jednotkového prvku“) Existuje prvek $1 \in T$ takový, že pro libovolné $a \in T$ platí $a \cdot 1 = a$.
(N3) („existence inverzního prvku“) Pro každé $0 \neq a \in T$ existuje $a^{-1} \in T$ takové, že $a \cdot a^{-1} = 1$.
(N4) („komutativita násobení“) Pro libovolné prvky $a, b \in T$ platí $a \cdot b = b \cdot a$.

(D) („distributivita“) Pro libovolné prvky $a, b, c \in T$ platí $a \cdot (b + c) = a \cdot b + a \cdot c$.
($\neg$ T) („netrivialita“) $|T| > 1$.

Prvek 0 z axiomu (S2) též nazýváme *neutrální prvek vzhledem k operaci* $+$ a prvek 1 z axiomu (N2) je *neutrální prvek vzhledem k* $\cdot$. V následujícím tvrzení ukážeme, že jsou určeny jednoznačně. Tyto jednoznačně určené prvky pak vystupují v axiomech (S3) a (N3).

Formulace (S3) může být trochu matoucí. Přesněji bychom měli říct, že pro každé $a \in T$ existuje $b \in T$ takové, že $a + b = 0$, a poté libovolné takové b označit $-a$. V následujícím tvrzení dokážeme, že $b = -a$ je pro dané a určeno jednoznačně. Podobně pro inverzní prvky.

Stejně jak je běžné u reálných čísel, prvek $a \cdot b$ často značíme jen ab. Definujeme

$$a - b = a + (-b) \quad \text{a} \quad \frac{a}{b} = ab^{-1}.$$

Těleso je zadané množinou T **a** určením dvou binárních operací $+$ a $\cdot$ na množině T. Samotná množina těleso neurčuje. Rovněž poznamenejme, že vzhledem k definici binární operace (definice 3.1) musí být $a+b$ a ab definované pro každou dvojici prvků $a, b \in T$ a výsledek musí ležet v množině T.

Příkladem tělesa je množina racionálních (nebo reálných, nebo komplexních) čísel spolu s běžnými operacemi. Množina celých čísel spolu s běžnými operacemi těleso netvoří kvůli axiomu (N3). Dříve než se podíváme na další příklady, dokážeme několik jednoduchých vlastností, které mají všechna tělesa.

Tvrzení 3.3. *V každém tělese* **T** *platí*

(1) *nulový prvek je určený jednoznačně,*
(2) *rovnice $a + x = b$ má vždy právě jedno řešení, speciálně, opačný prvek $-a$ je prvkem $a \in T$ určený jednoznačně,*
(3) *jednotkový prvek je určený jednoznačně,*
(4) *rovnice $ax = b$, $a \neq 0$, má vždy právě jedno řešení, speciálně, prvek a^{-1} inverzní k prvku $0 \neq a \in T$, je prvkem a určený jednoznačně,*
(5) *$0a = 0$ pro libovolný prvek $a \in T$,*
(6) *je-li $ab = 0$, pak buď $a = 0$ nebo $b = 0$,*
(7) *$(-1)a = -a$ pro každý prvek $a \in T$,*
(8) *z rovnosti $a + b = a + c$ plyne $b = c$,*
(9) *z rovnosti $ab = ac$ a předpokladu $a \neq 0$, vyplývá $b = c$,*
(10) *$0 \neq 1$*

Důkaz. (1) Předpokládejme, že 0 a $0'$ jsou prvky, pro které $a + 0 = a = a + 0'$ pro libovolné $a \in T$. Pak platí

$$0 = 0' + 0 = 0 + 0' = 0'.$$

V první rovnosti jsme využili, že $a = a + 0$ pro libovolné a (využili jsme to pro $a = 0'$), ve druhé rovnosti využíváme komutativitu sčítání (axiom (S3)) a ve třetí rovnosti využíváme, že $a + 0' = a$ (pro $a = 0$).

Tedy $0 = 0'$, což jsme chtěli.

(2) Vezmeme libovolné $a, b \in T$ a předpokládáme, že $x \in T$ i $x' \in T$ splňují $a + x = b$ a $a + x' = b$. Přičteme k oběma stranám rovnosti $a + x = a + x'$ libovolný pevně zvolený opačný prvek $-a$ k a, použijeme asociativitu sčítání a axiomy (S3),(S4) a (S2). Dostáváme

$$\begin{aligned} a + x &= a + x' \\ (-a) + (a + x) &= (-a) + (a + x') \\ ((-a) + a) + x &= ((-a) + a) + x' \\ 0 + x &= 0 + x' \\ x &= x' \ . \end{aligned}$$

Tvrzení o jednoznačnosti opačného prvku dostaneme volbou $b = 0$.

(3) Obdobně jako (1)
(4) Obdobně jako (2)
(5) Pro libovolné a máme užitím (D)

$$0a + 0a = (0 + 0)a = 0a.$$

Rovnice $0a + x = 0a$ má tedy řešení $x = 0a$, ale také $x = 0$ podle axiomu (S2). Z bodu (2) nyní vyplývá $0a = 0$.

(6) Předpokládejme, že $ab = 0$ a $a \neq 0$ a dokážeme, že $b = 0$. Rovnice $ax = 0$ má řešení $x = b$ a také $x = 0$ podle předešlého bodu. Takže $0 = b$ podle bodu (2).
(7) Je třeba ukázat, že $(-1)a$ je opačný prvek k a. Pak tvrzení plyne z jednoznačnosti opačného prvku (bod (2)). Skutečně
$$a + (-1)a = 1a + (-1)a = (1 + (-1))a = 0a = 0,$$
kde jsme využili (N2), (D), (S3) a předchozí bod.
(8) Rovnice $a + x = (a + c)$ má řešení $x = c$ (zřejmě) a $x = b$ (podle předpokladu). Z bodu (2) plyne $b = c$.
(9) Podobně jako předešlý bod.
(10) Pokud $0 = 1$, pak vynásobením obou stran libovolným číslem a a užitím (5) a (N2) dostaneme $0 = 0a = 1a = a$. Tedy každý prvek je roven nulovému, takže $|T| = 1$.

□

Další společné vlastnosti těles jsou ve cvičeních.

3.3. **Tělesa $\mathbb{Z}_p$.**

Důležitými příklady těles jsou tělesa $\mathbb{Z}_p$, kde p je prvočíslo. Tato a jiná konečná tělesa mají aplikace například v informatice při studiu kódů nebo k návrhu rychlých algoritmů pro počítání s celočíselnými polynomy.

Těleso $\mathbb{Z}_p$ má prvky $0, 1, 2, \ldots, p-1$ (má tedy p prvků) a operace $\oplus, \odot$ jsou definovány
$$a \oplus b = (a + b) \bmod p, \quad a \odot b = (a \cdot b) \bmod p.$$
Na levých stranách jsou operace v $\mathbb{Z}_p$, které definujeme, a na pravých stranách jsou běžné operace v $\mathbb{Z}$. Připomeňme, že $c \bmod p$ značí zbytek po dělení čísla c číslem p. Tento zbytek je vždy v množině $0, 1, \ldots, p-1$, takže operace jsou dobře definovány.

Ve skutečnosti pro zápis operací $\oplus, \odot$ používáme symboly $+, \cdot$. Z kontextu je třeba rozhodnout, ve kterém tělese počítáme. Například v $\mathbb{Z}_5$ máme
$$0 + 0 = 0,\ 1 + 4 = 0,\ 3 + 4 = 2,\ 2 \cdot 2 = 4,\ 2 \cdot 3 = 1,\ 3 \cdot 3 = 4, \ldots \ .$$

Věta 3.4. *Pro libovolné prvočíslo p tvoří množina $\mathbb{Z}_p$ spolu s výše definovanými operacemi těleso.*

Důkaz. Ověření téměř všech axiomů tělesa je vcelku snadné a přenecháme to do cvičení.

Dokážeme pouze axiom (N3) o existenci inverzních prvků. Nechť $0 \neq a \in \mathbb{Z}_p$, neboli $a \in \{1, 2, \ldots, p-1\}$. Chceme najít inverzní prvek k a. Protože p je prvočíslo a $0 < a < p$, platí $\gcd(a, p) = 1$. Podle Bezoutovy věty (věta **??**)existují čísla $s, t \in \mathbb{Z}$ taková, že $sa + tp = 1$. Tvrdíme, že $(s \bmod p)$ je inverzním prvkem k a. Platí
$$(s \bmod p)a \equiv sa = 1 - tp \equiv 1 \pmod p,$$
(kde všechny operace jsou běžné operace s celými čísly) neboli $(s \bmod p)a \bmod p = 1$. Z toho plyne, že $(s \bmod p)a = 1$ v $\mathbb{Z}_p$. □

Důkaz také dává návod na hledání inverzních prvků. Pokud p je malé, je asi nejrychlejší určovat inverzní prvky zkusmo.

Příklad 3.5. V tělese $\mathbb{Z}_5$ máme
$$1^{-1} = 1,\ 2^{-1} = 3,\ 3^{-1} = 2,\ 4^{-1} = 4 \ .$$
V tělese $\mathbb{Z}_7$ je
$$1^{-1} = 1,\ 2^{-1} = 4,\ 3^{-1} = 5,\ 4^{-1} = 2,\ 5^{-1} = 3,\ 6^{-1} = 6 \ .$$

Inverzní prvky jsme našli zkusmo, například $2^{-1} = 3$, protože $2 \cdot 3 = 1$. Uvedeme několik snadných pozorování, které usnadní práci. Každé z nich ověřte na uvedených příkladech.

V každém tělese platí $1^{-1} = 1$ a také $(-1)^{-1} = -1$. Tedy v $\mathbb{Z}_p$ je $(p-1)^{-1} = (p-1)$, protože $-1 = p - 1$ (čti „opačný prvek k 1 je $p - 1$“). Podle cvičení 3.5.6 je $(-a)^{-1} = -(a^{-1})$, takže známe-li inverzní prvek k a, můžeme též určit inverzní prvek k $-a = p - a$. Podle stejného cvičení je inverzní prvek k inverznímu prvku původní prvek, tj. víme-li, že $b = a^{-1}$, pak $a = b^{-1}$.

Příklad 3.6. V tělese $\mathbb{Z}_7$ platí
$$\frac{-3}{5} = \frac{4}{5} = 4 \cdot 5^{-1} = 4 \cdot 3 = 5 \ .$$
Využili jsme $5^{-1} = 3$, což jsme nahlédli v předchozím příkladu. Alternativně se lze rovnou zeptat kolika je třeba vynásobit pětku, abychom dostali 4. Ještě jinak můžeme počítat
$$\frac{-3}{5} = \frac{4}{-2} = -2 = 5 \ .$$

Poznamenejme, že zatímco v tělese reálných (nebo racionálních) čísel je $\frac{4}{5}$ číslo, v tělese $\mathbb{Z}_7$ jde o výraz „4 děleno 5“. Takové výrazy by se ve výsledcích příkladů neměly objevovat, protože jdou ještě dopočítat.

Příklad 3.7. Určíme 13^{-1} v tělese $\mathbb{Z}_{37}$. Prvočíslo 37 je již příliš velké na to, abychom počítali inverzní prvky zkusmo, proto použijeme postup z důkazu věty 3.4. Je potřeba zjistit Bezoutovy koeficienty pro čísla $13, 37$.

$$\begin{aligned}\mathbf{37} &= 2\cdot\mathbf{13}+11\\ \mathbf{13} &= 1\cdot\mathbf{11}+2\\ \mathbf{11} &= 5\cdot\mathbf{2}+1\end{aligned}$$

Zpětným chodem dopočítáme Bezoutovy koeficienty.

$$\begin{aligned}1 &= 1\cdot\mathbf{11}-5\cdot\mathbf{2} =\\ &= 1\cdot\mathbf{11}-5\cdot(\mathbf{13}-1\cdot\mathbf{11}) = (-5)\cdot\mathbf{13}+6\cdot\mathbf{11} =\\ &= (-5)\cdot\mathbf{13}+6\cdot(\mathbf{37}-2\cdot\mathbf{13}) = 6\cdot\mathbf{37}+(-17)\cdot\mathbf{13}\end{aligned}$$

Protože $(-17) \bmod 37 = 20$, v tělese $\mathbb{Z}_{37}$ platí $13^{-1} = 20$. Můžeme ověřit, že opravdu platí $13\cdot 20 \bmod 37 = 1$.

Příklad 3.8. V tělese $\mathbb{Z}_{11}$ vyřešíme soustavu lineárních rovnic s maticí

$$\left(\begin{array}{ccccc|c} 2 & 4 & 1 & 2 & 10 & 3\\ 4 & 1 & 3 & 8 & 6 & 7\\ 7 & 5 & 0 & 2 & 6 & 8 \end{array}\right) .$$

Soustavu převedeme do odstupňovaného tvaru.

$$\left(\begin{array}{ccccc|c} 2 & 4 & 1 & 2 & 10 & 3\\ 4 & 1 & 3 & 8 & 6 & 7\\ 7 & 5 & 0 & 2 & 6 & 8 \end{array}\right) \sim \left(\begin{array}{ccccc|c} 2 & 4 & 1 & 2 & 10 & 3\\ 0 & 4 & 1 & 4 & 8 & 1\\ 0 & 2 & 2 & 6 & 4 & 3 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccccc|c} 2 & 4 & 1 & 2 & 10 & 3\\ 0 & 4 & 1 & 4 & 8 & 1\\ 0 & 0 & 7 & 4 & 0 & 8 \end{array}\right) \sim \left(\begin{array}{ccccc|c} 1 & 2 & 6 & 1 & 5 & 7\\ 0 & 1 & 3 & 1 & 2 & 3\\ 0 & 0 & 1 & 10 & 0 & 9 \end{array}\right)$$

V první úpravě jsme 9-násobek prvního řádku přičetli ke druhému a 2-násobek prvního řádku jsme přičetli ke třetímu.

Jak jsme přišli například na číslo 9 při nulování pozice $(2,1)$? Jednou možností je spočítat $-\frac{4}{2} = -2 = 9$. Pro malá tělesa, zejména $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7$, je asi nejrychlejší určit potřebné číslo zkusmo. Tím myslíme v našem případě úvahou „kolika je třeba vynásobit 2, aby po přičtení 4 vznikla 0“. Možná o něco početně příjemnější než přičítat 9-násobek je přičítat (-2)-násobek.

Na koeficient 2 při nulování pozice $(3,1)$ můžeme obdobně přijít buď výpočtem nebo zkusmo. Výpočet provedeme přímočaře

$$-\frac{7}{2} = -7\cdot 2^{-1} = -7\cdot 6 = -9 = 2 \ ,$$

nebo šikovněji například takto:

$$-\frac{7}{2} = \frac{-7}{2} = \frac{4}{2} = 2 \ .$$

V další úpravě jsme 5-násobek druhého řádku přičetli k třetímu. V poslední úpravě jsme vynásobili řádky čísly tak, aby pivoty byly rovny 1. To nám usnadní zpětné substituce při dopočítání řešení. Konkrétně jsme první řádek vynásobili číslem $2^{-1} = 6$, druhý řádek číslem $4^{-1} = 3$ a třetí řádek číslem $7^{-1} = 8$.

Bázové proměnné jsou x_1, x_2 a x_3 a volné proměnné jsou x_4 a x_5. Řešení tedy bude tvaru

$$\left\{ \begin{pmatrix} \cdot\\ \cdot\\ \cdot\\ 0\\ 0 \end{pmatrix} + s \begin{pmatrix} \cdot\\ \cdot\\ \cdot\\ 1\\ 0 \end{pmatrix} + t \begin{pmatrix} \cdot\\ \cdot\\ \cdot\\ 0\\ 1 \end{pmatrix} : s,t \in \mathbb{Z}_{11} \right\} .$$

Zpětnou substitucí dopočítáme neznámé pozice a získáme řešení

$$\left\{ \begin{pmatrix} 1\\ 9\\ 9\\ 0\\ 0 \end{pmatrix} + s \begin{pmatrix} 1\\ 7\\ 1\\ 1\\ 0 \end{pmatrix} + t \begin{pmatrix} 10\\ 9\\ 0\\ 0\\ 1 \end{pmatrix} : s,t \in \mathbb{Z}_{11} \right\} .$$

3.4. **Charakteristika.** Důležitým číselným parametrem těles je jejich *charakteristika*:

Definice 3.9. Existuje-li kladné celé číslo n takové, že v tělese $\mathbf{T}$ platí

$$\underbrace{1+1+\cdots+1}_{n}=0\ ,$$

pak nejmenší takové kladné číslo nazýváme *charakteristika* tělesa $\mathbf{T}$.

Pokud žádné takové kladné celé číslo n neexistuje, tak říkáme, že těleso $\mathbf{T}$ má *charakteristiku* 0.

Charakteristika tedy určuje, kolikrát je nejméně třeba sečíst jedničku, abychom dostali 0. Někdy se zápisem n rozumí součet n jedniček. Charakteristika je při této úmluvě nejmenší kladné celé číslo n takové, že $n=0$. Pokud takové n neexistuje, charakteristika je 0.

Věta 3.10. *Charakteristika každého tělesa je buď* 0 *nebo prvočíslo.*

Důkaz. Jestliže charakteristika tělesa $\mathbf{T}$ není rovná 0, pak existuje nějaké kladné celé číslo $n\geq 2$, pro které platí

$$\underbrace{1+1+\cdots+1}_{n}=0.$$

Jestliže je n složené číslo, platí $n=kl$ pro nějaká kladná celá čísla $k,l<n$. V důsledku axiomu distributivity (D) platí

$$(\underbrace{1+1+\cdots+1}_{k})(\underbrace{1+1+\cdots+1}_{l})=\underbrace{1+1+\cdots+1}_{n}=0.$$

Podle tvrzení 3.3.(6) může být součin dvou prvků v tělese rovný 0 pouze pokud je aspoň jeden z činitelů rovný 0. Proto je buď

$$\underbrace{1+1+\cdots+1}_{k}=0$$

nebo

$$\underbrace{1+1+\cdots+1}_{l}=0.$$

V každém případě nemůže být složené číslo $n\geq 2$ nejmenším kladným celým číslem, pro které platí

$$\underbrace{1+1+\cdots+1}_{n}=0.$$

Protože je $1\neq 0$ podle tvrzení 3.3.(10), musí být nejmenší takové číslo prvočíslo. □

Charakteristika těles $\mathbb{Q},\mathbb{R},\mathbb{C}$ je 0. Pro libovolné prvočíslo p je charakteristika tělesa $\mathbb{Z}_p$ rovná p.

Tělesa charakteristiky 2 mají tu příjemnou vlastnost, že sčítání a odčítání splývají, viz cvičení. V některých situacích tato tělesa tvoří výjimečné případy, které je třeba zvlášť rozebírat. Jedním z důvodů je fakt, že v nich nelze počítat aritmetický průměr dvou čísel – výraz $\frac{a+b}{2}$ totiž nedává smysl, protože dělíme nulou.

3.5. **Další příklady těles.**

3.5.1. *Čtyřprvkové těleso.* Pokud n není prvočíslo, pak $\mathbb{Z}_n$, definované podobně jako $\mathbb{Z}_p$, není těleso. Tedy například $\mathbb{Z}_4$ není těleso. Selže axiom (N3), 2 nemá inverzní prvek. Můžeme také použít větu 3.10, protože charakteristika by byla 4, což je nemožné.

Čtyřprvkové těleso ale existuje. Nejlépe je počítat s polynomy

$$GF(4)=\{0,1,\alpha,\alpha+1\}$$

jedné proměnné α s koeficienty v $\mathbb{Z}_2$. Sčítání je definované jako přirozené sčítání polynomů (např. $\alpha+(\alpha+1)=(1+1)\alpha+1=1$), při násobení pak polynomy vynásobíme přirozeným způsobem a pak vezme zbytek po dělení polynomem

$$\alpha^2+\alpha+1\ ,$$

například

$$\begin{aligned}(\alpha+1)(\alpha+1)&=\big((\alpha+1)\cdot_{\text{běžné}}(\alpha+1)\big)\bmod(\alpha^2+\alpha+1)=\\&=(\alpha^2+1)\bmod(\alpha^2+\alpha+1)=\alpha\ .\end{aligned}$$

3.5.2. *Další konečná tělesa.* Těleso s n prvky existuje právě tehdy, když n je mocnina prvočísla. Důkaz uvidíte později v kurzu algebry. Naopak, pokud $n = p^k$ pro nějaké prvočíslo p, pak těleso s n prvky existuje a je dokonce jednoznačně určené až na přeznačení prvků. Jde zkonstruovat podobně jako čtyřprvkové těleso. Prvky budou polynomy stupně nejvýše $k-1$ s koeficienty v $\mathbb{Z}_p$ a počítat budeme modulo pevně zvolený nerozložitelný polynom stupně k, tj. polynom, který se nedá napsat jako (běžný) součin polynomů nižšího stupně.

Podobně jako u těles $\mathbb{Z}_p$ by se existence inverzních prvků dokázala pomocí Bezoutových koeficientů, analogie Bezoutovy věty totiž platí i pro polynomy s koeficienty v $\mathbb{Z}_p$. Důležité je, že počítáme modulo nerozložitelný polynom. Tento fakt hraje v důkazu stejnou roli jako fakt, že p je prvočíslo v důkazu věty 3.4 – největší společný dělitel zvoleného nerozložitelného polynomu a libovolného nenulového polynomu nižšího stupně bude díky tomu 1.

3.5.3. *Podtělesa komplexních čísel.* Existuje celá řada těles „mezi“ racionálními a komplexními čísly. Například množina komplexních čísel

$$\{a + bi : a, b \in \mathbb{Q}\}$$

tvoří s běžnými operacemi těleso. K důkazu musíme ověřit, že tato množina je uzavřena na sčítání a násobení. Většina zbylých axiomů je pak očividná, kromě existence inverzního prvku. Úplný důkaz přenecháme do cvičení.

Dalším příkladem je množina

$$\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

opět s běžnými operacemi.

Tato a podobná tělesa hrají velkou roli například při důkazu slavné věty, že neexistuje vzoreček (využívající operace $+, \cdot, -, :, \sqrt[n]{\ }$) pro kořeny polynomu většího než pátého stupně, nebo při důkazu nemožnosti kvadratury kruhu, trisekce úhlu a zdvojení krychle.

3.5.4. *Těleso racionálních funkcí.* Příkladem „většího“ tělesa je těleso racionálních funkcí, tedy funkcí tvaru $\frac{p(x)}{q(x)}$, kde $p(x)$ a $q(x) \neq 0$ jsou reálné polynomy s běžnými operacemi sčítání a násobení funkcí. Je potřeba ztotožnit racionální funkce, které se liší pouze definičním oborem, např. 1 je potřeba považovat za tu samou racionální funkci jako $(x+1)/(x+1)$, viz cvičení.

3.5.5. *Charakteristika a konečnost.* Každé těleso charakteristiky 0 má nekonečně mnoho prvků, protože čísla $0, 1, 1+1, 1+1+1$ jsou všechna navzájem různá. Jde ukázat, že takové těleso v jistém smyslu obsahuje těleso racionálních čísel (viz cvičení).

Na druhou stranu, není pravda, že těleso nenulové charakteristiky má nutně konečný počet prvků. Příkladem je těleso racionálních funkcí nad $\mathbb{Z}_p$, které má charakteristiku p a není konečné. Při zavádění tohoto tělesa je potřeba postupovat opatrněji než v případě tělesa racionálních funkcí nad $\mathbb{R}$, musíme pracovat s formálními podíly (nikoliv funkcemi tvaru podílu) a vhodné podíly ztotožnit. Detaily probírat nebudeme.

Každé těleso charakteristiky p „obsahuje“ těleso $\mathbb{Z}_p$ (opět viz cvičení).

3.5.6. *Kvaterniony.* Důležitým příkladem nekomutativního tělesa jsou kvaterniony. Kvaterniony definujeme jako výrazy tvaru

$$a + bi + cj + dk,$$

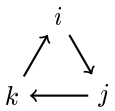
kde $a, b, c, d \in \mathbb{R}$ a i, j, k, l jsou „imaginární jednotky“. Sčítání je definováno přirozeně, tedy

$$(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = (a + a') + (b + b')i + (c + c')j + (d + d')k.$$

Při násobení roznásobíme závorky a využijeme vztahů $ai = ia, aj = ja, ak = ka$ pro libovolné $a \in \mathbb{R}$ a

$$i^2 = j^2 = k^2 = -1, \quad ij = k, jk = i, ki = j, \quad ji = -k, kj = -i, ik = -j,$$

které se dobře pamatují pomocí cyklu $i \to j \to k \to i$:



Pokud násobíme po směru cyklu, dostaneme třetí proměnnou s kladným znaménkem, a násobení proti směru znaménko obrací. Tedy

$$\begin{aligned}
&(a+bi+cj+dk)\cdot(a'+b'i+c'j+d'k) = \\
&= aa'+ab'i+ac'j+ad'k+ba'i+bb'i^2+bc'ij+bd'ik+ \\
&\quad +ca'j+cb'ji+cc'j^2+cd'jk+da'k+db'ki+dc'kj+dd'k^2 = \\
&= aa'+ab'i+ac'j+ad'k+ba'i-bb'+bc'k-bd'j+ \\
&\quad +ca'j-cb'k-cc'+cd'i+da'k+db'j-dc'i-dd' = \\
&= (aa'-bb'-cc'-dd')++(ab'+ba'+cd'-dc')i+ \\
&\quad +(ac'-bd'+ca'+db')j+(ad'+bc'-cb'+da')k\ .
\end{aligned}$$

Lineární algebru lze mimo jiné použít také ke zkoumání geometrických zobrazení. Rotace o úhel α kolem nějaké osy patří mezi důležitá geometrická zobrazení. V letním semestru si ukážeme, že složení dvou rotací kolem různých os je opět rotace kolem nějaké osy. Najít osu a úhel složené rotace není vůbec jednoduché. Hledání toho, jak osa a úhel složené rotace závisí na osách a úhlech rotací, které skládáme, vedlo k objevu kvaternionů.

Délkou kvaternionu $a+bi+cj+dk$ rozumíme reálné číslo $\sqrt{a^2+b^2+c^2+d^2}$. Kvaternion délky 1 nazýváme *jednotkový kvaternion*. Lze spočítat (viz cvičení), že součin dvou jednotkových kvaternionů je zase jednotkový kvaternion.

Rotaci kolem osy procházející počátkem souřadnic a bodem $(a,b,c)\neq(0,0,0)$ o úhel α v kladném směru (tj. proti směru hodinových ručiček díváme-li se na rovinu, ve které se body pohybují, z kladného směru osy rotace) zapíšeme pomocí kvaternionu

$$\cos(\alpha/2)+\sin(\alpha/2)(ai+bj+ck)\ .$$

Tak například otočení o úhel $\pi/2$ kolem první souřadné osy zapíšeme jako kvaternion $\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i$. Otočení kolem osy z o úhel $\pi/2$ v kladném směru zapíšeme pomocí kvaternionu $\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}k$.

Pro každé kladné reálné číslo r popisuje kvaternion $\cos(\alpha/2)+\sin(\alpha/2)(rai+rbj+rck)$ stejnou rotaci jako kvaternion $\cos(\alpha/2)+\sin(\alpha/2)(ai+bj+ck)$. Oba vektory $(a,b,c)^T$ a $(ra,rb,rc)^T$ totiž určují stejnou přímku procházející počátkem. Ze všech možných kvaternionů popisujících stejnou rotaci si vybereme jednotkový kvaternion. Oba příklady z předchozího odstavce jsou jednotkové kvaterniony.

Složíme-li dvě rotace, dostaneme osu a úhel složené rotace tak, že vynásobíme příslušné kvaterniony v daném pořadí.

Příklad 3.11. Složíme rotaci kolem osy x o úhel $\pi/2$ a rotací kolem osy z o úhel $\pi/2$. Osu a úhel složené rotace najdeme jako součin kvaternionů

$$\left(\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}k\right)\left(\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i\right)=\frac{1}{2}+\frac{\sqrt{3}}{2}\frac{1}{\sqrt{3}}(i+j+k)\ ,$$

použili jsme rovnost $ki=j$.

Platí tedy, že složená rotace je kolem osy prvního oktantu o úhel $2\pi/3$ v kladném směru.

Cvičení

1. Dokažte, že v libovolném tělese $\mathbf{T}$ platí pro každé dva prvky $a,b\in T$ vztahy $(-a)(-b)=ab$, $(-a)b=-(ab)$ a $\frac{a}{-b}=\frac{-a}{b}=-\frac{a}{b}$.

2. Dokažte, že v libovolném tělese $\mathbf{T}$ funguje převod na společný jmenovatel, tzn. dokažte, že pro libovolná $a,b,c,d\in T$, $b,d\neq 0$, platí

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$$

3. Dokažte, že v libovolném tělese platí $-0=0$, $1^{-1}=1$, $(-a)^{-1}=-a^{-1}$, $(a^{-1})^{-1}=a$ pro libovolné $0\neq a\in T$.

4. Dokončete důkaz, že $\mathbb{Z}_p$ je těleso pro libovolné prvočíslo p.

5. Dokažte, že $\mathbb{Z}_n$ je těleso právě tehdy, když n je prvočíslo.

6. Dokažte, že v libovolném tělese $\mathbf{T}$ charakteristiky 2 platí $a=-a$ pro libovolný prvek $a\in T$.

7. Vytvořte tabulku počítání ve čtyřprvkovém tělese a ověřte, že se skutečně jedná o těleso.

8. Rozhodněte (a odpověď dokažte), které z následujících podmnožin $\mathbb{C}$ tvoří s běžnými operacemi těleso.

- $\{a+bi : a,b\in\mathbb{Q}\}$
- $\{a+b\sqrt{2} : a,b\in\mathbb{Q}\}$
- $\{a+b\sqrt{n} : a,b\in\mathbb{Q}\}$, kde n je pevně zvolené přirozené číslo

- $\{a + b\sqrt[3]{2} : a, b \in \mathbb{Q}\}$
- $\{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$
- $\{a + b\sqrt{2} + c\sqrt{3} : a, b, c \in \mathbb{Q}\}$
- $\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$

9. Proč je při definici tělesa racionálních funkcí třeba ztotožňovat racionální funkce, které se liší pouze definičním oborem?

10. Dokažte, že v tělese charakteristiky 0 jsou všechna čísla $0, 1, 1+1, 1+1+1, \ldots$ navzájem různá.

11. Nechť $\mathbf{T}$ s operacemi $\oplus, \odot$ je těleso charakteristiky 0. Opačné prvky a dělení v tomto tělese budeme značit $\ominus, \oslash$. Pro libovolné přirozené číslo n označme

$$\overline{n} = \underbrace{1 \oplus 1 \oplus \cdots \oplus 1}_{n\times} \quad \text{a} \quad \overline{-n} = \ominus\overline{n}$$

Dokažte, že pro libovolné $p_1, p_2 \in \mathbb{Z}$ a $q_1, q_2 \in \mathbb{N}$ platí, že $\overline{p_1} \oslash \overline{q_1} = \overline{p_2} \oslash \overline{q_2}$ právě tehdy, když se racionální čísla p_1/q_1 a p_2/q_2 rovnají a platí

$$(\overline{p_1} \oslash \overline{q_1}) \odot (\overline{p_2} \oslash \overline{q_2}) = \overline{p_1 p_2} \oslash \overline{q_1 q_2}, \quad (\overline{p_1} \oslash \overline{q_1}) \oplus (\overline{p_2} \oslash \overline{q_2}) = \overline{p_1 q_2 + p_2 q_1} \oslash \overline{q_1 q_2} \ .$$

Prvky T typu $\overline{p} \oslash \overline{q}$, $p \in \mathbb{Z}$, $q \in \mathbb{N}$ se tedy sčítají a násobí jako racionální čísla. V tomto smyslu obsahuje každé těleso charakteristiky 0 těleso racionálních čísel.

12. Po vzoru předchozího tvrzení přesně zformulujte a dokažte tvrzení, že každé těleso charakteristiky p obsahuje těleso $\mathbb{Z}_p$.

13. V tělese kvaternionů najděte prvek inverzní k prvku $a + bi + cj + dk$.

14. Dokažte, že součin dvou jednotkových kvaternionů je opět jednotkový kvaternion.

4. Matice

Cíl. *Dozvíme se, že matice určují zobrazení. Naučíme se provádět základní operace s maticemi. Zajímavou operací je násobení, které odpovídá skládání zobrazení, a invertování, které odpovídá invertování zobrazení.*

Matice pro nás zatím byly pouze pomůckou k přehlednému zápisu soustav lineárních rovnic. V této kapitole se budeme dívat na matice jako na samostatné objekty. Definujeme základní operace, zmíníme některé aplikace a základní vlastnosti. K pochopení násobení matic nahlédneme, že matice přirozeným způsobem určují zobrazení. Takto jdou popsat například rotace nebo osové souměrnosti v rovině. Násobení matic pak odpovídá skládání zobrazení.

4.1. Matice a jednoduché operace.

Začneme definicí matice a speciálních typů matic. Nová definice rozšiřuje stávající definice 2.1 a 2.4 tím, že prvky mohou být z libovolného pevně zvoleného tělesa.

Definice 4.1. Nechť $\mathbf{T}$ je těleso. *Maticí nad tělesem* $\mathbf{T}$ *typu* $m \times n$ rozumíme obdélníkové schéma prvků T s m řádky a n sloupci. Matice typu $m \times m$ se nazývá *čtvercová matice řádu* m. Matice typu $m \times 1$ se nazývá *(sloupcový) aritmetický vektor* a matice typu $1 \times m$ se nazývá *řádkový aritmetický vektor*.

Připomeňme, že zápisem $A = (a_{ij})_{m\times n}$ rozumíme matici A typu $m \times n$, která má na pozici (i, j) prvek $a_{ij} \in T$. Index $m \times n$ vynecháváme, pokud nechceme typ specifikovat nebo je zřejmý z kontextu.

Definice 4.2. Čtvercovou matici $A = (a_{ij})$ nazýváme

- *diagonální*, pokud $a_{ij} = 0$ kdykoliv $i \neq j$,
- *horní trojúhelníková*, pokud $a_{ij} = 0$ kdykoliv $i > j$,
- *dolní trojúhelníková*, pokud $a_{ij} = 0$ kdykoliv $i < j$.

U libovolné matice říkáme, že prvky a_{ii} tvoří *hlavní diagonálu*.

Matice $A = (a_{ij})$ a $B = (b_{ij})$ považujeme za stejné, pokud mají stejný typ $m \times n$ a mají stejné prvky na odpovídajících pozicích (formálněji, pro každé $i \in \{1, 2, \dots, m\}$ a každé $j \in \{1, 2, \dots, n\}$ platí $a_{ij} = b_{ij}$).

Zavedeme několik jednoduchých operací s maticemi, které zobecňují příslušné operace pro vektory.

Definice 4.3. Jsou-li $A = (a_{ij})$ a $B = (b_{ij})$ matice nad stejným tělesem $\mathbf{T}$, stejného typu $m \times n$ a $t \in T$, pak definujeme

- *součet matic* A *a* B jako matici $A + B = (a_{ij} + b_{ij})_{m\times n}$,
- t*-násobek matice* A jako matici $t \cdot A = tA = (ta_{ij})_{m\times n}$,
- *matice opačnou k* A jako matici $-A = (-a_{ij})_{m\times n}$,
- *nulovou maticí* typu $m \times n$ jako matici $0_{m\times n} = (0)_{m\times n}$.

Součet matic různých typů nebo nad různými tělesy není definován. Rovněž nedefinujeme výraz At, t-násobek matice A píšeme vždy tA.

Příklad 4.4. Nad tělesem $\mathbb{Z}_5$ máme

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

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

$$-\begin{pmatrix} 2 & 1 & 3 \\ 4 & 0 & 1 \end{pmatrix} = \begin{pmatrix} -2 & -1 & -3 \\ -4 & -0 & -1 \end{pmatrix} = \begin{pmatrix} 3 & 4 & 2 \\ 1 & 0 & 4 \end{pmatrix}, \quad 0_{2\times 3} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Právě definované operace vůbec neberou v úvahu tabulkovou strukturu matice – kdybychom napsali sloupce matice pod sebe, dostali bychom aritmetický vektor s mn složkami a operace $+, t\cdot, -$ by se shodovaly se stejnými operacemi pro vektory. Jednoduchou operací, která není tohoto typu, je transpozice. Zavedené značení je v souladu s dříve používaným značením $(a_1, \dots, a_n)^T$ pro sloupcový vektor.

Definice 4.5. *Transponovaná matice* k matici $A = (a_{ij})_{m\times n}$ je matice $A^T = (b_{ji})_{n\times m}$, kde $b_{ji} = a_{ij}$ pro libovolné indexy $i \in \{1, 2, \dots, m\}$ a $j \in \{1, 2, \dots, n\}$.

Sloupce transponované matice jsou tedy řádky původní matice a naopak. Například

$$A = \begin{pmatrix} 2 & 1 & 3 \\ 4 & 0 & 1 \end{pmatrix}, \quad A^T = \begin{pmatrix} 2 & 4 \\ 1 & 0 \\ 3 & 1 \end{pmatrix} .$$

4.2. **Násobení matic.**

4.2.1. *Geometrická motivace.* Na rozdíl od sčítání, násobení matic není definováno po pozicích. Abychom pochopili na první pohled záhadnou definici, podíváme se trochu jinak na řešení soustav lineárních rovnic. Uvažujme například soustavu 2 rovnic o 2 neznámých nad reálnými čísly a její matici:

$$\begin{aligned} 2x_1 + 3x_2 &= 10 \\ 5x_1 + 2x_2 &= 20 \end{aligned}, \quad A = \begin{pmatrix} 2 & 3 \\ 5 & 2 \end{pmatrix} .$$

Levá strana soustavy, neboli matice soustavy, definuje zobrazení f_A z množiny $\mathbb{R}^2$ všech 2-složkových vektorů nad $\mathbb{R}$ do téže množiny $\mathbb{R}^2$:

$$f_A \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 2x_1 + 3x_2 \\ 5x_1 + 2x_2 \end{pmatrix} .$$

Řešení soustavy jsou ty vektory $(x_1, x_2)^T$, které zobrazení f_A zobrazí na vektor $(10, 20)^T$. (Jinými slovy, řešením je vzor vektoru $(10, 20)^T$ při zobrazení f_A.)

Obecněji, matice typu $m \times n$ definuje zobrazení z množiny $\mathbb{R}^n$ do množiny $\mathbb{R}^m$. Studiu těchto typů zobrazení je věnována kapitola **??**, my se zatím podíváme na tři příklady.

- *Otočení o* $30°$ *v* $\mathbb{R}^2$. Obraz vektoru $(x_1, x_2)^T$ určíme úvahou podle obrázku (přesněji bychom měli říkat obraz bodu, jehož polohový vektor je $(x_1, x_2)^T$, ale dělat to nebudeme).
  OBRAZEK
  Obrazem vektoru $(1, 0)^T$ je
  $$\begin{pmatrix} \cos(\pi/6) \\ \sin(\pi/6) \end{pmatrix} = \begin{pmatrix} \sqrt{3}/2 \\ 1/2 \end{pmatrix} ,$$
  z čehož vidíme, že obrazem vektoru $(x_1, 0)^T$ je
  $$x_1 \begin{pmatrix} \sqrt{3}/2 \\ 1/2 \end{pmatrix} = \begin{pmatrix} x_1\sqrt{3}/2 \\ x_1/2 \end{pmatrix} .$$
  Podobně zjistíme, že obrazem vektoru $(0, x_2)^T$ je vektor $(-x_2/2, x_2\sqrt{3}/2)$. Obraz součtu vektorů $(x_1, 0)^T$ a $(0, x_2)^T$ (což je vektor $(x_1, x_2)^T$) určíme jako součet jejich obrazů. Obrazem vektoru $(x_1, x_2)^T$ je tedy vektor
  $$\begin{pmatrix} \frac{\sqrt{3}}{2}x_1 \\ \frac{1}{2}x_1 \end{pmatrix} + \begin{pmatrix} -\frac{1}{2}x_2 \\ \frac{\sqrt{3}}{2}x_2 \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{3}}{2}x_1 - \frac{1}{2}x_2 \\ \frac{1}{2}x_1 + \frac{\sqrt{3}}{2}x_2 \end{pmatrix} .$$
  Vidíme, že rotace o $30°$ je zobrazení f_A, kde
  $$A = \begin{pmatrix} \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix} .$$
  Obecněji, rotace o úhel α je zobrazení f_A, kde
  $$A = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} .$$
- *Osová souměrnost podle osy* x *v* $\mathbb{R}^2$. Obrazem vektoru $(x_1, x_2)^T$ je vektor $(x_1, -x_2)^T$, takže souměrnost podle osy x je zobrazení f_A, kde
  $$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} .$$
- Zobrazení f_A z $\mathbb{R}^2$ do $\mathbb{R}^3$ dané maticí
  $$\begin{pmatrix} 1 & 2 \\ 1 & 0 \\ 1 & 3 \end{pmatrix}$$
  je znázorněné na obrázku.
  OBRAZEK

Uvažujme teď dvě zobrazení f_A a f_B z $\mathbb{R}^2$ do $\mathbb{R}^2$ dané maticemi

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} .$$

Podíváme se na složení zobrazení f_B a f_A, tedy zobrazení g definované vztahem $g(\mathbf{x}) = f_A(f_B(\mathbf{x}))$.

$$\begin{aligned} g\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = f_A\left(f_B\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = f_A\begin{pmatrix} b_{11}x_1 + b_{12}x_2 \\ b_{21}x_1 + b_{21}x_2 \end{pmatrix} = \\ = \begin{pmatrix} a_{11}(b_{11}x_1 + b_{12}x_2) + a_{12}(b_{21}x_1 + b_{22}x_2) \\ a_{21}(b_{11}x_1 + b_{12}x_2) + a_{22}(b_{21}x_1 + b_{22}x_2) \end{pmatrix} = \\ = \begin{pmatrix} (a_{11}b_{11} + a_{12}b_{21})x_1 + (a_{11}b_{12} + a_{12}b_{22})x_2 \\ (a_{21}b_{11} + a_{22}b_{21})x_1 + (a_{21}b_{12} + a_{22}b_{22})x_2 \end{pmatrix} . \end{aligned}$$

Vidíme, že $g = f_C$ pro matici

$$C = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix} .$$

Obecněji bychom mohli složit zobrazení f_B z $\mathbb{R}^p$ do $\mathbb{R}^n$ dané maticí typu $n \times p$ a zobrazení f_A z $\mathbb{R}^n$ do $\mathbb{R}^m$ dané maticí typu $m \times n$. Podobným výpočtem jako výše bychom zjistili, že výsledné zobrazení z $\mathbb{R}^p$ do $\mathbb{R}^m$ je dáno maticí C typu $m \times p$, která má na pozici (i, k) prvek

$$a_{i1}b_{1k} + a_{i2}b_{2k} + \cdots + a_{in}b_{nk}$$

4.2.2. *Definice násobení.* Dostali jsme se k definici součinu matic.

Definice 4.6. Je-li A matice typu $m \times n$ a B matice typu $n \times p$ nad stejným tělesem $\mathbf{T}$, pak definujeme *součin matic* $A \cdot B = AB = (c_{ik})$ jako matici nad $\mathbf{T}$ typu $m \times p$, kde

$$c_{ik} = \sum_{j=1}^{n} a_{ij}b_{jk} = a_{i1}b_{1k} + a_{i2}b_{2k} + \cdots + a_{in}b_{nk}$$

pro každé $i \in \{1, 2, \ldots, m\}$ a $k \in \{1, 2, \ldots, p\}$.

Součin AB je tedy definován, pokud počet sloupců matice A je rovný počtu řádků matice B. Jinak definován není. To souhlasí s motivací součinu matic jako skládání zobrazení.

Prvek na místě (i, k) dostaneme jako standardní skalární součin i-tého řádku matice A a k-tého sloupce matice B. Pro řádky a sloupce matice zavedeme speciální značení.

Definice 4.7. Je-li A matice typu $m \times n$ a $i \in \{1, 2, \ldots, m\}$, pak $(a_{i1}, a_{i2}, \ldots, a_{in})$ nazýváme *i-tý řádkový vektor matice A* a značíme jej A_{i*}. Podobně pro $j \in \{1, 2, \ldots, n\}$ definujeme *j-tý sloupcový vektor* jako $A_{*j} = (a_{1j}, a_{2j}, \ldots, a_{mj})^T$.

Prvek na místě (i, k) součinu AB je v tomto značení roven

$$c_{ik} = A_{i*}B_{*k} = (a_{i1}, a_{i2}, \ldots, a_{in}) \begin{pmatrix} b_{1k} \\ b_{2k} \\ \vdots \\ b_{nk} \end{pmatrix} .$$

OBRAZEK

Příklad 4.8. Nad tělesem $\mathbb{R}$ máme

$$(1, 2)\begin{pmatrix} 3 \\ 4 \end{pmatrix} = 1 \cdot 3 + 2 \cdot 4 = 11, \quad \begin{pmatrix} 3 \\ 4 \end{pmatrix}(1, 2) = \begin{pmatrix} 3 \cdot 1 & 3 \cdot 2 \\ 4 \cdot 1 & 4 \cdot 2 \end{pmatrix} = \begin{pmatrix} 3 & 6 \\ 4 & 8 \end{pmatrix}$$

Příklad 4.9. Počítáme opět nad $\mathbb{R}$.

$$\begin{pmatrix} 1 & 0 & -1 \\ 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 3 & 5 & 2 & 4 \\ 1 & 1 & -3 & 2 \\ 0 & 2 & -2 & 1 \end{pmatrix} =$$
$$= \begin{pmatrix} 1\cdot 3+0\cdot 1+(-1)\cdot 0 & 1\cdot 5+0\cdot 1+(-1)\cdot 2 \\ 1\cdot 3+1\cdot 1+0\cdot 0 & 1\cdot 5+1\cdot 1+0\cdot 4 \end{pmatrix}$$
$$\begin{pmatrix} 1\cdot 2+0\cdot(-3)+(-1)\cdot(-2) & 1\cdot 4+0\cdot 2+(-1)\cdot 1 \\ 1\cdot 2+1\cdot(-3)+0\cdot(-2) & 1\cdot 4+1\cdot 2+0\cdot 1 \end{pmatrix} =$$
$$= \begin{pmatrix} 3 & 3 & 4 & 3 \\ 4 & 6 & -1 & 6 \end{pmatrix}$$

Zobrazení f_A určené maticí A nad tělesem $\mathbf{T}$ typu $m \times n$ jde napsat pomocí maticového součinu. Obrazem n-složkového vektoru $\mathbf{x} = (x_1, x_2, \ldots, x_n)^T$ (nad $\mathbf{T}$) je m-složkový vektor $A\mathbf{x}$:

$$f_A : T^n \to T^m, \quad f_A(\mathbf{x}) = A\mathbf{x} \ .$$

Příklad 4.10.

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

Použili jsme součtové vzorce pro goniometrické funkce. Výsledek není překvapující. Odvodili jsme, že násobené matice určují pořadě otočení o α a otočení o β. Výsledná matice tedy odpovídá složení otočení o β a otočení o α, což je otočení o $\alpha+\beta$ a to odpovídá výsledné matici. Pokud bychom uměli rychle určit matici odpovídající otočení o nějaký úhel (to se naučíme v kapitole **??**), pak lze uvedený výpočet použít k rychlému odvození součtových vzorců pro cos a sin.

Příklad 4.11. Matice v předchozím příkladu mají tu vzácnou vlastnost, že komutují, tzn. nezáleží na pořadí, ve kterém je násobíme. To odpovídá geometricky tomu, že nezáleží, zda nejprve rotujeme o úhel α a pak o úhel β, nebo naopak. **Násobení matic ale obecně komutativní není**. Součin v opačném pořadí nemusí být dokonce vůbec definován, například pro matici A typu 2×3 a matici B typu 3×5 (nad stejným tělesem) je součin AB matice typu 2×5, ale součin BA není definován.

Součin není obecně komutativní ani pro čtvercové matice stejného řádu. Například složíme-li osovou souměrnost v $\mathbb{R}^2$ podle osy x a otočení o $\pi/2$ dostaneme zobrazení odpovídající matici

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

Pokud naopak nejprve rovinu otočíme o $\pi/2$ a pak překlopíme kolem osy x, dostaneme zobrazení odpovídající matici

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

Geometrický popis vzniklých zobrazení přenecháme do cvičení.

Příklad 4.12. Podíváme se ještě jednou na příklad 3.11, kde jsme v $\mathbb{R}^3$ pomocí kvaternionů skládali rotaci kolem osy x o úhel $\pi/2$ s rotací kolem osy z o úhel π.

OBRAZEK kladne orientace os

Obrazem vektoru $(x_1, x_2, x_3)^T$ při rotaci kolem osy x o úhel $\pi/2$ je $(x_1, x_3, -x_2)^T$, tedy tato rotace je rovna f_B pro

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

Obrazem vektoru $(x_1, x_2, x_3)^T$ při rotaci kolem osy z o úhel $\pi/2$ je $(x_1, x_3, -x_2)^T$, tedy tato rotace je rovna f_A pro

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

Složením je zobrazení f_C, kde $C = AB$.

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

Z matice C určíme snadno obraz vektoru $(x_1, x_2, x_3)^T$:

$$f_C \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = C \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_3 \\ x_1 \\ x_2 \end{pmatrix} .$$

Není ale vidět, že je to rotace kolem osy prvního oktantu o úhel $2\pi/3$ v kladném směru, jak jsme zjistili z kvaternionového přístupu.

4.2.3. *Násobení jako provádění lineárních kombinací.* Někdy je výhodný trochu jiný pohled na násobení matic. Násobíme-li matici $A = (a_{ij})$ maticí B, pak i-tý řádek výsledku získáme sečtením a_{i1}-násobku 1. řádku matice B, a_{i2}-násobku 2. řádku matice B, atd. Je to dobře vidět na příkladu 4.9. Toto pozorování a podobné pozorování pro sloupce jednak často usnadní numerické počítání a je také důležité z teoretického hlediska. Snadněji jde vyjádřit pomocí pojmu lineární kombinace matic.

Definice 4.13. Jsou-li $A_1, A_2, \ldots, A_k$ matice stejného typu nad stejným tělesem $\mathbf{T}$ a $t_1, t_2, \ldots, t_k$ prvky tělesa $\mathbf{T}$, pak součet

$$t_1 A_1 + t_2 A_2 + \cdots + t_k A_k$$

se nazývá *lineární kombinace matic* $A_1, A_2, \ldots, A_k$. Prvky $t_1, \ldots, t_k \in T$ nazýváme *koeficienty lineární kombinace.*

Pozorování lze nyní přeformulovat tak, že i-tý řádek součinu AB je lineární kombinací řádků matice B s koeficienty v i-tém řádku matice A. Podobně, k-tý sloupec součinu AB je lineární kombinací sloupců matice A, kde koeficienty jsou v k-tém sloupci matice B:

Tvrzení 4.14. *Je-li $A = (a_{ij})$ matice typu $m \times n$ a $B = (b_{jk})$ matice nad stejným tělesem typu $n \times p$, pak*

(1) *pro každé $i = 1, \ldots, m$ platí $(AB)_{i*} = a_{i1}B_{1*} + a_{i2}B_{2*} + \cdots + a_{in}B_{n*} = A_{i*}B$.*
(2) *pro každé $k = 1, \ldots, p$ platí $(AB)_{*k} = b_{1k}A_{*1} + b_{2k}A_{*2} + \cdots + b_{nk}A_{*n} = AB_{*k}$,*

Důkaz. (1). Označíme $C = (AB) = (c_{ik})$ a vezmeme libovolné $i \in \{1, 2, \ldots, m\}$. Pro libovolné $k \in \{1, 2, \ldots, p\}$ je k-tá složka řádkového vektoru na levé straně rovna c_{ik} a k-tá složka prostředního vektoru je $a_{i1}b_{1k} + a_{i2}b_{2k} + \cdots + a_{im}b_{mk}$, což je totéž podle definice součinu matic. Tento výraz je roven k-té složce řádkového vektoru $A_{i*}B$, rovněž podle definice součinu.

Část (2) se dokáže podobně. □

Příklad 4.15. Podívejme se ještě jednou na součin v příkladu 4.9.

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

Podle první části tvrzení je první řádek výsledku součet 1-násobku řádkového vektoru $B_{1*} = (3, 5, 2, 4)$, 0-násobku $B_{2*} = (1, 1, -3, 2)$ a (-1)-násobku $B_{3*} = (0, 2, -2, 1)$, to je $(3, 3, 4, 3)$. Druhý řádek výsledku je součtem prvních dvou řádku matice B, tedy $(4, 6, -1, 6)$. Tímto způsobem získáme výsledek

$$\begin{pmatrix} 3 & 3 & 4 & 3 \\ 4 & 6 & -1 & 6 \end{pmatrix}$$

daleko rychleji. Používat druhou část tvrzení se v tomto případě příliš nevyplatí.

Obě části si rozmyslete na příkladu 4.11.

4.2.4. *Jednotková matice.* Neutrální prvky vzhledem k násobení tvoří tzv. jednotkové matice:

Definice 4.16. *Jednotková matice řádu n nad tělesem* $\mathbf{T}$ je čtvercová matice $I_n = (a_{ij})_{n\times n}$, kde $a_{ii} = 1$ pro každé $i \in \{1, 2, \ldots, n\}$ a $a_{ij} = 0$ kdykoliv $i \neq j$, $i, j \in \{1, 2, \ldots, n\}$, tj.

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} .$$

Prvky jednotkové matice také označujeme pomocí symbolu δ_{ij}, tzn. *Kroneckerovo delta*. Ten se rovná 1, pokud $i = j$, a 0 jinak. Těleso, ve kterém pracujeme musí být zřejmé z kontextu.

Z tvrzení 4.14 nahlédneme, že $I_n A = A$, kdykoliv je součin definován, tj. pokud A má n řádků. Skutečně, i-tý řádek výsledku je rovný lineární kombinaci řádků matice A s koeficienty $0, 0, \ldots, 0, 1, 0, 0, \ldots, 0$, kde 1 je na pozici i. Tato kombinace je rovná i-tému řádku výsledku. Podobně z druhé části stejného tvrzení dostaneme, že $AI_n = A$, kdykoliv A má n sloupců.

Geometricky, jednotková matice I_n odpovídá identickému zobrazení z T^n do T^n.

4.3. **Maticový zápis soustavy lineárních rovnic.** Uvažujme soustavu m lineárních rovnic o n neznámých $x_1, x_2, \ldots, x_n$ s rozšířenou maticí $(A \mid \mathbf{b})$ nad tělesem $\mathbf{T}$.

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m \end{aligned}$$

Označíme-li $\mathbf{x}$ vektor neznámých, tj. $\mathbf{x} = (x_1, x_2, \ldots, x_n)^T$, pak máme

$$A\mathbf{x} = \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \end{pmatrix} .$$

Vektor $A\mathbf{x}$ je tedy sloupcový vektor vzniklý dosazením $\mathbf{x}$ do levé strany soustavy. Vidíme, že soustavu rovnic lze psát ve tvaru

$$A\mathbf{x} = \mathbf{b} .$$

I elementární úpravy matic lze interpretovat maticově.

Tvrzení 4.17. *Nechť C je matice typu $m \times n$ nad tělesem $\mathbf{T}$, $i, j \in \{1, 2, \ldots, m\}$, $i \neq j$ a $0 \neq t \in T$.*

(1) *Nechť E je matice, která vznikne z I_m prohozením i-tého a j-tého řádku. Pak EC vznikne z C prohozením i-tého a j-tého řádku.*

$$E = \begin{array}{c} \\ i \\ \\ j \\ \\ \end{array} \begin{array}{c} \begin{array}{cccccccc} & & & i & & j & & \end{array} \\ \begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \ddots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix} \end{array}$$

(2) *Nechť E je matice, která vznikne z I_m nahrazením prvku 1 na místě (i, i) prvkem t. Pak EC vznikne z C vynásobením i-tého řádku prvkem t.*

$$E = \begin{array}{c} \\ i \\ \\ \end{array} \begin{array}{c} \begin{array}{cccccc} & & & i & & \end{array} \\ \begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & t & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix} \end{array}$$

(3) *Nechť E je matice, která vznikne z I_m nahrazením prvku 0 na místě (i, j) prvkem t. Pak EC vznikne z C přičtením t-násobku j-tého řádku k i-tému řádku.*

$$E = \begin{array}{c} \\ \\ \\ i \\ \\ \\ \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccccccc} & & & & i & & & j & \\ \end{array} \\ \begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & \cdots & t & \cdots & 0 \\ \vdots & \vdots & & \vdots & \ddots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots & & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix} \end{array}$$

Důkaz. Pozorování plyne z první části tvrzení 4.14. □

Definice 4.18. Maticím E z předchozího tvrzení říkáme *elementární matice.*

4.4. **Vlastnosti maticových operací.** V této části zformulujeme několik základních algebraických vlastností maticových operací. Téměř všechny z nich, snad až na asociativitu násobení, jsou očividné. Nicméně používání maticové algebry může například značně zpřehlednit a zkrátit technické výpočty.

Sčítání matic má podobné vlastnosti jako sčítání v tělese. Musíme dát ale pozor, abychom sčítali matice stejných typů.

Tvrzení 4.19. *Jsou-li A, B, C matice stejného typu $m \times n$ nad stejným tělesem $\mathbf{T}$, pak platí*

(1) $(A + B) + C = A + (B + C)$,
(2) $A + 0_{m\times n} = A$,
(3) $A + (-A) = 0_{m\times n}$,
(4) $A + B = B + A$.

Důkaz. Matice mají stejný typ, takže výrazy $(A + B) + C$ a $A + (B + C)$ jsou definovány a výsledkem jsou matice typu $m \times n$. Prvek na místě (i, j) v matici $(A + B) + C$ se rovná $(a_{ij} + b_{ij}) + c_{ij}$, na místě (i, j) v matici $A + (B + C)$ se rovná $a_{ij} + (b_{ij} + c_{ij})$. Protože sčítání prvků tělesa je asociativní (axiom (S1) v definici tělesa), prvky na stejném místě v maticích $(A + B) + C$ a $A + (B + C)$ se rovnají. Proto platí $(A + B) + C = A + (B + C)$.

Ostatní vlastnosti sčítání se dokáží podobně. □

Násobení matic a násobení v tělese mají některé společné vlastnosti. Násobení je asociativní (pokud násobíme matice správných typů) a jednotkové matice jsou neutrálním prvkem. Navíc platí oboustranný distributivní zákon. Rozdíl oproti násobení v tělese je ve dvou podstatných vlastnostech. Násobení matic není komutativní (ani pro čtvercové matice stejného řádu), jak jsme si již všimli. Dále není pravda, že ke každé nenulové matici existuje matice inverzní.

Tvrzení 4.20. *Jsou-li A, B matice typu $m \times n$, C matice typu $n \times p$ a D, E matice typu $p \times q$, kde všechny matice jsou nad stejným tělesem $\mathbf{T}$, pak*

(1) $(BC)D = B(CD)$,
(2) $I_m A = A I_n = A$,
(3) $(A + B)C = AC + BC$, $C(D + E) = CD + CE$.

Důkaz. Dokážeme asociativitu násobení. Nejprve si všimneme, že výrazy $(BC)D$ a $B(CD)$ na obou stranách jsou definované a vyjdou matice typu $m \times q$. Na levé straně je BC matice typu $m \times p$, takže součin matic BC a D je definován a výsledkem je matice typu $m \times q$. Podobně se ukáže, že na pravé straně vyjde matice typu $m \times q$.

Vezmeme nyní libovolné $i \in \{1, 2, \ldots, m\}$ a $l \in \{1, 2, \ldots, q\}$ a spočítáme prvek na místě (i, l) v matici $(BC)D$. Označíme-li $BC = (e_{ij})$, pak hledaný prvek je

$$\sum_{k=1}^{p} e_{ik} d_{kl} = \sum_{k=1}^{p} \left(\sum_{j=1}^{n} b_{ij} c_{jk} \right) d_{kl} = \sum_{k=1}^{p} \sum_{j=1}^{n} b_{ij} c_{jk} d_{kl} = \sum_{j=1}^{n} \sum_{k=1}^{p} b_{ij} c_{jk} d_{kl} \ .$$

Ve druhé úpravě jsme použili distributivitu platnou v tělese $\mathbf{T}$ a v poslední úpravě jsme prohodili sumy, což můžeme díky asociativitě sčítání v $\mathbf{T}$. (Zde si můžeme všimnout, že prohazování sum jde interpretovat jako sčítání všech prvků matice dvojím způsobem – po řádcích a po sloupcích.)

Označíme-li $(CD) = (f_{jl})$, pak prvek na místě (i, l) v matici $B(CD)$ je

$$\sum_{j=1}^{n} b_{ij} f_{jl} = \sum_{j=1}^{n} b_{ij} \left(\sum_{k=1}^{p} c_{jk} d_{kl} \right) = \sum_{j=1}^{n} \sum_{k=1}^{p} b_{ij} c_{jk} d_{kl} \ .$$

Prvky na stejných místech v maticích $(BC)D$ a $B(CD)$ se rovnají, takže $(BC)D = B(CD)$.

Zbylé dvě vlastnosti přenecháme do cvičení. □

Asociativitu lze (zatím pouze neformálně) odůvodnit geometricky: Víme, že násobení matic odpovídá skládání zobrazení a skládání zobrazení je asociativní.

Díky asociativitě můžeme pro přirozené číslo n definovat n-tou mocninu čtvercové matice vztahem

$$A^n = \underbrace{AA\dots A}_{n\times} \ .$$

Výsledek totiž nezávisí na uzávorkování.

Další tvrzení hovoří o vztahu násobení matice prvkem tělesa a operacemi sčítání a násobení. Důkazy jsou snadné a přenecháme je jako cvičení.

Tvrzení 4.21. *Jsou-li A, B matice nad tělesem $\mathbf{T}$ typu $m \times n$, C matice nad $\mathbf{T}$ typu $n \times p$ a $a, b \in T$, pak*

(1) $(a+b)A = aA + bA$,
(2) $a(A+B) = aA + aB$,
(3) $a(bA) = (ab)A$,
(4) $1A = A$,
(5) $a(BC) = (aB)C = B(aC)$.

K bodu poznamenejme, že výraz $(Ba)C$ není definován, protože není definován výraz Ba.

Nakonec zformulujeme vztah transpozice a zbylých operací.

Tvrzení 4.22. *Jsou-li A, B matice nad tělesem $\mathbf{T}$ typu $m \times n$, C je matice typu $n \times p$ nad $\mathbf{T}$ a $a \in T$, pak*

(1) $(A+B)^T = A^T + B^T$,
(2) $(aA)^T = aA^T$,
(3) $(A^T)^T = A$.
(4) $(BC)^T = C^T B^T$.

Příklad 4.23. Čtvercová matice $A = (a_{ij})$ řádu n se nazývá *symetrická*, pokud $a_{ij} = a_{ji}$ pro libovolné $i, j \in \{1, 2, \dots, n\}$. Ekvivalentně, A je symetrická, pokud $A^T = A$. Pomocí vlastností z tvrzení 4.22 ukážeme, že pro libovolnou čtvercovou matici A je matice $B = 2AA^T + A^T A$ symetrická:

$$\begin{aligned} B^T &= (2AA^T + A^T A)^T = (2AA^T)^T + (A^T A)^T = 2(AA^T)^T + (A^T A)^T = \\ &= 2(A^T)^T A^T + A^T (A^T)^T = 2AA^T + A^T A = B \ . \end{aligned}$$

Ukázali jsme, že $B = B^T$, matice B je tedy symetrická. Mlčky jsme používali i vlastnosti z tvrzení 4.21, kdy jsme například nepsali závorky ve výrazu $2AA^T$.

Příklad 4.24. Vlastnosti (p1) až (p4) v důkazu věty 2.14 se dokazují pohodlně pomocí vlastností maticových operací. Podívejme se na (p2).

(p2) Jsou-li vektory $\mathbf{w}, \mathbf{z}$ řešením soustavy $(A \mid \mathbf{o})$, pak je vektor $\mathbf{w} + \mathbf{z}$ řešením soustavy $(A \mid \mathbf{o})$.

Skutečně, pokud $\mathbf{w}, \mathbf{z}$ řeší soustavu $(A \mid \mathbf{o})$, čili $A\mathbf{w} = \mathbf{o}$ a $A\mathbf{z} = \mathbf{o}$, pak $A(\mathbf{w}+\mathbf{z}) = A\mathbf{w} + A\mathbf{z} = \mathbf{o}$, neboli $\mathbf{w}+\mathbf{z}$ řeší stejnou soustavu. Použili jsme distributivitu.

4.5. **Další aplikace.**

Viděli jsme, že maticové operace se hodí na práci s některými zobrazeními (jako třeba rotace) a na kompaktní popis soustav lineárních rovnic. Uvedeme některé další příklady využití.

4.5.1. *Rekurentní rovnice.* Asi jste se už setkali s Fibonacciho posloupností definovanou předpisem

$$a_1 = a_2 = 1, \quad a_{i+2} = a_{i+1} + a_i \text{ pro každé } i = 1, 2, \dots$$

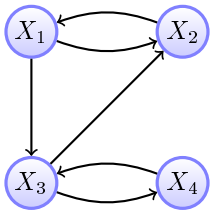
Chtěli bychom najít explicitní vzorec pro výpočet n-tého členu.

Z definice posloupnosti nahlédneme, že dvojice sousedních členů splňuje vztah

$$\begin{pmatrix} a_{i+2} \\ a_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{i+1} \\ a_i \end{pmatrix}$$

(Pro ověření tohoto vztahu použijeme tvrzení 4.14.) Označíme-li C matici 2×2 vystupující v tomto vztahu, vidíme, že

$$\begin{pmatrix} a_3 \\ a_2 \end{pmatrix} = C \begin{pmatrix} a_2 \\ a_1 \end{pmatrix}, \begin{pmatrix} a_4 \\ a_3 \end{pmatrix} = C \begin{pmatrix} a_3 \\ a_2 \end{pmatrix} = C \left(C \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \right) = C^2 \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \ ,$$



Obrázek 5. Letecká spojení mezi městy X_1, X_2, X_3 a X_4 z části 4.5.2

a indukcí dostaneme

$$\begin{pmatrix} a_{i+2} \\ a_{i+1} \end{pmatrix} = C^i \begin{pmatrix} a_2 \\ a_1 \end{pmatrix} = C^i \begin{pmatrix} 1 \\ 1 \end{pmatrix} \ .$$

Podstatným způsobem zde využíváme asociativitu násobení matic. K výpočtu n-tého členu Fibonacciho posloupnosti tedy stačí umět mocnit matice. To se naučíme v kapitole o vlastních číslech a vektorech. Vyjde možná překvapivý vzorec

$$a_n = \frac{\varphi^n}{\sqrt{5}} - \frac{(1-\varphi)^n}{\sqrt{5}} \ ,$$

kde $\varphi = (1+\sqrt{5})/2$ je hodnota zlatého řezu.

4.5.2. *Počet cest.* Na obrázku **??** jsou vyznačena letecká spojení mezi městy X_1, X_2, X_3, X_4. Vypočítáme počet spojení s nejvýše čtyřmi přestupy mezi každou dvojicí měst.

Spojení mezi městy uspořádáme do matice $A = (a_{ij})_{4\times 4}$ nad $\mathbb{R}$ tak, že a_{ij} definujeme rovné 1, pokud z X_i vede cesta do X_j, a $a_{ij} = 0$ jinak.

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

Nyní se zamyslíme jaký je význam prvku na místě (i,j) v matici A^2. Tento prvek je rovný $a_{i1}a_{1j} + a_{i2}a_{2j} + a_{i3}a_{3j} + a_{i4}a_{4j}$. Všimněte si, že k-tý člen součtu je rovný jedné právě tehdy, když z X_i vede spojení do X_j a z X_j vede spojení do X_k, a je rovný nule jinak. Prvek na místě (i,j) v matici A^2 je proto rovný počtu cest z X_i do X_k s právě jedním přestupem.

Podobně nahlédneme, že prvek na místě (i,k) v matici A^n je rovný počtu cest z X_i do X_k s právě $(n-1)$ přestupy. Hledaný počet cest s nejvýše čtyřmi přestupy z X_i do X_k je tedy prvek na místě (i,k) v matici

$$A + A^2 + A^3 + A^4 + A^5 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} +$$
$$+ \begin{pmatrix} 1 & 1 & 2 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 2 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 3 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 2 & 1 & 1 & 1 \\ 0 & 2 & 1 & 1 \end{pmatrix} + \begin{pmatrix} 3 & 2 & 3 & 1 \\ 1 & 3 & 1 & 2 \\ 1 & 3 & 3 & 1 \\ 2 & 1 & 1 & 1 \end{pmatrix} =$$
$$= \begin{pmatrix} 6 & 8 & 7 & 4 \\ 4 & 6 & 4 & 3 \\ 4 & 7 & 6 & 4 \\ 3 & 4 & 4 & 3 \end{pmatrix}$$

4.6. **Blokové matice.**

Někdy je výhodné nahlížet na matici jako rozdělenou do bloků a operace, zejména násobení, provádět blokově.

Vezměme dvě matice nad tělesem $\mathbf{T}$: matici A typu $m\times n$ a matici B typu $n\times p$. Dále nechť $m_1,\dots,m_r$, $n_1,\dots,n_s$ a $p_1,\dots,p_t$ jsou přirozená čísla, pro která

$$m = m_1 + m_2 + \cdots + m_r, \quad n = n_1 + n_2 + \cdots + n_s \quad \text{a} \quad p = p_1 + \cdots + p_t \ .$$

Matici A rozdělíme podélně na prvních m_1 řádků, dalších m_2 řádků, atd. až posledních m_r řádků, a a vertikálně na prvních n_1 sloupců, dalších n_2 sloupců, atd. až posledních n_s sloupců. Matice A se nyní skládá z rs bloků A_{11},

$A_{12}, \dots, A_{1s}, A_{21}, \dots, A_{rs}$.

$$A = \begin{array}{c} \\ m_1 \\ m_2 \\ \vdots \\ m_r \end{array} \begin{array}{c} \begin{array}{cccc} n_1 & n_2 & & n_s \end{array} \\ \left(\begin{array}{c|c|c|c} A_{11} & A_{12} & \vdots\,\vdots & A_{1s} \\ \hline A_{21} & A_{22} & \dots & A_{2s} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline A_{r1} & A_{r2} & \dots & A_{rs} \end{array}\right) \end{array}$$

Každý blok A_{ij} je matice typu $m_i \times n_j$.

Podobně, matici B rozdělíme podélně na oddíly velikosti $n_1, n_2, \dots, n_s$ a vertikálně na oddíly velikosti $p_1, p_2, \dots, p_t$. Matici B tím rozdělíme na st bloků $B_{11}, \dots, B_{st}$:

$$B = \begin{array}{c} \\ n_1 \\ n_2 \\ \vdots \\ n_s \end{array} \begin{array}{c} \begin{array}{cccc} p_1 & p_2 & & p_t \end{array} \\ \left(\begin{array}{c|c|c|c} B_{11} & B_{12} & \vdots\,\vdots & B_{1t} \\ \hline B_{21} & B_{22} & \dots & B_{2t} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline B_{s1} & B_{s2} & \dots & B_{st} \end{array}\right) \end{array} .$$

Součin $C = AB$ lze potom rozdělit do bloků následovně.

$$C = AB = \begin{array}{c} \\ m_1 \\ m_2 \\ \vdots \\ m_r \end{array} \begin{array}{c} \begin{array}{cccc} p_1 & p_2 & & p_t \end{array} \\ \left(\begin{array}{c|c|c|c} C_{11} & C_{12} & \vdots\,\vdots & C_{1t} \\ \hline C_{21} & C_{22} & \dots & C_{2t} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline C_{s1} & C_{s2} & \dots & C_{st} \end{array}\right) \end{array} ,$$

kde pro každé $i \in \{1, 2, \dots, r\}$ a $k \in \{1, 2, \dots, t\}$ platí

$$C_{ik} = \sum_{j=1}^{s} A_{ij} B_{jk} \ .$$

Důkaz, který pouze vyžaduje správně si napsat jednotlivé prvky ve všech maticích a jejich blocích, přenecháme do cvičení.

Příklad 4.25. Matice A, B z příkladu 4.12 o rotacích v prostoru mají přirozenou blokovou strukturu.

$$\left(\begin{array}{cc|c} 0 & 1 & 0 \\ -1 & 0 & 0 \\ \hline 0 & 0 & 1 \end{array}\right), \quad \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & 0 & 1 \\ 0 & -1 & 0 \end{array}\right)$$

Příklad 4.26. Najdeme A^2 pro matici A nad $\mathbb{Z}_7$.

$$A = \begin{pmatrix} 1 & 0 & 2 & 3 & 4 \\ 0 & 1 & 5 & 0 & 6 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Označíme-li

$$B = \begin{pmatrix} 2 & 3 & 4 \\ 5 & 0 & 6 \end{pmatrix} ,$$

máme

$$A^2 = \left(\begin{array}{c|c} I_2 & B \\ \hline 0_{3\times 2} & I_3 \end{array}\right)\left(\begin{array}{c|c} I_2 & B \\ \hline 0_{3\times 2} & I_3 \end{array}\right) = \left(\begin{array}{c|c} II + B0 & IB + BI \\ \hline 0I + I0 & 0B + II \end{array}\right) =$$

$$= \left(\begin{array}{c|c} I & 2B \\ \hline 0 & I \end{array}\right) = \begin{pmatrix} 1 & 0 & 4 & 6 & 1 \\ 0 & 1 & 3 & 0 & 5 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Pro přehlednost jsme od druhé úpravy vynechávali indexy u jednotkových a nulových matic.

4.7. **Regulární matice.** V poslední části této kapitoly se budeme zabývat otázkou, kdy lze čtvercovou matici (nebo příslušné zobrazení) invertovat.

4.7.1. *Geometrický a algebraický pohled.* Začneme geometrickým pohledem. Jak víme, čtvercová matice A nad tělesem $\mathbf{T}$ řádu n určuje zobrazení

$$f_A : T^n \to T^n, \quad f_A(\mathbf{x}) = A\mathbf{x} \ .$$

K tomuto zobrazení existuje inverzní zobrazení $T^n \to T^n$ právě tehdy, když f_A je bijekce. To se dá říct tak, že pro každý aritmetický vektor $\mathbf{b} \in T^n$ existuje právě jeden vzor při zobrazení f_A, tj. právě jeden aritmetický vektor $\mathbf{x} \in T^n$ takový, že $A\mathbf{x} = \mathbf{b}$. V takovém případě říkáme, že A je *regulární.*

Definice 4.27. Čtvercová matice A nad tělesem $\mathbf{T}$ řádu n se nazývá *regulární*, pokud je příslušné zobrazení f_A bijekce, ekvivalentně, pokud má soustava rovnic $A\mathbf{x} = \mathbf{b}$ právě jedno řešení pro každou pravou stranu $\mathbf{b} \in T^n$.

Čtvercová matice, která není regulární, se nazývá *singulární.*

Příklad 4.28. Z geometrického náhledu vidíme, že matice odpovídající rotaci kolem počátku a zrcadlení podle přímky procházející počátkem jsou regulární, protože tato zobrazení jsou bijektivní. Matice odpovídající projekci na osu x v $\mathbb{R}^2$ je singulární, protože toto zobrazení není bijekcí (není dokonce ani prosté ani na).

Je-li A regulární, tedy f_A je bijekce, pak musí existovat inverzní zobrazení $g : T^n \to T^n$, tj. zobrazení, které splňuje $f_A \circ g = g \circ f_A = \mathrm{id}_{T^n}$. Za okamžik ukážeme, že g je opět tvaru f_X pro jistou čtvercovou matici X. Protože skládání zobrazení odpovídá součinu matic a identické zobrazení odpovídá jednotkové matici, vztahy $f_A \circ f_X = f_X \circ f_A = \mathrm{id}_{T^n}$ se ekvivalentně přepíší na $f_{AX} = f_{XA} = f_{I_n}$, a protože různé matice určují různá zobrazení (viz cvičení), dostáváme ekvivalentně $AX = XA = I_n$. Z tohoto důvodu říkáme matici X *matice inverzní k* A.

Definice 4.29. Čtvercová matice A nad tělesem $\mathbf{T}$ řádu n se nazývá *invertovatelná*, pokud existuje čtvercová matice X nad $\mathbf{T}$ řádu n taková, že $AX = XA = I_n$. Matici X nazýváme *inverzní matice k* A a označujeme ji A^{-1}.

Několik poznámek, než ověříme, že zavedené pojmy regulární a invertibilní matice splývají.

- Zdůrazněme, že zavedené pojmy se týkají **pouze čtvercových matic**.
- Z geometrického i algebraického pohledu vidíme, že pro matice obecně neplatí obdoba vlastnosti (N3) z definice tělesa o existenci inverzních prvků. Například projekce na osu x chápaná jako zobrazení z $\mathbb{R}^2$ do $\mathbb{R}^2$ je zobrazení f_A pro matici
$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$
Toto zobrazení není bijekce (není dokonce ani prosté, ani na), takže A není regulární.

  Z algebraického pohledu: Neexistuje matice X taková, že $AX = I_2$ (protože druhý řádek matice AX je vždy nulový), ani matice Y taková, že $YA = I_2$ (protože druhý sloupec matice YA je vždy nulový). Říkáme, že matice A nemá matici *zprava inverzní* ani matici *zleva inverzní.*
- Inverzní matice k invertovatelné matici je určená jednoznačně. Pokud jsou totiž X, Y dvě inverzní matice k A, pak
$$X = XI_n = X(AY) = (XA)Y = I_nY = Y.$$

Je-li matice invertovatelná, pak je regulární. Pokud totiž $AX = XA = I_n$ pak $f_Af_X = f_Xf_A = f_{I_n} = \mathrm{id}_{I_n}$, tedy k f_A existuje oboustrané inverzní zobrazení $f_A^{-1} = f_X$, tedy f_A je bijekce. Opačnou implikaci dokážeme tím, že popíšeme postup jak inverzní matici nalézt. Připomeňme, že vlastně dokazujeme, že inverzní zobrazení k f_A je opět tvaru f_X pro jistou matici X.

4.7.2. *Hledání pravého inverzu.* Pokusme se nyní k dané regulární čtvercové matici A řádu n najít matici X takovou, že $AX = I_n$. (Matici X nazýváme maticí zprava inverzní k A.) Budeme provádět obecnou diskuzi a zároveň ji ilustrovat na příkladu reálné matice

$$A = \begin{pmatrix} 1 & 3 \\ 2 & 9 \end{pmatrix} \ .$$

Pro $i = 1, 2, \ldots, n$ srovnáme i-té sloupce ve vztahu $AX = I_n$ a využijeme $(AX)_{*i} = AX_{*i}$ (viz tvrzení 4.14). Dostáváme, že rovnice $AX = I_n$ je ekvivalentní s

$$AX_{*1} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad AX_{*2} = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \quad \ldots \quad , \quad AX_{*n} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \ .$$

Řešíme tedy n soustav lineárních rovnic se stejnou maticí A s různými pravými stranami. Protože A je regulární, soustavy mají právě jedno řešení. V našem případě řešíme soustavy

$$\begin{pmatrix} 1 & 3 \\ 2 & 9 \end{pmatrix} \begin{pmatrix} x_{11} \\ x_{21} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 3 \\ 2 & 9 \end{pmatrix} \begin{pmatrix} x_{21} \\ x_{22} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \ .$$

Soustavy vyřešíme.

$$\left(\begin{array}{cc|c} 1 & 3 & 1 \\ 2 & 9 & 0 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 3 & 1 \\ 0 & 3 & -2 \end{array}\right), \quad \begin{pmatrix} x_{11} \\ x_{12} \end{pmatrix} = \begin{pmatrix} 3 \\ -\frac{2}{3} \end{pmatrix}$$

$$\left(\begin{array}{cc|c} 1 & 3 & 0 \\ 2 & 9 & 1 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 3 & 0 \\ 0 & 3 & 1 \end{array}\right), \quad \begin{pmatrix} x_{21} \\ x_{22} \end{pmatrix} = \begin{pmatrix} -1 \\ \frac{1}{3} \end{pmatrix}$$

Matice inverzní zprava je tedy

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

Provedeme nyní dvě modifikace tohoto postupu.

Protože je matice všech n-soustav stejná, totiž A, je možné všechny řešit stejnými úpravami. Proto je můžeme řešit najednou tak, že pravé strany napíšeme vedle matice soustavy všechny vedle sebe a upravíme celou matici do odstupňovaného tvaru. Dopočtení zpětnou substitucí pak proběhne jako předtím, zvlášť pro každou pravou stranu. V našem případě

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

Před druhou modifikací si uvědomme, jak vypadá odstupňovaný tvar matice A po Gaussově eliminaci. Protože předpokládáme, že rovnice $A\mathbf{x} = \mathbf{b}$ má právě jedno řešení pro každé $\mathbf{b}$, nemůžou při řešení soustav $AX_{*1} = (1, 0, \dots, 0)^T, \dots$ existovat volné proměnné (pokud by existovaly, pak $A\mathbf{x} = \mathbf{b}$ buď nemá žádné řešení, nebo každé volbě volné proměnné odpovídá řešení, takže by soustava měla více než jedno řešení). Tím pádem musí pro odstupňovaný tvar matice A platit $r = n$ a $k_1 = 1, k_2 = 2, \dots, k_n = n$. Jinými slovy, odstupňovaný tvar je horní trojúhelníková matice s nenulovými všemi prvky na diagonále. (Pro čtvercové matice je tato podmínka zřejmě ekvivalentní tomu, že odstupňovaný tvar neobsahuje nulový řádek.)

Ke slíbené modifikaci. Po převedení soustav na odstupňovaný tvar budeme dále pokračovat v řádkových úpravách tak, aby na levé straně vznikla jednotková matice. To lze provést díky tomu, že odstupňovaný tvar je horní trojúhelníková matice s nenulovými prvky na diagonále. Postup je takový, že nejprve „doeliminujeme“ druhý sloupec – přičtením vhodného násobku druhého řádku k prvnímu docílíme, že hodnota na pozici $(1, 2)$ je nula. Pak vynulujeme přičtením vhodných násobků pozice $(1, 3)$ a $(2, 3)$, atd. Tímto vznikne diagonální matice s nenulovými prvky na diagonále, ze které umíme udělat jednotkovou vynásobením řádků vhodnými prvky.

V našem případě máme

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

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

Soustavu s jednotkovou maticí je velmi snadné vyřešit – řešením je zřejmě přímo pravá strana. Postup lze nyní shrnout takto: řádkovými úpravami převedeme matici $(A \mid I_n)$ do tvaru $(I_n \mid X)$ a vpravo si přečteme výslednou matici zprava inverzní k A.

4.7.3. *Jiný pohled.* Ukázali jsme, že k regulární matici existuje matice inverzní zprava. V řeči zobrazení, nalezli jsme X takovou, že $f_A \circ f_X = \mathrm{id}_{T^n}$. Protože f_A je bijekce, lze z tohoto vztahu usoudit (viz cvičení **??** v kapitole 1), že $f_X \circ f_A = \mathrm{id}_{T^n}$, což v řeči matic znamená, že $XA = I_n$.

My ukážeme, že platí $XA = I_n$, jiným způsobem, který se nám jednak bude hodit k důkazu hlavní věty 4.30 a který rovněž poskytuje alternativní pohled na odvozený postup

$$(A \mid I_n) \sim \cdots \sim (I_n \mid X) .$$

Podívejme se na tento postup maticově. V tvrzení 4.17 jsme nahlédli, že elementární řádková úprava odpovídá násobení jistou maticí zleva. Úpravy lze tedy psát

$$(A \mid I_n) \sim E_1(A \mid I_n) \sim E_2(E_1(A \mid I_n)) \sim \dots ,$$

kde $E_1, E_2, \dots$ jsou elementární matice příslušných úprav. Vezmeme v úvahu asociativitu násobení a pravidlo o násobení po blocích, můžeme postup psát

$$(A \mid I_n) \sim (E_1A \mid E_1I_n) = (E_1A \mid E_1) \sim (E_2E_1A \mid E_2E_1) \sim \cdots \sim$$

$$\sim (E_k \dots E_2E_1A \mid E_k \dots E_2E_1) = (I_n \mid X) .$$

Srovnáním pravých bloků dostaneme $X = E_k \dots E_2E_1$, takže srovnáním levých bloků dostaneme $XA = I_n$. Máme $XA = AX = I_n$, tedy X je inverzní matice k A. Rovněž vidíme, že X je součinem elementárních matic.

4.7.4. *Matice inverzní zprava a zleva.* Pro zobrazení $f : X \to X$ obecně neplatí, že f je bijekce, pokud f je prosté, ani neplatí, že f je bijekce, pokud f je na, viz **??**. To je rozdíl oproti situaci, kdy množina X je konečná. Ve větě 4.30 si všimneme, že zobrazení tvaru f_A (pro čtvercovou matici A) jsou „spořádaná“ v tom smyslu, že kdykoliv f_A je prosté nebo na, pak f_A je bijekce.

Z kapitoly 1 víme, že f je prosté právě tehdy, když k f existuje zobrazení inverzní zleva, a f je na právě tehdy, když k f existuje zobrazení inverzní zprava[1]. Maticově tedy lze zmíněnou spořádanost přeformulovat tak, že kdykoliv má čtvercová matice A matici X inverzní zprava nebo zleva, pak již je A invertovatelná a platí $X = A^{-1}$.

4.7.5. *Charakterizace.* Následující věta shrnuje různé ekvivalentní charakterizace regularity – geometrické charakterizace, charakterizace pomocí odstupňovaného tvaru a algebraické charakterizace pomocí invertovatelnosti a elementárních matic.

Věta 4.30. *Nechť A je čtvercová matice nad tělesem $\mathbf{T}$ řádu n. Následující tvrzení jsou ekvivalentní.*

(1) *A je regulární.*
(2) *Zobrazení f_A je na.*
(3) *Zobrazení f_A je prosté.*
(4) *Soustava $A\mathbf{x} = \mathbf{o}$ má jediné řešení ($\mathbf{x} = \mathbf{o}$).*

(5) *Gaussova eliminace převede matici A do horního trojúhelníkového tvaru s nenulovými prvky na diagonále (ekvivalentně odstupňovaného tvaru bez nulových řádků).*
(6) *Matici A lze převést elementárními řádkovými (ekvivalentně sloupcovými) úpravami do jednotkové matice I_n.*

(7) *A je invertovatelná.*
(8) *Existuje čtvercová matice X řádu n taková, že $AX = I_n$.*
(9) *Existuje čtvercová matice X řádu n taková, že $XA = I_n$.*
(10) *A je součinem elementárních matic.*

Důkaz. Implikace (1) ⇒ (3) ⇒ (4) a (1) ⇒ (2) jsou triviální.

Argumenty pro (2) nebo (4) ⇒ (5) ⇒ (6) ⇒ (7) ⇒ (1) byly již předvedeny výše, takže je jen stručně shrneme. U (6) budeme pracovat s řádkovou verzí.

(4) ⇒ (5). Řešíme-li soustavu rovnic $A\mathbf{x} = \mathbf{o}$ Gaussovou eliminací a získáme odstupňovaný tvar s alespoň jednou volnou proměnnou, pak má soustava více řešení (u homogenní soustavy se ani nemůže stát, že řešení neexistuje). Podobně ukážeme (2) ⇒ (5). Pokud odstupňovaný tvar matice A má nulový řádek, pak soustava $A\mathbf{x} = \mathbf{b}$ nemá pro nějakou pravou stranu řešení, takže f_A není na. Toto si rozmyslete podrobně jako cvičení.

(5) ⇒ (6). Matici A převedeme do horní trojúhelníkové matice s nenulovými prvky na diagonále a pak doeliminujeme postupně druhý sloupec, třetí sloupec, atd. Získáme diagonální matici a stačí vynásobit řádky vhodnými prvky tělesa.

(6) ⇒ (7). Použijeme postup $(A \mid I_n) \sim \cdots \sim (I_n \mid X)$. Díváme-li se na tento postup jako na řešení n-soustav lineárních rovnic, máme $AX = I_n$. Díváme-li se na něj jako na násobení elementárními maticemi zleva, získáme $XA = I_n$.

(7) ⇒ (1). Předvedeme algebraický argument, již jsme viděli geometrický. Platí-li $A\mathbf{x} = \mathbf{b}$, pak $A^{-1}A\mathbf{x} = A^{-1}\mathbf{b}$, takže rovnice má nejvýše jedno řešení, a to $\mathbf{x} = A^{-1}\mathbf{b}$. Na druhou stranu, tento vektor je skutečně řešením, protože $A(A^{-1}\mathbf{b}) = \mathbf{b}$.

Nyní jsme dokázali, že tvrzení (1), (2), (3), (4), (5), (6), (7) jsou ekvivalentní. Ekvivalenci regularity s podmínkou (10) ukážeme v tvrzení 4.39.

Triviálně platí (7) ⇒ (8), (9), takže stačí dokázat třeba (8) ⇒ (2) a (9) ⇒ (3).

(8) ⇒ (2). Je-li $AX = I_n$, pak $f_A f_X = f_{I_n} = \mathrm{id}_{T^n}$, takže k zobrazení f_A existuje zobrazení inverzní zprava, tedy f_A je na. Implikace (9) ⇒ (2) se dokáže obdobně. □

Příklad 4.31. Najdeme matici inverzní k matici A nad tělesem $\mathbb{Z}_5$, pokud existuje.

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

[1] to je axiom výběru

Řádkovými úpravami upravujeme $(A \mid I_3)$:

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

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

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

Takže A je regulární a platí

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

Příklad 4.32. Najdeme matici inverzní k matici A nad tělesem $\mathbb{Z}_2$, pokud existuje.

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

Opět řádkovými úpravami upravujeme $(A \mid I_n)$:

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

Odstupňovaný tvar matice A není horní trojúhelníková matice s nenulovými prvky na diagonále, takže A je singulární podle (1)⇔(5) z věty 4.30 a inverzní matice neexistuje (podle bodu (7) stejné věty).

Chápeme-li A jako matici nad tělesem $\mathbb{Z}_3$ nebo $\mathbb{R}$, pak je regulární.

Příklad 4.33. Matice

$$A = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$$

nad $\mathbb{R}$ je pro libovolné $\alpha \in \mathbb{R}$ regulární a inverzní matice je

$$A^{-1} = \begin{pmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos(-\alpha) \end{pmatrix} = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} .$$

To lze nahlédnout z úvahy, že f_A je rotace o α, což je bijekce a inverzním zobrazení je rotace o $-\alpha$.

Příklad 4.34. Dalším příkladem, kdy je výhodnější se trochu zamyslet, než ihned začít počítat podle odvozeného algoritmu, je výpočet inverzní matice k reálné matici

$$A = \begin{pmatrix} 1 & 1 & 1 \\ \frac{1}{2} & 0 & 0 \\ 1 & 0 & \frac{1}{3} \end{pmatrix} .$$

Hledáme matici X takovou, že $AX = I_3$. Znovu si uvědomíme, že při násobení matice X zleva maticí A děláme lineární kombinace řádků matice X, kde koeficienty jsou v řádcích matice A (tvrzení 4.14.(1)). Druhý řádek matice A nám říká, že druhý řádek výsledku (to je řádek $(0,1,0)$) je $1/2$-násobek prvního řádku matice X. Z toho okamžitě vidíme, že první řádek matice X je $(2,0,0)$.

$$X = \begin{pmatrix} 0 & 2 & 0 \\ ? & ? & ? \\ ? & ? & ? \end{pmatrix} .$$

Z posledního řádku matice A vidíme, že třetí řádek výsledku (to je $(0,0,1)$) je roven 1-násobku prvnímu řádku matice X (to už víme, že je $(2,0,0)$) plus $1/3$-násobek třetího řádku matice X. Z toho snadno dopočteme, že třetí řádek X je $(0,-6,3)$.

$$X = \begin{pmatrix} 0 & 2 & 0 \\ ? & ? & ? \\ 0 & -6 & 3 \end{pmatrix} .$$

Z prvního řádku matice A pak podobně dopočítáme druhý řádek matice X a získáme

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

Snadno ověříme, že X je skutečně matice inverzní.

Jako cvičení proveďte podobnou úvahu sloupcově pro rovnici $XA = I_3$ a řádkově pro rovnici $XA = I_3$.

Příklad 4.35. Pokud A je regulární matice, pak každá soustava rovnic $A\mathbf{x} = \mathbf{b}$ má podle definice právě jedno řešení. Vynásobením obou stran maticí A^{-1} zleva získáme explicitní vzorec:

$$\mathbf{x} = A^{-1}\mathbf{b} .$$

Například řešením soustavy rovnic nad $\mathbb{Z}_5$

$$\begin{pmatrix} 0 & 2 & 4 \\ 3 & 1 & 4 \\ 4 & 2 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

je vektor

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = A^{-1}\mathbf{b} = A = \begin{pmatrix} 2 & 4 & 1 \\ 2 & 1 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 3 \\ 3 \\ 0 \end{pmatrix} ,$$

kde A^{-1} jsme spočítali v příkladu 4.31.

Na praktické řešení se tento vzorec nehodí, protože Gaussova eliminace a zpětná substituce je rychlejší. Vzorec se hodí pro teoretické úvahy, nebo pokud řešíme mnoho soustav s jednou pravou stranou, i když i v tomto případě spíše používáme jiné techniky, jako LU-rozklad.

Příklad 4.36. V odstavci 4.5.1 jsme odvodili, že pro členy Fibonacciho posloupnosti $a_1, a_2, \ldots$ platí

$$\begin{pmatrix} a_{i+2} \\ a_{i+1} \end{pmatrix} = C^i \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad \text{kde } \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} .$$

Matici C lze zapsat ve tvaru

$$C = XDX^{-1}, \quad \text{kde } D = \begin{pmatrix} \varphi & 0 \\ 0 & 1-\varphi \end{pmatrix}, \quad X = \begin{pmatrix} 1 & 1 \\ \varphi - 1 & -\varphi \end{pmatrix} .$$

Tento vztah můžeme samozřejmě ověřit. Jak jej lze získat se dozvíme v kapitole o vlastních číslech a vlastních vektorech.

Když už jej známe, můžeme vypočítat n-tou mocninu matice C:

$$C^n = \underbrace{(XDX^{-1})(XDX^{-1})\ldots(XDX^{-1})}_{n\times} = XD^nX^{-1}$$

Mocninu diagonální matice vypočítáme snadno a dosazením pak získáme vzorec pro n-tý člen.

Důležité příklady regulárních matic tvoří elementární matice. To je v souladu se skutečností, že elementární úpravy jsou vratné.

Tvrzení 4.37. *Každá elementární matice je regulární, navíc inverzní matice k regulární matici je opět elementární.*

Důkaz. K důkazu můžeme přímo najít matice inverzní, jsou jimi matice úprav, které vrací příslušnou elementární úpravu. Pak pouze využijeme ekvivalenci invertovatelnosti a regulárnosti z charakterizační věty 4.30. □

4.7.6. *Regularita a maticové operace.* Nakonec se podíváme na vztah invertování a maticových operací.

Tvrzení 4.38. *Jsou-li A, B regulární matice nad stejnými tělesem $\mathbf{T}$ stejného řádu a $t \in T$ nenulový prvek, pak platí*

(1) *A^{-1} je regulární a platí $(A^{-1})^{-1} = A$,*
(2) *A^T je regulární a platí $(A^T)^{-1} = (A^{-1})^T$,*
(3) *$(tA)^T$ je regulární a platí $(tA)^{-1} = t^{-1}A^{-1}$,*
(4) *AB je regulární a platí $(AB)^{-1} = B^{-1}A^{-1}$.*

Důkaz. Důkaz můžeme provést tak, že ukážeme, že popsané matice jsou skutečně matice inverzní (stačí z jedné strany). Například $(AB)^{-1} = B^{-1}A^{-1}$, protože $(B^{-1}A^{-1})(AB) = B^{-1}(A^{-1}A)B = B^{-1}B = I$. □

Body (1), (3), (4) v tvrzení mají geometrickou interpretaci, kterou si rozmyslete jako cvičení. Transponování budeme umět geometricky interpretovat až později.

Pro sčítání podobné tvrzení neplatí, stačí se podívat na součet $A + (-A)$, kde matice A (a tím pádem i $-A$) je regulární, například $A = I_n$.

Pomocí bodu (4) dokončíme důkaz charakterizační věty 4.30.

Tvrzení 4.39. *Čtvercová matice A je regulární právě tehdy, když jde napsat jako součin elementárních matic.*

Důkaz. Každá elementární matice je regulární podle tvrzení 4.37, takže podle bodu (4) v předchozím tvrzení je libovolný součin elementárních matic regulární. To dokazuje implikaci zprava doleva.

Naopak, je-li A regulární, pak ji lze elementárními řádkovými úpravami převést na jednotkovou matici (podle bodu (5) charakterizační věty 4.30). Elementární řádkové úpravy se dají napsat jako násobení zleva elementární maticí, takže existují elementární matice $E_1, E_2, \dots, E_k$ takové, že

$$E_k \dots E_2 E_1 A = I_n \ ,$$

kde n je řád A. Protože elementární matice jsou regulární (podle tvrzení 4.37), tedy i invertibilní, můžeme vztah upravit na

$$A = E_1^{-1} E_2^{-1} \dots E_k^{-1} \ .$$

Teď jsme hotovi, protože inverzní matice k elementárním maticí jsou elementární (opět podle tvrzení 4.37). □

Příklad 4.40. Z důkazu také vidíme postup, jak rozklad na elementární matice nalézt. Najdeme rozklad matice

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

Matici převedeme elementárními řádkovými úpravami na jednotkovou a zaznamenáme si úpravy.

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

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

Matice úprav jsou

$$E_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad E_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix}, \quad E_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{pmatrix},$$

$$E_4 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad E_5 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

Takže máme

$$A = E_1^{-1} E_2^{-1} E_3^{-1} E_4^{-1} E_5^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 3 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

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

Cvičení

1. Co musí splňovat matice A, B, aby byly definovány oba součiny AB i BA.

2. Geometricky interpretujte násobení matice prvkem tělesa a sčítání matic.

3. Geometricky popište zobrazení, které vznikne složením osové souměrnosti v $\mathbb{R}^2$ podle osy x a otočením o $\pi/2$. Srovnejte s algebraickým výpočtem v příkladu na násobení matic. Stejnou úlohu řešte pro složení v opačném pořadí.

4. Najděte matici, která odpovídá osové souměrnosti podle přímky $y = ax$, kde $a \in \mathbb{R}$.

5. Dokažte, že součin dvou horních trojúhelníkových matic stejného řádu je opět horní trojúhelníková matice. Podobně pro dolní trojúhelníkové matice i diagonální matice.

6. Najděte nenulovou reálnou matici A typu 2×2, ke které neexistuje matice inverzní (tj. neexistuje matice B taková, že $AB = BA = I_2$). Interpretujte geometricky.

7. Pro matice neplatí obdoba tvrzení 3.3.(6): Najděte reálnou čtvercovou matici $A \neq 0_{2\times 2}$, pro kterou $A^2 = 0_{2\times 2}$. Interpretujte geometricky.

8. Dokažte vlastnosti (p1), (p3) a (p4) z důkazu věty 2.14.

9. Vypočítejte n-tou mocninu matice

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

10. Ukažte, že násobení elementární maticí zprava odpovídá elementární sloupcové úpravě.

11. Ukažte, že pro čtvercové matice stejného řádu nad stejným tělesem obecně neplatí vztah $(A+B)^2 = A^2 + 2AB + B^2$. Nalezněte podobný, ale platný vztah.

12. Dokončete důkaz tvrzení 4.20.

13. Dokažte tvrzení 4.21.

14. Dokažte tvrzení 4.22.

15. Matice se nazývá antisymetrická, pokud $A = -A^T$. Je pravda, že antisymetrická matice má vždy na hlavní diagonále nuly? (Pozor na vlastnosti tělesa, ve kterém pracujeme!)

16. Dokažte vzorec pro blokové násobení matic.

17. Najděte A^n pro matici z příkladu 4.26.

18. Nechť $A \neq B$ jsou matice stejného typu nad stejným tělesem. Dokažte, že příslušná zobrazení f_A a f_B jsou různá.

19. Navrhněte alternativní postup na převod regulární matice na jednotkovou řádkovými úpravami tak, aby po eliminaci sloupce byly rovnou všechny členy, kromě diagonálního, nulové.

20. Spočítejte znovu příklad 4.34 alternativními postupy navržené v tomto příkladu.

21. Ke každé elementární matici najděte příslušnou matici inverzní, viz tvrzení 4.37.

22. Předpokládejme, že odstupňovaný tvar matice A obsahuje nulový řádek. Dokažte, že potom existuje pravá strana $\mathbf{b}$ taková, že soustava $A\mathbf{x} = \mathbf{b}$ nemá ani jedno řešení (tj. f_A není na).

23. Dokažte implikaci (2) $\Rightarrow$ (5) z věty 4.30.

24. Dokažte přímo implikaci (9) $\Rightarrow$ (3) z věty 4.30.

25. Dokažte tvrzení 4.38 a vysvětlete geometrický význam.

26. Dokažte, že n-tá mocnina diagonální matice je diagonální a na diagonále jsou n-té mocniny původních prvků. Dokončete výpočet n-tého členu Fibonacciho posloupnosti v příkladu 4.36.

5. Vektorové prostory

Cíl. *Zobecněním aritmetických vektorů definujeme základní pojem lineární algebry, vektorový prostor. Budeme zkoumat důležité pojmy jako podprostor, lineární obal, množina generátorů, lineární závislost a nezávislost, báze a dimenze. Motivací je porozumět geometrickým vztahům mezi vektory a podprostory (rovné útvary procházející počátkem) například v rovině a v prostoru. To nám také umožní lépe porozumět řešení soustav lineárních rovnic.*

5.1. **Definice, příklady a základní vlastnosti.** V kapitole o tělesech jsme si všimli, jaké vlastnosti čísel využíváme při řešení lineárních rovnic, a reálná čísla jsme zobecnili na tělesa. Odměnou za větší abstraktnost je větší použitelnost. Stejné věty, například o soustavách rovnic nebo invertování matic, můžeme použít jak pro reálná čísla, tak pro komplexní čísla, tělesa $\mathbb{Z}_p$, nebo také například pro racionální funkce.

V této kapitole zobecníme $\mathbb{R}^n$, tedy množinu n-tic reálných čísel, na *vektorový prostor*. Vektorový prostor nad $\mathbb{R}$ tvoří množina (jejíž prvky nazýváme vektory), operace sčítání vektorů a operace násobení vektoru reálným číslem. Tyto ingredience musí splňovat sadu axiomů, které jsou ve shodě s představou vektoru jako „šipky“ a operací prováděných podle obrázku **??**.

OBRAZEK

Obecněji definujeme vektorový prostor nad tělesem $\mathbf{T}$, kde místo násobení vektoru reálným číslem máme operace násobení vektoru prvkem T.

Definice 5.1. Nechť $\mathbf{T}$ je těleso. *Vektorovým prostorem* $\mathbf{V}$ *nad tělesem* $\mathbf{T}$ rozumíme množinu V spolu s binární operací $+$ na V (tj. $+$ je zobrazení z $V \times V$ do V) a operací $\cdot$ násobení vektorů prvky tělesa (tj. $\cdot$ je zobrazení z $T \times V$ do V), které splňují následující axiomy.

(vS1) Pro libovolné $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ platí $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$.
(vS2) Existuje $\mathbf{o} \in V$ takový, že pro libovolné $\mathbf{v} \in V$ platí $\mathbf{v} + \mathbf{o} = \mathbf{v}$.
(vS3) Pro každé $\mathbf{v} \in V$ existuje $-\mathbf{v} \in V$ takové, že $\mathbf{v} + (-\mathbf{v}) = \mathbf{o}$.
(vS4) Pro libovolné $\mathbf{u}, \mathbf{v} \in V$ platí $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$.
(vN1) Pro libovolné $\mathbf{v} \in V$ a $a, b \in T$ platí $a \cdot (b \cdot \mathbf{v}) = (a \cdot b) \cdot \mathbf{v}$.
(vN2) Pro libovolné $\mathbf{v} \in V$ platí $1 \cdot \mathbf{v} = \mathbf{v}$.
(vD1) Pro libovolné $\mathbf{v} \in V$ a $a, b \in T$ platí $(a + b) \cdot \mathbf{v} = a \cdot \mathbf{v} + b \cdot \mathbf{v}$.
(vD2) Pro libovolné $\mathbf{u}, \mathbf{v} \in V$ a $a \in T$ platí $a \cdot (\mathbf{u} + \mathbf{v}) = a \cdot \mathbf{u} + a \cdot \mathbf{v}$.

Prvkům V říkáme *vektory* a prvky T nazýváme *skaláry*.

„Operace“ $\cdot$ není binární operací ve smyslu definice 3.1, protože násobíme prvky dvou různých množin. Místo $a \cdot \mathbf{v}$, kde $a \in T$ a $\mathbf{v} \in V$, píšeme často $a\mathbf{v}$. Nikdy neprohazujeme pořadí, tj. výrazy $\mathbf{v} \cdot a$ a $\mathbf{v}a$ nejsou definované. Jak je běžné u těles, úmluva je, že $\cdot$ má přednost před $+$, proto nemusíme ve výrazech na pravé straně v axiomech (vD1) a (vD2) psát závorky.

V definici je implicitně obsaženo, že součet $\mathbf{u} + \mathbf{v}$ je definován pro každou dvojici vektorů $\mathbf{u}, \mathbf{v} \in V$ a násobení vektoru skalárem $a\mathbf{v}$ je definováno pro každé $a \in T, \mathbf{v} \in V$. Z definice rovněž vyplývá, že množina V je neprázdná, protože musí obsahovat podle (vS2) alespoň nulový vektor.

Axiomy (vS1), (vS2), (vS3), (vS4) jsou stejné jako axiomy pro sčítání v tělese. Stejně jako v tělese platí, že nulový prvek a opačné prvky jsou určené jednoznačně. Máme teď dvě různé nuly, 0 v tělese $\mathbf{T}$ a $\mathbf{o}$ ve vektorovém prostoru $\mathbf{V}$. Axiom (vN1) připomíná asociativitu násobení a (vN2) existenci jednotkového prvku, i když zde je podstatný rozdíl v tom, že násobíme prvky různých množin. Axiomy (vD1) a (vD2) připomínají distributivitu.

5.1.1. *Aritmetické vektorové prostory a další příklady.* Základním příkladem vektorového prostoru je množina n-tic prvků tělesa.

Definice 5.2. Nechť $\mathbf{T}$ je těleso a n je přirozené číslo. *Aritmetickým vektorovým prostorem nad* $\mathbf{T}$ *dimenze* n rozumíme množinu všech n-složkových aritmetických (sloupcových) vektorů T^n spolu s přirozenými operacemi $+$ a $\cdot$ (definovanými jako v definici 2.2). Značíme $\mathbf{T}^n$.

To, že aritmetický vektorový prostor je skutečně vektorovým prostorem jsme formulovali a dokázali obecně pro matice v tvrzení 4.19 a tvrzení 4.21.

Aritmetické vektorové prostory (a jejich nekonečně dimenzionální varianty, viz cvičení) jsou velmi konkrétní, zároveň ale v jistém smyslu „jediné“ příklady vektorových prostorů. Uvidíme, že v každém vektorovém prostoru lze zvolit soustavu souřadnic (tzv. bázi), a místo vektorů můžeme počítat s jejich souřadnicemi stejně jako v

aritmetickém vektorovém prostoru. Omezit se ale na studium aritmetických vektorových prostorů není výhodné z mnoha důvodů.

Jedním z nich je, že vektorový prostor (hlavně nad $\mathbb{R}$) si představujeme jako množinu šipek na nekonečném papíru, v prostoru, apod. Z tohoto prostoru se stává aritmetický vektorový prostor až po volbě nějaké soustavy souřadnic, kdežto operace s vektory na této volbě nezávisí. Žádná volba souřadnic nemusí být přirozená, nebo různé volby mohou být výhodné v různých situacích. Například množina všech řešení rovnice $2x_1 + 3x_2 + 4x_3 = 0$ je rovina, tedy „v podstatě totéž co $\mathbb{R}^2$“, ale asi by bylo těžké argumentovat, že nějaká konkrétní volba souřadnic je ta nejlepší. Přesný význam výrazů typu „v podstatě totéž co $\mathbb{R}^2$“ uvidíme později.

Dalším důvodem je, že u některých vektorových prostorů není ihned patrné, že se v podstatě jedná jen o n-tice prvků tělesa. Navíc i když to někdy vidět je, není vždy výhodné se na prostory takto dívat, například proto, že na dané množině máme i jiné operace, které jsou při takovém pohledu nepřehledné, apod. Uvedeme několik příkladů vektorových prostorů.

- Množina všech polynomů stupně nejvýše 173 s reálnými koeficienty (nebo jiného daného maximálního stupně, s koeficienty v jiném tělese) s běžnými operacemi sčítání polynomů a násobení polynomu reálným číslem. Tento vektorový prostor je „v podstatě“ $\mathbb{R}^{174}$, protože na polynom $a_0 + a_1x + \cdots + a_{173}x^{173}$ se můžeme dívat jako na 174-ici koeficientů $(a_0, a_1, \ldots, a_{174})^T$ a operace jsou při tomto pohledu stejné jako v $\mathbb{R}^{174}$.
- Množina všech matic typu 7×15 nad tělesem $\mathbb{Z}_3$ s běžnými operacemi + a $\cdot$ (nebo jiného daného typu nad jiným tělesem). Vzhledem k operacím + a $\cdot$ se tato množina chová stejně jako množina $7 \cdot 15 = 105$-tic, takže tento vektorový prostor je „v podstatě“ $\mathbb{Z}_3^{105}$. (To, že množina matic daného typu nad daným tělesem je vektorový prostor jsem formulovali v tvrzení 4.19 a tvrzení 4.21.) Když matice daného typu sčítáme a násobíme skalárem, můžeme se na ně dívat jako na n-tice prvků tělesa, ale tento pohled není výhodný například když matice interpretujeme jako zobrazení, násobíme je nebo invertujeme.

Pro prostory matic zavedeme značení.

Definice 5.3. Vektorový prostor matic nad $\mathbf{T}$ typu $m \times n$ s běžnými operacemi sčítání a násobení prvkem T značíme $\mathbf{T}^{m\times n}$.

Aritmetický vektorový prostor $\mathbf{T}^n$ lze chápat jako $\mathbf{T}^{n\times 1}$.

Následují další příklady vektorových prostorů.

- Množina všech podmnožin množiny $\{1, 2, \ldots, 11\}$ (nebo jiné dané množiny X) spolu s operací symetrické diference, tj. $A+B = (A \setminus B)\cup(B \setminus A)$, je vektorový prostor nad $\mathbb{Z}_2$. Násobení skalárem je $0 \cdot A = \emptyset, 1 \cdot A = A$ pro libovolné $A \subseteq X$. Jako cvičení dokažte, že toto je skutečně vektorový prostor, a vysvětlete, proč je tento prostor „v podstatě“ $\mathbb{Z}_2^{11}$.
- Množina komplexních čísel je vektorovým prostorem nad $\mathbb{R}$ (s běžnými operacemi). Vzhledem ke sčítání a násobení reálným číslem se komplexní číslo $a + bi$ chová stejně jako dvojice $(a, b)^T$, takže z tohoto pohledu je $\mathbb{C}$ v podstatě $\mathbb{R}^2$. Pokud chápeme komplexní čísla jako vektorový prostor nad $\mathbb{R}$, zapomínáme vlastně na násobení v $\mathbb{C}$, pamatujeme si pouze sčítání a násobení reálným číslem.
- Obecněji, každé těleso $\mathbf{T}$ je vektorový prostor nad libovolným svým podtělesem $\mathbf{S}$. (Podtěleso tělesa $\mathbf{T}$ je podmnožina, která tvoří spolu se stejnými operacemi těleso.) Například $\mathbb{R}$ je vektorový prostor nad $\mathbb{Q}$, ale není vidět, že reálná čísla jdou vnímat jako n-tice racionálních. Dimenze n je zde nespočetná a potřebovali bychom zobecnění definice aritmetického prostoru (viz cvičení). U tohoto příkladu souřadná soustava dokonce nejde v jistém smyslu zkonstruovat.

  U jiných příkladů je situace přehlednější, například $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ s běžnými operacemi je vektorový prostor nad $\mathbb{Q}$. Skutečně, číslo $a + b\sqrt{2}$ lze chápat jako dvojici $(a, b)^T \in \mathbb{Q}^2$. Není ale na první pohled patrné, že každá dvojice odpovídá právě jednomu číslu, důkaz je přenechán jako cvičení.

  Vlastnosti těchto vektorových prostorů, jako například dimenze, jsou důležité například v již zmíněných problémech kvadratury kruhu, trisekce úhlu, zdvojení krychle a „neřešitelnosti“ rovnic pátého stupně.
- Množina všech funkcí z $\mathbb{R}$ do $\mathbb{R}$ tvoří spolu s přirozenými operacemi vektorový prostor nad $\mathbb{R}$. Podobnými příklady jsou množina všech spojitých funkcí na $\mathbb{R}$, množina diferencovatelných funkcí, množina polynomiálních funkcí, nebo třeba množina spojitých funkcí na intervalu $[0, 1]$.

  Toto jsou důležité příklady vektorových prostorů, kterými se budete dále zabývat hlavně v jiných předmětech (například funkcionální analýze). My se budeme soustředit hlavně na tzv. prostory konečné dimenze.

5.1.2. *Jednoduché vlastnosti.* Formulujeme některé vlastnosti všech vektorových prostorů. Dokazují se podobně jako příslušné vlastnosti pro tělesa v tvrzení 3.3, proto důkaz přenecháme jako cvičení.

Tvrzení 5.4. *V každém vektorovém prostoru* $\mathbf{V}$ *nad tělesem* $\mathbf{T}$ *platí*

(1) *nulový vektor* $\mathbf{o}$ *je určen jednoznačně,*
(2) *rovnice* $\mathbf{u}+\mathbf{x}=\mathbf{v}$ *má pro pevná* $\mathbf{u},\mathbf{v}\in V$ *právě jedno řešení, speciálně, opačný vektor* $\mathbf{v}$ *je vektorem* $\mathbf{v}$ *určen jednoznačně,*
(3) $0\mathbf{v}=\mathbf{o}$ *pro libovolný vektor* $\mathbf{v}\in V$*,*
(4) $a\mathbf{o}=\mathbf{o}$ *pro libovolný skalár* $a\in T$*,*
(5) *je-li* $a\mathbf{v}=\mathbf{o}$*, pak buď* $a=0$ *nebo* $\mathbf{v}=\mathbf{o}$*,.*
(6) $-\mathbf{v}=(-1)\mathbf{v}$ *pro libovolný vektor* $\mathbf{v}\in V$*, speciálně* $-(-\mathbf{v})=\mathbf{v}$*,*

Axiomy vektorového prostoru i uvedené jednoduché důsledky budeme používat zcela automaticky. Je dobré si při prvním čtení důkazů v této kapitole podrobně rozmyslet všechny kroky a použité axiomy.

5.2. **Podprostory.**

Prvním pojmem, který budeme pro vektorové prostory studovat, je *podprostor*.

Definice 5.5. Nechť $\mathbf{V}$ je vektorový prostor nad $\mathbf{T}$. Vektorový prostor $\mathbf{U}$ nad $\mathbf{T}$ je *podprostorem* $\mathbf{V}$, pokud $U\subseteq V$ a operace $+$ a $\cdot$ v $\mathbf{U}$ se shodují s příslušnými operacemi ve $\mathbf{V}$. Skutečnost, že $\mathbf{U}$ je podprostorem $\mathbf{V}$ zapisujeme $\mathbf{U}\leq\mathbf{V}$.

Protože operace v podprostoru $\mathbf{U}$ jsou určené původními operacemi ve $\mathbf{V}$ nemusíme je uvádět a stačí říkat, že množina U tvoří podprostor prostoru $\mathbf{V}$. K tomu aby U byl podprostor $\mathbf{V}$, musí být U neprázdná množina uzavřená na operace sčítání a násobení skalárem. Naopak, pokud U splňuje tyto podmínky, pak U spolu s příslušnými operacemi tvoří podprostor.

Tvrzení 5.6. *Nechť* $\mathbf{V}$ *je vektorový prostor nad* $\mathbf{T}$*. Neprázdná podmnožina* U *množiny* V *je podprostorem* $\mathbf{V}$ *právě tehdy, když*

- *(„uzavřenost na sčítání“) pro libovolné* $\mathbf{u},\mathbf{v}\in U$ *platí* $\mathbf{u}+\mathbf{v}\in U$ *a*
- *(„uzavřenost na násobení skalárem“) pro libovolné* $\mathbf{v}\in U$ *a* $a\in T$ *platí* $a\mathbf{v}\in U$*.*

Důkaz. Pokud $U\leq\mathbf{V}$, pak U musí být zřejmě uzavřená na sčítání a násobení skalárem.

Předpokládejme, že U je neprázdná množina uzavřená na sčítání a násobení skalárem. Pak opačný vektor k $\mathbf{u}\in U$ je v U, protože $-\mathbf{u}$ lze napsat jako $(-1)\cdot\mathbf{u}$. Rovněž nulový vektor vektorového prostoru $\mathbf{V}$ je prvkem U, protože U je neprázdná a platí $0\cdot\mathbf{u}=\mathbf{o}$. Všechny axiomy nyní vyplývají z toho, že jsou splněny ve $\mathbf{V}$. □

Množina tvořená pouze prvkem $\mathbf{o}$ je vždy podprostorem, rovněž celý prostor $\mathbf{V}$ je podprostorem $\mathbf{V}$. Těmto podprostorům říkáme *triviální*, ostatní podprostory nazýváme *netriviální* nebo *vlastní*. Zdůrazněme pozorování z důkazu předchozího tvrzení — nulový vektor je obsažen v každém podprostoru.

5.2.1. *Podprostory* $\mathbb{R}^n$. Uvažujme podprostor $U\leq\mathbb{R}^2$. Pokud U obsahuje nenulový vektor $\mathbf{x}=(x_1,x_2)^T$, pak musí obsahovat všechny jeho násobky: $\{t\mathbf{x}:t\in\mathbb{R}\}\subseteq U$. Geometricky tvoří tyto násobky přímku procházející bodem $\mathbf{x}$ a počátkem. Pokud U obsahuje ještě jiný nenulový vektor $\mathbf{y}$, který neleží na přímce $\{t\mathbf{x}:t\in\mathbb{R}\}$, pak opět obsahuje všechny jeho násobky, a z toho již geometricky nahlédneme, že $U=\mathbb{R}^2$, protože každý vektor z $\mathbb{R}^2$ je součtem nějakého vektoru na přímce $\{t\mathbf{x}:t\in\mathbb{R}\}$ a nějakého vektoru na přímce $\{t\mathbf{y}:t\in\mathbb{R}\}$.

OBRAZEK

Formální důkaz tohoto tvrzení přenecháme jako cvičení, později budeme podobné věci umět dokazovat snadno a rychle pomocí pojmu báze.

Ukázali jsme, že kromě triviálních podprostorů $\{(0,0)^T\}$ a $\mathbb{R}^2$ jsou jedinými kandidáty na podprostory $\mathbb{R}^2$ množiny tvaru $\{t\mathbf{x}:t\in\mathbb{R}\}$. Snadno ověříme, že pro libovolný vektor $\mathbf{o}\neq\mathbf{x}\in\mathbb{R}^2$ je tato množina uzavřená na sčítání a násobení skalárem. Podprostory $\mathbb{R}^2$ jsou tedy $\{\mathbf{o}\}$, přímky procházející počátkem a celý prostor $\mathbb{R}^2$.

Podobnou úvahou nalezneme všechny podprostory $\mathbb{R}^3$. Pokud $\mathbf{o}\neq\mathbf{x}\in U$, pak U obsahuje celou přímku $\{t\mathbf{x}:t\in\mathbb{R}\}$. Pokud U obsahuje ještě jiný vektor $\mathbf{y}$, pak $\{t\mathbf{y}:t\in\mathbb{R}\}\subseteq U$ a pak obsahuje celou rovinu určenou $\mathbf{x},\mathbf{y}$ a počátkem, což je rovina

$$\{s\mathbf{x}+t\mathbf{y}:s,t\in\mathbb{R}\}\ .$$

Obsahuje-li U ještě nějaký jiný vektor, pak $U=\mathbb{R}^3$. Podprostory $\mathbb{R}^3$ jsou tedy triviální podprostory, přímky procházející počátkem a roviny procházející počátkem.

I když vizuální představa prostoru $\mathbb{R}^n$ pro $n>3$ chybí, intuice stále je, že podprostory jsou rovné útvary procházející počátkem.

5.2.2. *Podprostory* $\mathbf{T}^n$. Nad jinými tělesy již nemáme tak dobrou vizuální představu aritmetického prostoru, ale stále můžeme podobné úvahy jako výše provádět algebraicky. Tak například stále platí (viz cvičení), že podprostory $\mathbf{T}^2$ jsou triviální podprostory a „přímky“ procházející počátkem, tj. množiny tvaru $\{t\mathbf{x} : t \in T\}$, kde $\mathbf{o} \neq \mathbf{x} \in T^2$.

OBRAZEK primky v Z_5^2

S podprostory $\mathbb{R}^n$ jsme se již setkali při řešení homogenních soustav rovnic. Vlastnosti (p1), (p2) z věty 2.14 vlastně přesně říkají, že množina všech řešení homogenní soustavy rovnic nad $\mathbb{R}$ s maticí A typu $m \times n$ je podprostorem $\mathbb{R}^n$. Tento podprostor zobecníme na případ libovolného tělesa.

Definice 5.7. Nechť A je matice nad tělesem $\mathbf{T}$ typu $m \times n$. Pak množinu všech řešení homogenní soustavy rovnic s maticí A nazýváme *jádro matice* A a značíme $\operatorname{Ker} A$, tzn.

$$\operatorname{Ker} A = \{\mathbf{x} : A\mathbf{x} = \mathbf{o}\} \ .$$

Tvrzení 5.8. *Pro libovolnou matici A nad $\mathbf{T}$ typu $m \times n$ platí* $\operatorname{Ker} A \leq \mathbf{T}^n$.

Důkaz. Podle tvrzení 5.6 stačí ověřit, že množina $\operatorname{Ker} A$ je neprázdná a uzavřená na sčítání a násobení skalárem.

$\operatorname{Ker} A$ obsahuje nulový vektor, takže je neprázdná.

Pokud $\mathbf{u}, \mathbf{v} \in \operatorname{Ker} A$, pak podle definice $\operatorname{Ker} A$ je $A\mathbf{u} = \mathbf{o} = A\mathbf{v}$. Z distributivity násobení matic nyní dostaneme $A(\mathbf{u} + \mathbf{v}) = A\mathbf{u} + A\mathbf{v} = \mathbf{o} + \mathbf{o} = \mathbf{o}$, takže $\mathbf{u} + \mathbf{v} \in \operatorname{Ker} A$.

Pokud $\mathbf{u} \in \operatorname{Ker} A$ a $a \in T$, pak $A(a\mathbf{u}) = a(A\mathbf{u}) = a\mathbf{o} = \mathbf{o}$, tedy $a\mathbf{u} \in \operatorname{Ker} A$. □

Geometricky je $\operatorname{Ker} A$ vzorem nulového vektoru při zobrazení f_A. Vzor jiného vektoru (neboli množina řešení soustavy $A\mathbf{x} = \mathbf{b}$, kde $\mathbf{b} \neq \mathbf{o}$) podprostor netvoří, viz cvičení. Tato množina je sice rovný útvar, ale neprochází počátkem. Takovým množinám budeme později říkat afinní podprostory $\mathbf{T}^n$.

5.2.3. *Další příklady podprostorů.* Množina spojitých funkcí z $\mathbb{R}$ do $\mathbb{R}$ je podprostorem vektorového prostoru všech funkcí z $\mathbb{R}$ do $\mathbb{R}$, protože množina spojitých funkcí je uzavřená na operace sčítání a násobení reálným číslem. Podobně, prostor diferencovatelných funkcí z $\mathbb{R}$ do $\mathbb{R}$ je podprostorem prostoru spojitých funkcí. Množina reálných čísel je podprostorem prostoru komplexních čísel, kde obě tělesa chápeme jako vektorové prostory nad $\mathbb{Q}$.

5.2.4. *Lineární kombinace, podprostor generovaný množinou, množina generátorů.* Už několikrát jsme potkali množiny vektorů typu $t\mathbf{u} + s\mathbf{v} + \ldots$, kde $\mathbf{u}$, $\mathbf{v}$, ... jsou nějaké vektory. Naposledy při popisu podprostorů $\mathbb{R}^3$. Takovým výrazům se říká lineární kombinace vektorů $\mathbf{u}$, $\mathbf{v}$, ... Již jsme tento pojem definovali pro matice (tedy např. i pro aritmetické vektory) v definici 4.13.

Definice 5.9. Jsou-li $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ vektory z vektorového prostoru $\mathbf{V}$ nad $\mathbf{T}$ a $t_1, t_2, \ldots, t_k$ prvky $\mathbf{T}$, pak součet

$$t_1\mathbf{v}_1 + t_2\mathbf{v}_2 + \cdots + t_k\mathbf{v}_k$$

se nazývá *lineární kombinace vektorů* $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_k$. Skaláry $t_1, t_2, \ldots, t_k$ nazýváme *koeficienty lineární kombinace.*

Lineární kombinaci prázdného systému vektorů definujeme jako nulový vektor.

Zdůrazněme, že v lineární kombinaci máme vždy konečný počet vektorů.

Příklad 5.10. Lineární kombinaci vektorů $\mathbf{u}, \mathbf{v}$ s koeficienty 2,3, tj. vektor $2\mathbf{u}+3\mathbf{v}$, je vlastně „vektor o souřadnicích $(2, 3)$ vzhledem k soustavě souřadnic $\mathbf{u}, \mathbf{v}$“. Přesný význam dáme této větě později, ale smysl je snad zřejmý z obrázku.

OBRAZEK - linearni kombinace 2u+3v

Lineární kombinace se vyskytují v popisu podprostorů, například množina $\{t\mathbf{x} + s\mathbf{y} : s, t \in \mathbf{T}\}$ je množinou všech lineárních kombinací vektorů $\mathbf{x}, \mathbf{y}$. Obecně definujeme *lineární obal množiny* X jako množinu všech lineárních kombinací prvků X. Tato množina tvoří vždy podprostor.

Definice 5.11. Nechť $\mathbf{V}$ je vektorový prostor nad $\mathbf{T}$ a $X \subseteq V$. Pak *lineárním obalem množiny* X rozumíme množinu $\langle X \rangle$ všech lineárních kombinací prvků X, tj. množinu

$$\langle X \rangle = \{t_1\mathbf{v}_1 + t_2\mathbf{v}_2 + \cdots + t_k\mathbf{v}_k : k \in \mathbb{N}_0,\ \mathbf{v}_1, \ldots, \mathbf{v}_k \in X,\ t_1, \ldots, t_k \in T\}$$

Geometricky, lineární obal je „rovný útvar procházející počátkem“ obsahující dané vektory.

Příklad 5.12. $\langle \emptyset \rangle = \{\mathbf{o}\}$ – lineární obal prázdné množiny je triviální prostor tvořený nulovým vektorem.

Příklad 5.13. V prostoru $\mathbb{R}^3$ máme

$$\left\langle \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix}, \begin{pmatrix} 9 \\ 12 \\ 15 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} \right\rangle =$$
$$= \left\{ s \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + t \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} : s, t \in \mathbb{R} \right\} .$$

Inkluze $\subseteq$ v první rovnosti plyne z toho, že každou lineární kombinaci vektorů $(1,2,3)^T$, $(4,5,6)^T$, $(9,12,15)^T$ lze psát jako lineární kombinace vektorů $(1,2,3)^T$, $(4,5,6)^T$, protože vektor $(9,12,15)^T$ lze napsat jako lineární kombinaci prvních dvou vektorů:

$$t_1 \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + t_2 \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} + t_3 \begin{pmatrix} 9 \\ 12 \\ 15 \end{pmatrix} =$$
$$= t_1 \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + t_2 \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} + t_3 \left(\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + 2 \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} \right) =$$
$$= (t_1 + t_3) \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + (t_2 + 2t_3) \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} .$$

Geometricky, lineární obal daných tří vektorů je rovina procházející počátkem, třetí vektor leží v rovině určené prvními dvěma vektory.

V zápisech lineární kombinace množiny vektorů dané výčtem jako výše vynecháváme pro přehlednost závorky $\{,\}$ označující množinu. Někdy říkáme „lineární obal vektorů ...“, místo formálně přesného „lineární obal množiny vektorů $\{\dots\}$“.

Tvrzení 5.14. *Pro libovolný vektorový prostor* $\mathbf{V}$ *nad* $\mathbf{T}$ *a libovolnou* $X \subseteq V$ *je* $\langle X \rangle$ *podprostorem* $\mathbf{V}$.

Důkaz. Je třeba ověřit, že $\langle X \rangle$ je neprázdná množina uzavřená na sčítání a násobení libovolným $r \in T$.

Předně $\langle X \rangle$ je neprázdná, protože obsahuje lineární kombinaci prázdné množiny, tj. vektor $\mathbf{o}$.

Součet lineární kombinace vektorů $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k \in X$ s koeficienty $s_1, s_2, \dots, s_k \in T$ a lineární kombinace vektorů $\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_l \in X$ s koeficienty $t_1, t_2, \dots, t_l$ je lineární kombinace vektorů $\mathbf{v}_1, \dots, \mathbf{v}_k, \mathbf{w}_1, \dots, \mathbf{w}_l \in X$ s koeficienty $s_1, \dots, s_k, t_1, \dots, t_l$.

Konečně, r-násobkem lineární kombinace vektorů $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k \in X$ s koeficienty $s_1, s_2, \dots, s_k$ je lineární kombinace stejných vektorů s koeficienty $rs_1, rs_2, \dots, rs_k$. □

Obsahuje-li podprostor $U \leq \mathbf{V}$ množinu X, pak, díky uzavřenosti na sčítání a násobení skalárem, obsahuje i všechny lineární kombinace prvků X. To znamená, že $\langle X \rangle$ je „nejmenší“ podprostor, který obsahuje X. (Slovo nejmenší je zde třeba chápat vzhledem k inkluzi, tj. tak, že jakýkoliv podprostor obsahující X obsahuje $\langle X \rangle$.) Proto se rovněž hovoří o podprostoru generovaném X.

Definice 5.15. Nechť $\mathbf{V}$ je vektorový prostor nad $\mathbf{T}$ a $X \subseteq V$. Pokud $\langle X \rangle = V$, pak říkáme, že X je *množina generátorů prostoru* $\mathbf{V}$, nebo říkáme, že X *generuje* $\mathbf{V}$.

Jinými slovy, množina $X \subseteq V$ generuje $\mathbf{V}$, pokud každý vektor ve V lze zapsat jako lineární kombinaci vektorů z X.

Příklad 5.16. Prázdná množina generuje triviální prostor $\{\mathbf{o}\}$.

Množina $\{(1,0)^T, (0,1)^T\}$ generuje pro libovolné $\mathbf{T}$ prostor $\mathbf{T}^2$, protože každý vektor $(x_1, x_2)^T$ v T^2 lze napsat jako lineární kombinaci vektorů $(1,0)^T$ a $(0,1)^T$ takto:

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = x_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} .$$

Tedy také libovolná množina obsahující vektory $(1,0)^T$ a $(0,1)^T$ je množinou generátorů $\mathbf{T}$.

Množina $\{(1,2,3)^T\}$ generuje podprostor $\mathbf{V} = \langle (1,2,3)^T \rangle$ vektorového prostoru $\mathbb{R}^3$. Jiné množiny generátorů stejného prostoru $\mathbf{V}$ jsou například $\{(2,4,6)^T\}$, $\{(2,4,6)^T, (3,6,9)^T\}$, V. Množina $\{(1,2,3)^T, (4,5,6)^T\}$ není množinou generátorů $\mathbf{V}$, protože není ani jeho podmnožinou.

Množina $\{1, x, x^2\}$ je množinu generátorů prostoru všech reálných polynomů stupně nejvýše 2.

Příklad 5.17. V části 5.2.1 jsme si geometricky zdůvodnili, že pro každý netriviální podprostor $\mathbb{R}^3$ existuje množina generátorů, která má jeden, nebo dva prvky.

Příklad 5.18. Definujeme $\mathbb{R}^\omega$ jako prostor všech posloupností reálných čísel s operacemi prováděnými po složkách, podobně jako s aritmetickými vektory. Množina

$$X = \{(1,0,0,\dots),(0,1,0,0,\dots),(0,0,1,0,\dots),\dots\}$$

negeneruje prostor $\mathbb{R}^\omega$. Jako cvičení zjistěte lineární obal této množiny.

Zajímavým podprostorem $\mathbb{R}^\omega$ je například množina Y všech posloupností $(a_1, a_2, \dots)$ splňujících $a_n = a_{n-1} + a_{n-2}$ pro každé $n \geq 3$. Mezi prvky tohoto podprostoru patří Fibonacciho posloupnost.

5.2.5. *Sloupcový a řádkový prostor matice.* Ke každé matici máme přirozeně přiřazeny dvě skupiny aritmetických vektorů, řádkové a sloupcové. Prostorům, které generují, říkáme řádkový a sloupcový prostor.

Definice 5.19. Nechť A je matice nad $\mathbf{T}$ typu $m \times n$. *Sloupcovým prostorem matice* A rozumíme podprostor $\mathbf{T}^m$ generovaný sloupci matice a značíme jej $\operatorname{Im} A$.

$$\operatorname{Im} A = \langle A_{*1}, A_{*2}, \dots, A_{*n}\rangle \leq \mathbf{T}^m$$

Řádkovým prostorem matice A rozumíme sloupcový prostor matice A^T, tj.

$$\operatorname{Im} A^T = \langle A^T_{1*}, A^T_{2*}, \dots, A^T_{m*}\rangle \leq \mathbf{T}^n$$

Příklad 5.20. Pro reálnou matici

$$A = \begin{pmatrix} 1 & 3 & 4 \\ 2 & 7 & -1 \end{pmatrix}$$

je

$$\operatorname{Im} A = \left\langle \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 7 \end{pmatrix}, \begin{pmatrix} 4 \\ -1 \end{pmatrix} \right\rangle$$

$$\operatorname{Im} A^T = \left\langle \begin{pmatrix} 1 \\ 3 \\ 4 \end{pmatrix}, \begin{pmatrix} 2 \\ 7 \\ -1 \end{pmatrix} \right\rangle \ .$$

Jak poznáme, že vektor $\mathbf{b} \in T^m$ leží v $\operatorname{Im} A$? Stačí si připomenout, že $A\mathbf{x}$ je lineární kombinace sloupců matice A, kde koeficienty jsou složky vektoru $\mathbf{x}$. Takže $\mathbf{b} \in \operatorname{Im} A$ právě když rovnice $A\mathbf{x} = \mathbf{b}$ má řešení, přičemž koeficienty lineární kombinace jsou složky libovolného řešení. Také vidíme, že $\operatorname{Im} A$ je obraz (obor hodnot) zobrazení f_A, což ospravedlňuje zavedené značení $\operatorname{Im} A$:

$$\operatorname{Im} A = \{A\mathbf{x} : \mathbf{x} \in T^n\} = \{f_A(\mathbf{x}) : \mathbf{x} \in T^n\} = f_A(T^n) \ .$$

Příklad 5.21. Pro matici A z předchozího příkladu zjistíme, zda $(0,1)^T \in \operatorname{Im} A$ a $(1,0)^T \in \operatorname{Im} A$. Protože máme dvě soustavy rovnic se stejnou maticí, můžeme je řešit najednou.

$$\left(\begin{array}{ccc|cc} 1 & 3 & 4 & 1 & 0 \\ 2 & 7 & -1 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|cc} 1 & 3 & 4 & 1 & 0 \\ 0 & 1 & -9 & -2 & 1 \end{array}\right)$$

Pro pravou stranu $(1,0)^T$ dostaneme volbou 0 za volnou proměnnou řešení $\mathbf{x} = (7,-2,0)^T$, což dává vyjádření

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = 7\begin{pmatrix} 1 \\ 2 \end{pmatrix} - 2\begin{pmatrix} 3 \\ 7 \end{pmatrix} + 0\begin{pmatrix} 4 \\ -1 \end{pmatrix} \ .$$

Koeficienty nejsou určeny jednoznačně, například volbou 2 za volnou proměnnou dostaneme $\mathbf{x} = (-55,16,2)^T$, což odpovídá vyjádření

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = -55\begin{pmatrix} 1 \\ 2 \end{pmatrix} + 16\begin{pmatrix} 3 \\ 7 \end{pmatrix} + 2\begin{pmatrix} 4 \\ -1 \end{pmatrix} \ .$$

Pro vektor $(0,1)^T$ dostaneme například vyjádření

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = -3\begin{pmatrix} 1 \\ 2 \end{pmatrix} + 1\begin{pmatrix} 3 \\ 7 \end{pmatrix} + 0\begin{pmatrix} 4 \\ -1 \end{pmatrix} \ .$$

Tím jsme ukázali, že oba vektory $(1,0)^T, (0,1)^T$ patří do $\operatorname{Im} A$, tím pádem $\operatorname{Im} A = \mathbb{R}^2$, protože z příkladu 5.16 víme, že $\langle (1,0)^T, (0,1)^T\rangle = \mathbb{R}^2$.

Leží vektor $(2,1,1)^T$ v prostoru $\operatorname{Im} A^T$?

$$\left(\begin{array}{cc|c} 1 & 2 & 2 \\ 3 & 7 & 1 \\ 4 & -1 & 1 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 2 & 2 \\ 0 & 1 & -5 \\ 0 & -9 & -7 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 2 & 2 \\ 0 & 1 & -5 \\ 0 & 0 & -52 \end{array}\right)$$

Soustava nemá řešení, takže vektor $(2,1,1)^T$ v $\operatorname{Im} A^T$ neleží.

5.2.6. *Prostory přidružené k matici a elementární úpravy.* Důležitým pozorováním je, že řádkové elementární úpravy nemění lineární obal řádků (tj. prostor $\operatorname{Im} A^T$). Obecněji, násobení zleva regulární maticí nemění $\operatorname{Im} A^T$ a násobení zprava nemění $\operatorname{Im} A$. Násobení zleva obecně mění $\operatorname{Im} A$ tak, že sloupcový prostor vzniklé matice je lineární obal R-násobků původních sloupců.

Dalším prostorem přidruženým k matici A je $\operatorname{Ker} A$. Ten se řádkovými úpravami (nebo násobením zleva regulární maticí) rovněž nemění. To již vlastně víme: $\operatorname{Ker} A$ je množina řešení soustavy $A\mathbf{x} = \mathbf{o}$, ta se nemění provedením elementární úpravy. Maticově, $\operatorname{Ker}(EA) = \operatorname{Ker} A$ pro každou elementární matici E. Protože však každá regulární matice R je součinem elementárních matic, máme $\operatorname{Ker}(RA) = \operatorname{Ker} A$. V důkazu následujícího tvrzení zvolíme rychlejší postup.

Tvrzení 5.22. *Nechť A je matice nad $\mathbf{T}$ typu $m \times n$ a R je regulární matice řádu m. Pak*

$$\operatorname{Ker} A = \operatorname{Ker}(RA), \quad \operatorname{Im} A^T = \operatorname{Im}(RA)^T \ , \quad \operatorname{Im}(RA) = \langle RA_{*1}, RA_{*2}, \dots, RA_{*n} \rangle .$$

Důkaz. Třetí část je důsledkem vztahu $(RA)_{*i} = RA_{*i}$ z tvrzení o násobení matic vnímaném jako tvoření lineárních kombinací (tvrzení 4.14).

Je-li $\mathbf{x} \in \operatorname{Ker} A$, pak $A\mathbf{x} = \mathbf{o}$. Vynásobením R zleva získáme $RA\mathbf{x} = R\mathbf{o} = \mathbf{o}$, čili $\mathbf{x} \in \operatorname{Ker}(RA)$. Naopak, je-li $\mathbf{x} \in \operatorname{Ker}(RA)$, pak $RA\mathbf{x} = \mathbf{o}$. Protože R je regulární, máme $A\mathbf{x} = \mathbf{o}$ (použijeme například bod (4) charakterizace regulárních matic z věty 4.30), ekvivalentně $\mathbf{x} \in \operatorname{Ker} A$.

K důkazu druhé rovnosti si opět uvědomíme, že násobení matice A zleva maticí R odpovídá provádění lineárních kombinací na řádky matice A. Proto každý řádek matice RA je lineární kombinací řádků matice A, takže $\operatorname{Im}(RA)^T \subseteq \operatorname{Im} A^T$. Stejnou úvahou, kde místo A uvažujeme matici RA a místo R uvažujeme R^{-1} získáme $\operatorname{Im}(R^{-1}RA)^T \subseteq \operatorname{Im}(RA)^T$, což je po úpravě druhá inkluze. □

Pro sloupcové úpravy máme obdobně například $\operatorname{Im} A = \operatorname{Im}(AR)$, pokud R je regulární matice řádu n. Důkaz můžeme provést buď užitím sloupcových úprav místo řádkových, nebo přechodem k transponované matici: Použitím předchozí věty pro A^T místo A a R^T místo R dostaneme $\operatorname{Im}(A^T)^T = \operatorname{Im}(R^T A^T)^T$, což je po úpravě dokazovaný vztah.

Důsledek 5.23. *Elementární řádkové úpravy nemění* $\operatorname{Ker} A$ *a* $\operatorname{Im} A^T$. *Elementární sloupcové úpravy nemění* $\operatorname{Ker} A^T$ *a* $\operatorname{Im} A$.

5.3. Lineární závislost a nezávislost.

5.3.1. *Definice.* Množina aritmetických vektorů $(1,2,3)^T$, $(4,5,6)^T$, $(9,12,15)^T$ generuje ten samý podprostor $\mathbf{V} \leq \mathbb{R}^3$ jako množina $(1,2,3)^T$, $(4,5,6)^T$, jak jsme viděli v příkladu 5.13. Důvod je ten, že třetí vektor lze napsat jako lineární kombinaci prvních dvou vektorů. Množinám vektorů, ve které žádné takové lineární závislosti nelze najít říkáme *lineárně nezávislé*. Z technických důvodů definujeme lineární (ne)závislost pro posloupnosti vektorů, nikoliv množiny.

Definice 5.24. Nechť $\mathbf{V}$ je vektorový prostor. Posloupnost vektorů $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k)$ ve $\mathbf{V}$ se nazývá *lineárně závislá*, pokud některý z vektorů $\mathbf{v}_i$ je lineární kombinací ostatních vektorů $\mathbf{v}_1$, $\mathbf{v}_2$, …, $\mathbf{v}_{i-1}$, $\mathbf{v}_{i+1}$, …, $\mathbf{v}_k$.

V opačném případě říkáme, že posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k)$ je *lineárně nezávislá*.

(Lineární (ne)závislost definujeme i pro nekonečné skupiny vektorů, to ale necháme do samostatného oddílu.)

Užitím pojmu lineárního obalu můžeme definici přeformulovat tak, že posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k)$ je lineárně závislá, pokud existuje $i \in \{1, 2, \dots, k\}$ tak, že

$$\mathbf{v}_i \in \langle \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_{i-1}, \mathbf{v}_{i+1}, \dots, \mathbf{v}_k \rangle \ ,$$

ekvivalentně

$$\langle \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k \rangle = \langle \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_{i-1}, \mathbf{v}_{i+1}, \dots, \mathbf{v}_k \rangle \ .$$

Geometricky to znamená, že $\mathbf{v}_i$ leží v „rovném útvaru“ určeném zbylými vektory.

Naopak, posloupnost je lineárně nezávislá, když žádné takové i neexistuje, jinými slovy, když každý vektor $\mathbf{v}_i$ „něco přidá“ k lineárnímu obalu zbylých vektorů.

Často budeme hovořit poněkud nepřesně a říkat, že vektory … jsou lineárně nezávislé, apod.

Příklad 5.25. Posloupnost $((1,2,3)^T, (9,12,15)^T, (4,5,6)^T)$ ve vektorovém prostoru $\mathbb{R}^3$ je lineárně závislá, protože druhý vektor lze napsat jako lineární kombinaci zbylých dvou:

$$\begin{pmatrix} 9 \\ 12 \\ 15 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + 2 \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} .$$

Geometricky to znamená, že vektor $(9,12,15)^T$ leží v rovině určené zbylými dvěma vektory.

Posloupnost vektorů $(1,0,0,0)^T$, $(0,1,0,0)^T$, $(0,0,1,0)^T$, $(0,0,0,1)^T$ v prostoru $\mathbb{Z}_3^4$ je lineárně nezávislá, protože, žádný z vektorů není lineární kombinací ostatních: lineární obal druhého až čtvrtého vektoru je množina $\{(0,a,b,c)^T : a,b,c \in \mathbb{Z}_3^4\}$, do níž vektor $(1,0,0,0)^T$ nepatří. Podobně pro ostatní vektory.

Posloupnost vektorů $(\cos x \sin x + 5, 1, \sin(2x)+3)$ v prostoru reálných funkcí reálné proměnné (nad $\mathbb{R}$) je lineárně závislá, protože $\sin(2x)+3$ lze napsat jako $2\cdot(\cos x \sin x + 5) + (-7)\cdot 1$.

Několik snadných obecných pozorování:

- Kdykoliv posloupnost obsahuje nulový vektor, je lineárně závislá, protože nulový vektor je lineární kombinací prázdné skupiny vektorů.
- Jednočlenná posloupnost $(\mathbf{v})$ je lineárně nezávislá právě tehdy, když $\mathbf{v} \neq \mathbf{o}$.
- Kdykoliv posloupnost obsahuje dva stejné vektory, je lineárně závislá. Obecněji, pokud je některý z vektorů násobkem jiného, je posloupnost lineárně závislá. **Neplatí to ale naopak**. V posloupnosti $((1,2,3)^T$, $(9,12,15)^T$, $(4,5,6)^T)$ z předchozího příkladu není žádný z vektorů násobkem jiného, přesto je posloupnost lineárně závislá.
- Lineární závislost nebo nezávislost posloupnosti nezávisí na pořadí prvků.
- Podposloupnost lineárně nezávislé posloupnosti je lineárně nezávislá. Jinak řešeno, pokud je podposloupnost lineárně závislá, je lineárně závislá i původní posloupnost.

Pokud bychom ověřovali, že nějaká posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$ je lineárně nezávislá, z definice, museli bychom pro každý z vektorů $\mathbf{v}_1, \ldots, \mathbf{v}_k$ ukázat, že nelze vyjádřit jako lineární kombinace ostatních. Snazší je použít bod (2) z následujícího snadného pozorování, které dává elegantnější charakterizaci lineární nezávislosti.

Tvrzení 5.26. *Nechť $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ je posloupnost vektorů ve vektorovém prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$. Následující tvrzení jsou ekvivalentní.*

(1) *Posloupnost $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ je lineárně nezávislá.*

(2) *Vektor $\mathbf{o}$ lze vyjádřit jako lineární kombinaci vektorů $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ pouze triviálním způsobem $\mathbf{o} = 0\mathbf{v}_1 + 0\mathbf{v}_2 + \cdots + 0\mathbf{v}_k$.*

Jinými slovy, pro libovolné $a_1, a_2, \ldots, a_k \in T$ platí, že když

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k = \mathbf{o} \ ,$$

pak $a_1 = a_2 = \cdots = a_k = 0$.

(3) *Každý vektor $\mathbf{b} \in V$ lze vyjádřit jako lineární kombinaci vektorů $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_k$ nejvýše jedním způsobem.*

Důkaz. (1) $\Rightarrow$ (2). Pokud platí

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k = \mathbf{o}$$

a jedno z čísel $a_1, a_2, \ldots, a_k$, řekněme a_i, je nenulové, pak můžeme upravit

$$a_i\mathbf{v}_i = -a_2\mathbf{v}_2 - \ldots - a_k\mathbf{v}_k$$

a

$$\mathbf{v}_i = -a_1^{-1}a_2\mathbf{v}_2 - \ldots - a_1^{-1}a_k\mathbf{v}_k \ ,$$

z čehož vidíme, že posloupnost je lineárně závislá.

(2) $\Rightarrow$ (3). Pokud máme dvě vyjádření vektoru $\mathbf{u}$

$$\mathbf{u} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k = b_1\mathbf{v}_1 + b_2\mathbf{v}_2 + \cdots + b_k\mathbf{v}_k \ ,$$

pak úpravou získáme rovnost

$$\mathbf{o} = (a_1 - b_1)\mathbf{v}_1 + (a_2 - b_2)\mathbf{v}_2 + \cdots + (a_k - b_k)\mathbf{v}_k,$$

takže z (2) dostáváme, že $a_i - b_i = 0$ pro každé i, neboli $a_i = b_i$ a tedy vyjádření vektoru $\mathbf{u}$ jsou stejná.

(3) $\Rightarrow$ (2) je triviální.

(2) $\Rightarrow$ (1). Pokud je posloupnost $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ lineárně závislá, pak pro nějaké i je vektor $\mathbf{v}_i$ lineární kombinací ostatních, tedy

$$\mathbf{v}_i = b_1\mathbf{v}_1 + b_2\mathbf{v}_2 + \cdots + b_{i-1}\mathbf{v}_{i-1} + b_{i+1}\mathbf{v}_{i+1} + \cdots + b_k\mathbf{v}_k \ .$$

Pak můžeme psát

$$\mathbf{o} = b_1\mathbf{v}_1 + b_2\mathbf{v}_2 + \cdots + b_{i-1}\mathbf{v}_{i-1} + (-1)\mathbf{v}_i + b_{i+1}\mathbf{v}_{i+1} + \cdots + b_k\mathbf{v}_k \ ,$$

takže dostáváme netriviální kombinaci, která dává nulový vektor s koeficienty $a_i = -1$ a $a_j = b_j$ pro $j \neq i$. □

Bod (2) lze formulovat tak, že posloupnost je lineárně závislá právě tehdy, když existuje její *netriviální* lineární kombinace, která dá nulový vektor. Netriviální znamená, že alespoň jeden koeficient je nenulový. Ještě jedna ekvivalentní formulace je ve cvičeních: Posloupnost vektorů $(\mathbf{v}_1, \dots, \mathbf{v}_k)$ lineárně nezávislá právě tehdy, když žádný z vektorů není v lineárním obalu předchozích (tj. pro každé i platí $\mathbf{v}_i \notin \langle \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_{i-1} \rangle$).

Připomeňme, že vektory $\mathbf{v}_1, \dots, \mathbf{v}_k$ generují $\mathbf{V}$, pokud se každý vektor dá napsat jako lineární kombinace těchto vektorů alespoň jedním způsobem. Bod (3) ukazuje, že lineární nezávislost je jakýmsi opakem.

Příklad 5.27. Zjistíme, zda je posloupnost vektorů

$$((1,1,1,1)^T, (1,2,1,1)^T, (0,1,0,1)^T)$$

v prostoru $\mathbb{Z}_3^4$ lineárně nezávislá. Pokusíme se vyjádřit nulový vektor jako lineární kombinaci vektorů z dané posloupnosti

$$x_1 \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} + x_2 \begin{pmatrix} 1 \\ 2 \\ 1 \\ 1 \end{pmatrix} + x_3 \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} .$$

To je vlastně homogenní soustava rovnic!

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 2 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Soustavu převedeme do odstupňovaného tvaru. Pravé strany psát nebudeme, protože je soustava homogenní.

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

Nemáme žádnou volnou proměnnou, takže soustava má pouze triviální řešení $\mathbf{x} = (0,0,0)^T$. Jediná lineární kombinace daných vektorů, která dává nulový vektor je triviální, takže posloupnost je podle předchozího tvrzení lineárně nezávislá.

Tento příklad nám dává návod, jak zjistit, zda daná posloupnost aritmetických vektorů je lineárně (ne)závislá. Formulujeme učiněné pozorování jako tvrzení.

Tvrzení 5.28. *Sloupce matice A typu $m \times n$ nad $\mathbf{T}$ tvoří lineárně nezávislou posloupnost v $\mathbf{T}^m$ právě tehdy, když* $\operatorname{Ker} A = \{\mathbf{o}\}$*, tj. rovnice $A\mathbf{x} = \mathbf{o}$ má jen triviální řešení $\mathbf{x} = \mathbf{o}$.*

Důkaz. Podle stále používaného tvrzení o vnímaní násobení matic jako lineárního kombinování máme $A\mathbf{x} = x_1 A_{*1} + x_2 A_{*2} + \cdots + x_n A_{*n}$, kde $\mathbf{x} = (x_1, x_2, \dots, x_m)$. Tvrzení nyní okamžitě plyne z charakterizace v tvrzení 5.26. □

Příklad 5.29. Posloupnost $(3i+5, 2, 3), (5, 2+i, 1), (4, 2, 12), (\pi, e^\pi, 4)$ v prostoru $\mathbb{C}^3$ je lineárně závislá.

Můžeme argumentovat užitím předchozího tvrzení. Dané aritmetické vektory si napíšeme do sloupců matice A typu 3×4. Při řešení soustavy $A\mathbf{x} = \mathbf{o}$ máme díky typu alespoň jednu volnou proměnnou (protože proměnné jsou 4 a pivotů může být nejvíce tolik, kolik řádků, tedy 3). Z toho plyne, že soustava má netriviální řešení (stačí za volnou proměnnou dosadit například 1 a dopočítat zpětnou substitucí).

Později budeme moci argumentovat obecnějším tvrzením.

Na tomto místě si znovu uvědomme, že aritmetické prostory tvoří jen jeden z mnoha příkladů vektorových prostorů. (I když jsme v úvodu tvrdili, že jsou „v podstatě jediné“. Uvozovky jsou zde podstatné, na přesný význam si musíme ještě chvíli počkat.) Častá chybná odpověď studentů na otázku, jak určit, zda jsou dané vektory lineárně závislé, je typu „Napíšeme si je do sloupců, vyeliminujeme a zjistíme, zda existují volné proměnné“. Odpověď je správná jen v aritmetických vektorových prostorech, obecně nedává žádný smysl: Jak napsat do sloupců vektory $\cos(2x), \sin x + e^x, \dots$ z vektorového prostoru spojitých funkcí?

Příklad 5.30. Posloupnost $(1, \sqrt{2})$ je lineárně nezávislá v $\mathbb{R}$ jako vektorovém prostoru nad $\mathbb{Q}$, protože $\sqrt{2}$ je iracionální. Stejná posloupnost je lineárně závislá v $\mathbb{R}$ jako vektorovém prostoru nad $\mathbb{R}$, protože např. $\sqrt{2}$ je $\sqrt{2}$-násobkem vektoru 1.

5.3.2. *Odstupňovaný tvar a elementární úpravy.* Jinou možností jak zjistit, zda jsou dané aritmetické vektory lineárně (ne)závislé je napsat je do řádků matice a elementárními řádkovými úpravami převádět matici do odstupňovaného tvaru. Tyto úpravy totiž nemění lineární (ne)závislost řádků a z odstupňovaného tvaru matice poznáme (ne)závislost řádků snadno. Výhodou také je, že řádkové úpravy nemění ani lineární obal řádků, což se nám bude později hodit při hledání báze.

Rovnou si také všimneme, že řádkové úpravy nemění ani lineární (ne)závislost sloupců. Tvrzení nejprve formulujeme pro sloupce. Řádkovou verzi dostaneme transponováním.

Tvrzení 5.31. *Nechť A je matice nad $\mathbf{T}$ typu $m \times n$, R je regulární matice řádu m a Q je regulární matice řádu n. Pak platí:*

(1) *Sloupce matice A jsou lineárně nezávislé právě tehdy, když jsou lineárně nezávislé sloupce matice AQ*
(2) *Sloupce matice A jsou lineárně nezávislé právě tehdy, když jsou lineárně nezávislé sloupce matice RA.*

Důkaz. Použijeme pozorování formulované jako tvrzení 5.28, totiž, že sloupce matice B jsou lineárně nezávislé, právě tehdy, když $B\mathbf{x} = \mathbf{o}$ má pouze triviální řešení.

Předpokládejme, že sloupce matice A jsou lineárně nezávislé a že $\mathbf{x}$ je řešením $AQ\mathbf{x} = \mathbf{o}$. Pak $Q\mathbf{x} = \mathbf{o}$, protože sloupce A jsou lineárně nezávislé. Z toho plyne, že $\mathbf{x} = \mathbf{o}$ (použijeme například bod (4) charakterizace regulárních matic z věty 4.30, nebo bod (7) a vynásobíme rovnost zleva Q^{-1}). Ukázali jsme, že soustava $AQ\mathbf{x} = \mathbf{o}$ má pouze triviální řešení, takže AQ má lineárně nezávislé sloupce.

Opačná implikace se dá dokázat užitím první implikace na matici AQ místo A a Q^{-1} místo Q.

Druhou ekvivalenci jsme již vlastně dokázali v tvrzení 5.22, protože $\operatorname{Ker}(RA) = \operatorname{Ker} A$, takže A má netriviální řešení právě tehdy, když má RA netriviální řešení. □

Ekvivalence v bodu (2) jde zesílit. Matice A má stejné lineární závislosti mezi sloupci jako matice RA. Například pokud $2A_{*1} + 3A_{*2} - 4A_{*3} = \mathbf{o}$, pak $2(RA)_{*1} + 3(RA)_{*2} - 4(RA)_{*3} = \mathbf{o}$, a naopak. Slovy, součet 2-násobku prvního sloupce, 3-násobku druhého sloupce a (-4)-násobku třetího sloupce je nulový vektor v matici A právě tehdy, když stejný vztah platí pro sloupce matice RA.

Důsledek 5.32. *Sloupcové úpravy nemění lineární (ne)závislost sloupců ani řádků matice. Řádkové úpravy nemění lineární (ne)závislost sloupců ani řádků matice.*

Důkaz. Z předchozího tvrzení použitého na elementární matice plyne, že řádkové ani sloupcové úpravy nemění lineární obal sloupců. K důkazu řádkových verzí použijeme stejné tvrzení pro transponovanou matici. □

Zbývá nahlédnout, kdy má řádkově odstupňovaný tvar lineárně nezávislé řádky. (Z předchozího tvrzení a tvrzení 5.28 vidíme, kdy má matice v odstupňovaném tvaru lineárně nezávislé sloupce: právě tehdy, když příslušná homogenní soustava nemá žádné volné proměnné, viz cvičení.) Je zřejmé, že je-li v matici nulový řádek, pak jsou řádky lineárně závislé. V opačném případě jsou již lineárně nezávislé.

Tvrzení 5.33. *Řádky matice v odstupňovaném tvaru jsou lineárně nezávislé právě tehdy, když matice neobsahuje nulový řádek.*

Důkaz. Implikace zleva doprava je zřejmá.

Předpokládejme, že matice A typu $m \times n$ bez nulového řádku je v odstupňovaném tvaru a vezmeme $r, k_1, \ldots, k_r$ z definice odstupňovaného tvaru. Protože A nemá nulový řádek je $r = n$. Chceme ukázat, že rovnice $A^T\mathbf{x} = \mathbf{o}$ má pouze triviální řešení (viz opět tvrzení 5.28). To je však snadné, protože již rovnice s pořadovými čísly k_1, k_2, …, k_n určují dolní trojúhelníkovou matici s nenulovými prvky na diagonále a ta má pouze triviální řešení.

OBRAZEK □

Myšlenku důkazu můžeme zobecnit na užitečné pozorování. Máme-li posloupnost vektorů v $\mathbf{T}^n$ takovou, že již vybraných m souřadnic tvoří lineárně nezávislou množinu v $\mathbf{T}^m$, pak je původní posloupnost lineárně nezávislá.

Příklad 5.34. Posloupnost

$$((1, 37, 3, 45, 1)^T, (0, -e, 1, \pi^e, 4)^T, (0, -12, 0, 33, 2)^T)$$

v prostoru $\mathbb{R}^5$ je lineárně nezávislá, protože první, třetí a páté složky vektorů tvoří posloupnost

$$((1, 3, 1)^T, (0, 1, 4)^T, (0, 0, 2)^T),$$

v $\mathbb{R}^3$, která je lineárně nezávislá podle předchozího tvrzení.

Příklad 5.35. Podíváme se znovu na příklad 5.27, tam jsme zjišťovali, zda je posloupnost

$$((1,1,1,1)^T, (1,2,1,1)^T, (0,1,0,1)^T)$$

v prostoru $\mathbb{Z}_3^4$ lineárně nezávislá. Tentokrát si vektory napíšeme do řádků a převedeme řádkovými úpravami do odstupňovaného tvaru.

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

Původní posloupnost je podle důsledku 5.32 lineárně nezávislá právě tehdy, když jsou řádky vzniklé matice B lineárně nezávislé. Matice B je v odstupňovaném tvaru bez nulového řádku, takže podle předchozího tvrzení jsou řádky B lineárně nezávislé. Původní posloupnost je tedy lineárně nezávislá.

Příklad 5.36. Zjistíme, zda je posloupnost vektorů

$$((1,1,1,0)^T, (0,1,0,1)^T, (1,0,1,1)^T)$$

v prostoru $\mathbb{Z}_2^4$ lineárně nezávislá. Napíšeme si vektory do řádků a upravujeme řádkovými úpravami.

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

V úpravách už nemusíme pokračovat, protože vidíme, že řádky vzniklé matice, tedy i původní matice, jsou lineárně závislé.

Shrneme poznatky o invariantech řádkových úprav. Řádkové úpravy nemění lineární závislost řádků ani sloupců, lineární obal řádků (to je $\operatorname{Im} A^T$) a $\operatorname{Ker} A$. Obecně mění lineární obal sloupců a $\operatorname{Ker} A^T$.

5.4. **Báze.**

5.4.1. *Definice.* Dostali jsme se ke stěžejnímu pojmu *báze* vektorového prostoru. Jako u lineární nezávislosti zadefinujeme konečnou verzi a obecnou definici odložíme na později.

Definice 5.37. Posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$ ve vektorovém prostoru $\mathbf{V}$ nad $\mathbf{T}$ se nazývá *báze*, pokud je lineárně nezávislá a generuje $\mathbf{V}$.

(Tím, že posloupnost $(\mathbf{v}_1, \dots, \mathbf{v}_n)$ generuje $\mathbf{V}$ přirozeně myslíme to, že množina $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ generuje $\mathbf{V}$.)

Intuice je taková, že báze je „dost malá“, ve smyslu, že mezi vektory nejsou žádné lineární závislosti, a zároveň dost velká, ve smyslu, že vektory generují celý prostor.

Daná posloupnost vektorů $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$ generuje prostor $\mathbf{V}$ právě tehdy, když lze každý vektor zapsat jako jejich lineární kombinace alespoň jedním způsobem. Podle tvrzení 5.26 je posloupnost lineárně nezávislá právě tehdy, když lze každý vektor vyjádřit jako lineární kombinace $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n$ nejvýše jedním způsobem. Dohromady dostáváme následující důležité pozorování.

Pozorování 5.38. *Posloupnost vektorů $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$ tvoří bázi vektorového prostoru $\mathbf{V}$ právě tehdy, když lze každý vektor $\mathbf{b} \in V$ vyjádřit právě jedním způsobem jako lineární kombinace vektorů $\mathbf{v}_1$, $\mathbf{v}_2$, …, $\mathbf{v}_n$.*

Příklad 5.39. Sloupce jednotkové matice I_n nad tělesem $\mathbf{T}$, tj. n-tice vektorů $((1,0,0,\dots,0)^T, (0,1,0,\dots,0)^T, \dots, (0,0,\dots,0,1)^T$ je bází aritmetického vektorového prostoru $\mathbf{T}^n$.

Tato posloupnost je totiž lineárně nezávislá, například podle tvrzení 5.33, a generuje $\mathbf{T}^n$, protože každý vektor $(x_1, \dots, x_n)^T$ jde vyjádřit jako lineární kombinaci

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = x_1 \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \cdots + x_n \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} .$$

Obě podmínky (lineární nezávislost i generování) jde najednou nahlédnout z toho, že každý vektor lze jednoznačně vyjádřit jako lineární kombinaci uvedenou výše.

Báze z příkladu jsou význačné báze aritmetických prostorů, proto mají svoje pojmenování a značení.

Definice 5.40. *Kanonická báze* (též *standardní báze*) v aritmetickém prostoru $\mathbf{T}^n$ je posloupnost

$$(\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n) = \left(\begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \right) .$$

Příklad 5.41. Posloupnost $((1,1)^T, (3,2)^T)$ je bází prostoru $\mathbb{R}^2$. Můžeme argumentovat tak, že matice

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

je regulární, takže podle charakterizační věty regulárních matic má rovnice $A\mathbf{x} = \mathbf{b}$ právě jedno řešení pro každé $\mathbf{b}$. To znamená, že každý vektor $\mathbf{b} \in \mathbb{R}^2$ lze vyjádřit jako lineární kombinaci sloupců matice A právě jedním způsobem, což nastane podle pozorování právě tehdy, když tvoří sloupce bázi.

Obecněji lze z charakterizační věty pro regulární matice nahlédnout, že sloupce (nebo řádky) čtvercové matice řádu n tvoří bázi $\mathbf{T}^n$ právě tehdy, když A je regulární (viz cvičení). Tedy například sloupce (řádky) horní trojúhelníkové matice s nenulovými prvky na diagonále tvoří bázi.

Příklad 5.42. Jednočlenná posloupnost $((3,3,3)^T)$ je báze prostoru $\langle (1,1,1)^T \rangle \leq \mathbb{R}^3$.

Posloupnost $(1, x, x^2)$ je báze prostoru reálných polynomů stupně nejvýše 2, protože každý polynom lze napsat právě jedním způsobem ve tvaru $a \cdot 1 + b \cdot x + c \cdot x^2$.

Prázdná posloupnost je bází triviálního prostoru $\{\mathbf{o}\}$.

Posloupnost $((1,2,3)^T, (9,12,15)^T, (4,5,6)^T)$ není bází prostoru

$$\mathbf{V} = \langle (1,2,3)^T, (9,12,15)^T, (4,5,6)^T \rangle \leq \mathbb{R}^3 \ ,$$

protože je lineárně závislá podle příkladu 5.25. Posloupnost $((1,2,3)^T)$ je sice lineárně nezávislá, ale není bází $\mathbf{V}$, protože daný prostor negeneruje (například vidíme, že $(4,5,6)^T$ není v lineárním obalu vektoru $(1,2,3)^T$). Posloupnost $((1,2,3)^T, (2,1,1)^T)$ není bází $\mathbf{V}$, protože vektor $(2,1,1)^T$ není ani prvkem $\mathbf{V}$, jak jsme se přesvědčili v příkladu 5.21. Posloupnost $((1,2,3)^T, (4,5,6)^T)$ je bází $\mathbf{V}$, protože generuje $\mathbf{V}$ (viz opět 5.25) a je lineárně nezávislá, jak se snadno přesvědčíme.

Příklad 5.43. Najdeme nějakou bázi prostoru

$$\mathbf{V} = \left\langle \begin{pmatrix} 2 \\ 1 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 4 \\ 5 \\ 0 \end{pmatrix}, \begin{pmatrix} 6 \\ 3 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 4 \\ 6 \\ 6 \end{pmatrix} \begin{pmatrix} 3 \\ 5 \\ 2 \\ 3 \end{pmatrix} \right\rangle \leq \mathbb{Z}_7^4 \ .$$

Využijeme toho, že řádkové úpravy matice nemění lineární obal řádků (viz důsledek 5.23). Vektory tedy napíšeme do řádků a převedeme řádkovými úpravami na odstupňovaný tvar. Nenulové řádky generují stejný prostor a navíc jsou podle tvrzení 5.33 lineárně nezávislé, tedy tvoří bázi.

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

Bází $\mathbf{V}$ je tedy například posloupnost $((2,1,3,0)^T, (0,0,6,1)^T, (0,0,0,4)^T)$.

Příklad 5.44. Uvažujme prostor $\mathbf{V}$ nekonečných posloupností $(a_1, a_2, \dots)$ splňujících $a_n = a_{n-1} + a_{n-2}$ pro každé $n \geq 3$, s běžnými operacemi sčítání a násobení skalárem. Prostor $\mathbf{V}$ je podprostorem $\mathbb{R}^\omega$ mezi jehož prvky patří Fibonacciho posloupnost, viz příklad 5.18.

Příkladem báze je dvoučlenná posloupnost

$$(p_1, p_2) = ((\varphi^1, \varphi^2, \dots), \ ((1-\varphi)^1, (1-\varphi)^2, \dots)) \ ,$$

kde $\varphi = (1+\sqrt{5})/2$ je hodnota zlatého řezu. Tato posloupnost je lineárně nezávislá, protože již první dvě souřadnice tvoří lineárně nezávislou posloupnost v $\mathbb{R}^2$. Rovněž generuje $\mathbf{V}$, protože první dvě souřadnice generují $\mathbb{R}^2$ a prvky $\mathbf{V}$ jsou určeny prvními dvěma souřadnicemi. Jako cvičení si rozmyslete detaily, tedy například proč oba vektory p_1, p_2 patří do $\mathbf{V}$.

Nyní můžeme nalézt vzorec pro n-tý člen Fibonacciho posloupnosti, protože víme, že Fibonacciho posloupnost lze vyjádřit jako lineární kombinace posloupností p_1 a p_2, takže stačí zjistit koeficienty. Dostaneme vzorec z části 4.5.1.

5.4.2. *Steinitzova věta o výměně a důsledky, dimenze.* Z vizuální představy prostorů $\mathbb{R}^2$ je patrné, že všechny báze mají dva prvky. Méně vektorů prostor nemůže generovat a množina třech a více vektorů nemůže být lineárně nezávislá. Podobně, v $\mathbb{R}^3$ mají všechny báze právě tři prvky. Obecně platí, že každý vektorový prostor má bázi a všechny báze mají stejný počet prvků. Tomuto počtu říkáme dimenze. Tyto zásadní skutečnosti v této části dokážeme pro konečně generované prostory.

Definice 5.45. Vektorový prostor se nazývá *konečně generovaný*, pokud má nějakou konečnou množinu generátorů.

Jedna možnost, jak se můžeme pokusit hledat bázi vektorového prostoru je vzít nějakou posloupnost generátorů a vynechávat vektory z posloupnosti, dokud vzniklé posloupnosti stále generují daný prostor. Pokud již nemůžeme pokračovat, máme minimální posloupnost generátorů. Minimální zde znamená, že vynecháním libovolného vektoru vznikne posloupnost, která prostor negeneruje. Následující tvrzení říká, že v tomto případě již máme bázi.

Tvrzení 5.46. *Minimální posloupnost generátorů $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$ vektorového prostoru $\mathbf{V}$ je báze $\mathbf{V}$.*

Důkaz. Podle poznámek za definicí 5.24 je posloupnost lineárně závislá právě tehdy, když

$$\langle \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n \rangle = \langle \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_{i-1}, \mathbf{v}_{i+1}, \dots, \mathbf{v}_n \rangle$$

pro nějaké $i \in \{1, 2, \dots, n\}$. To se ale nestane, protože předpokládáme, že máme minimální posloupnost generátorů. Posloupnost je tedy lineárně nezávislá, takže je to báze. □

Důsledek 5.47. *Z každé konečné množiny generátorů vektorového prostoru lze vybrat bázi.*

Důkaz. Postupně vynecháváme vektory dokud nevznikne minimální množina generátorů. Množinu seřadíme do posloupnosti a ta je podle tvrzení bází. □

Obecně z každé (ne nutně konečné) množiny generátorů konečně generovaného prostoru jde vybrat bázi. Myšlenka je, že nejprve vybereme konečnou množinu generátorů a pak použijeme předchozí výsledek. Detaily si rozmyslete jako cvičení.

Speciálně dostáváme důležitý důsledek:

Důsledek 5.48. *Každý konečně generovaný vektorový prostor má bázi.*

Příklad 5.49. Podíváme znovu na příklad prostoru $\mathbf{V} = \langle X \rangle \leq \mathbb{R}^3$, kde $X = \{(1,2,3)^T, (9,12,15)^T, (4,5,6)^T\}$. Množina generátorů X není minimální, protože např. vektor $(9,12,15)^T$ lze vynechat (viz příklad 5.25). Množina $Y = \{(1,2,3)^T, (4,5,6)^T\}$ je minimální množina generátorů, protože, jak je vidět, vynecháním kteréhokoliv ze dvou vektorů vznikne podprostor, který neobsahuje druhý z vektorů. Takže posloupnost $((1,2,3)^T, (4,5,6)^T)$ musí být báze podle tvrzení 5.46, což skutečně je.

K důkazu dalších zásadních skutečností se nám bude hodit tzv. Steinitzova věta o výměně. Ta říká, že pro libovolnou lineárně nezávislou posloupnost N délky k lze v libovolné posloupnosti generující $\mathbf{V}$ vyměnit některých k členů za členy N tak, že vzniklá posloupnost stále generuje $\mathbf{V}$.

Věta 5.50 (Steinitzova věta o výměně)**.** *Nechť $N = (\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k)$ je lineárně nezávislá posloupnost ve vektorovém prostoru $\mathbf{V}$ nad $\mathbf{T}$ a nechť $G = (\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_l)$ generuje $\mathbf{V}$. Pak $k \leq l$ a při vhodném uspořádání $G' = (\mathbf{w}'_1, \mathbf{w}'_2, \dots, \mathbf{w}'_l)$ posloupnosti G platí, že $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k, \mathbf{w}'_{k+1}, \mathbf{w}'_{k+2}, \dots, \mathbf{w}'_l)$ generuje $\mathbf{V}$.*

Důkaz. Dokážeme indukcí podle k. Pro $k = 0$ je tvrzení zřejmé, takže předpokládáme, že $k > 0$ a že tvrzení platí pro $|N| < k$.

Podle indukčního předpokladu platí $k - 1 \leq l$ a můžeme najít přeuspořádání $G'' = (\mathbf{w}''_1, \mathbf{w}''_2, \dots, \mathbf{w}''_l)$ takové, že

$$P = (\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_{k-1}, \mathbf{w}''_k, \mathbf{w}''_{k+1}, \dots, \mathbf{w}''_l)$$

generuje $\mathbf{V}$. Zbývá do P umístit vektor $\mathbf{v}_k$ výměnou za některý z vektorů $\mathbf{w}''_k$, $\mathbf{w}''_{k+1}$, ...

Protože P generuje $\mathbf{V}$, vektor $\mathbf{v}_k$ jde napsat jako lineární kombinace vektorů z P:

$$\mathbf{v}_k = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_{k-1}\mathbf{v}_{k-1} + a_k\mathbf{w}''_k + a_{k+1}\mathbf{w}''_{k+1} + \cdots + a_l\mathbf{w}''_l \ .$$

Posloupnost N je lineárně nezávislá, proto $\mathbf{v}_k$ není lineární kombinací vektorů $\mathbf{v}_1, \dots, \mathbf{v}_{k-1}$. To znamená, že platí $k \leq l$ a navíc alespoň jeden z prvků a_k, a_{k+1}, ..., a_l tělesa $\mathbf{T}$ je nenulový. Předpokládejme, že $a_k \neq 0$, jinak můžeme posloupnost G'' přeuspořádat do posloupnosti G' (a patřičně změnit P), aby toto platilo.

Ukážeme, že

$$Z = (\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k, \mathbf{w}''_{k+1}, \mathbf{w}''_{k+2}, \dots, \mathbf{w}''_l)$$

generuje $\mathbf{V}$. Vektor $\mathbf{w}''_k$ jde napsat jako lineární kombinace vektorů $\mathbf{v}_1, \ldots, \mathbf{v}_k, \mathbf{w}''_{k+1}, \ldots, \mathbf{w}''_l$, což lze nahlédnout z rovnosti výše (z rovnosti vyjádříme $a_k\mathbf{w}''_k$ a vynásobíme a_k^{-1}). Takže lineární obal Z obsahuje vektor $\mathbf{w}''_k$ a tím pádem

$$\langle Z\rangle \supseteq \left\langle \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{k-1}, \mathbf{w}''_k, \mathbf{w}''_{k+1}, \ldots, \mathbf{w}''_l\right\rangle = \langle P\rangle = V \ .$$

□

Nejdůležitější důsledek Steinitzovy věty je, že všechny báze obsahují stejný počet vektorů. To umožňuje dát přesný význam slovu dimenze.

Důsledek 5.51. *Každé dvě báze konečně generovaného vektorového prostoru mají stejný počet prvků.*

Důkaz. Předpokládejme, že $B = (\mathbf{v}_1, \ldots, \mathbf{v}_k)$ a $C = (\mathbf{w}_1, \ldots, \mathbf{w}_l)$ jsou dvě báze vektorového prostoru $\mathbf{V}$. Protože posloupnost B je lineárně nezávislá a posloupnost C generuje $\mathbf{V}$, platí podle Steinitzovy věty $k \leq l$. Z téže věty plyne také $l \leq k$, protože C je lineárně nezávislá a B generuje $\mathbf{V}$. Dohromady dostáváme $k = l$. □

Definice 5.52. *Dimenzí* konečně generovaného vektorového prostoru $\mathbf{V}$ nad $\mathbf{T}$ rozumíme počet prvků jeho libovolné báze. Dimenzi prostoru $\mathbf{V}$ značíme $\dim(V)$.

Příklad 5.53. V souladu s intuicí je dimenze aritmetického vektorového prostoru $\mathbf{T}^n$ rovna n, protože kanonická báze má n prvků.

Triviální prostor $\{\mathbf{o}\}$ má dimenzi 0 protože prázdná posloupnost je jeho báze.

Prostor $\langle(1,1,1)\rangle \leq \mathbb{R}^3$ má dimenzi 1, protože $((1,1,1))$ je jeho bází. To odpovídá geometrické představě, že daný prostor je přímkou.

Dimenze prostoru

$$\mathbf{V} = \left\langle \begin{pmatrix} 2\\1\\3\\0 \end{pmatrix}, \begin{pmatrix} 1\\4\\5\\0 \end{pmatrix}, \begin{pmatrix} 6\\3\\1\\1 \end{pmatrix}, \begin{pmatrix} 1\\4\\4\\1 \end{pmatrix} \begin{pmatrix} 3\\5\\2\\3 \end{pmatrix} \right\rangle \leq \mathbb{Z}_7^4$$

je 3, protože v příkladu 5.43 jsme nalezli tříprvkovou bázi.

Zdůvodnění následujících tvrzení přenecháme do cvičení. Dimenze prostoru všech matic nad $\mathbf{T}$ typu $m \times n$ je mn. Dimenze prostoru reálných polynomů stupně nejvýše n je $n+1$. Dimenze prostoru $\mathbb{C}$ jako vektorového prostoru nad $\mathbb{R}$ je 2.

V důsledku 5.47 jsme viděli, že z každé konečné množiny generátorů lze vybrat bázi. Při hledání báze můžeme postupovat i opačně – k lineárně nezávislé množině doplnit vektory, aby vznikla báze. Následující důsledek říká, že to jde, navíc můžeme doplňovat pouze vektory z libovolně zvolené množiny generátorů. Důsledek formulujeme pro konečné množiny, obecněji necháme důkaz do cvičení.

Důsledek 5.54. *Nechť G je konečná množina generátorů vektorového prostoru $\mathbf{V}$. Každá lineárně nezávislá posloupnost N ve $\mathbf{V}$ jde doplnit prvky G na bázi $\mathbf{V}$.*

Důkaz. Označme $N = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$ Nejprve pomocí důsledku 5.47 vybereme z G bázi $B = (\mathbf{w}_1, \ldots, \mathbf{w}_l)$. Ze Steinitzovy věty dostaneme, že při vhodném přeuspořádání báze B, posloupnost $Z = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k, \mathbf{w}_{k+1}, \ldots, \mathbf{w}_l)$ generuje $\mathbf{V}$. Ze Z jde podle důsledku 5.47 vybrat bázi. My ale víme, že dimenze $\mathbf{V}$ je l (protože B je báze), takže již Z musí být báze. □

Formulujeme dva triviální důsledky.

Důsledek 5.55. *Maximální lineárně nezávislá posloupnost v konečně generovaném prostoru je bází.*

Obecněji, maximální lineárně nezávislá podposloupnost konečné množiny generátorů je bází.

Příklad 5.56. V příkladu 5.43 jsme hledali nějakou bázi prostoru

$$\mathbf{V} = \langle \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_5\rangle = \left\langle \begin{pmatrix} 2\\1\\3\\0 \end{pmatrix}, \begin{pmatrix} 1\\4\\5\\0 \end{pmatrix}, \begin{pmatrix} 6\\3\\1\\1 \end{pmatrix}, \begin{pmatrix} 1\\4\\6\\6 \end{pmatrix} \begin{pmatrix} 3\\5\\2\\3 \end{pmatrix} \right\rangle \leq \mathbb{Z}_7^4 \ .$$

Teď z vektorů $\mathbf{v}_1$, $\mathbf{v}_2$, …, $\mathbf{v}_5$ bázi $\mathbf{V}$ vybereme. Z důsledku 5.47 plyne, že to jde. Předchozí důsledek 5.54 nám dává návod, jak to jde udělat. Stačí totiž vzít libovolnou maximální lineárně nezávislou podmnožinu $\{\mathbf{v}_1, \ldots, \mathbf{v}_5\}$, ta již musí být bází. Můžeme postupovat například tak, že začneme s lineárně nezávislou posloupností $(\mathbf{v}_1)$. Pokusíme se přidat $\mathbf{v}_2$ – otestujeme řádkovými úpravami, zda $(\mathbf{v}_1, \mathbf{v}_2)$ je lineárně nezávislá.

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

Dvojice $(\mathbf{v}_1, \mathbf{v}_2)$ je lineárně závislá, vektor $\mathbf{v}_2$ tedy přidávat nebudeme. Zkusíme $\mathbf{v}_3$.

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

Máme lineárně nezávislou posloupnost $(\mathbf{v}_1, \mathbf{v}_3)$. Pokusíme se k ní přidat $\mathbf{v}_4$. Při testování lineární závislosti můžeme využít již provedených úprav.

$$\begin{pmatrix} 2 & 1 & 3 & 0 \\ 0 & 0 & 6 & 1 \\ 1 & 4 & 6 & 6 \end{pmatrix} \sim \begin{pmatrix} 2 & 1 & 3 & 0 \\ 0 & 0 & 6 & 1 \\ 0 & 0 & 1 & 6 \end{pmatrix} \sim \begin{pmatrix} 2 & 1 & 3 & 0 \\ 0 & 0 & 6 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} .$$

Vektor $\mathbf{v}_4$ přidávat nebudeme. Nakonec zkusíme $\mathbf{v}_5$.

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

Protože $(\mathbf{v}_1, \mathbf{v}_3, \mathbf{v}_5)$ je lineárně nezávislá posloupnost a navíc je maximální lineárně nezávislá posloupnost tvořená vektory v množině $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_5\}$ (neboť přidáním $\mathbf{v}_2$ nebo $\mathbf{v}_4$ již vznikne lineárně závislá množina), tvoří tato posloupnost bázi $\mathbf{V}$.

Dokázaná tvrzení umožňují dokazovat a zobecňovat i další fakta, která jsou geometricky zřejmá pro $\mathbb{R}^2$ nebo $\mathbb{R}^3$:

Pozorování 5.57. *V každém prostoru $\mathbf{V}$ dimenze n platí:*

(1) *Každá množina generátorů $\mathbf{V}$ obsahuje alespoň n vektorů.*
(2) *Každá n-prvková posloupnost generátorů je bází $\mathbf{V}$.*
(3) *Každá lineárně nezávislá posloupnost ve $\mathbf{V}$ obsahuje nejvýše n vektorů.*
(4) *Každá n-prvková lineárně nezávislá posloupnost ve $\mathbf{V}$ je bází $\mathbf{V}$.*

Důkaz. Z každé množiny generátorů lze vybrat bázi a všechny báze obsahují n vektorů. Z toho plynou první dva body.

Každou lineárně nezávislou množinu lze doplnit na n-prvkovou bázi. Z toho plynou zbylé dva body. □

Příklad 5.58. V příkladu 5.29 jsme zdůvodnili, že posloupnost $(3i+5, 2, 3)^T, (5, 2+i, 1)^T, (4, 2, 12)^T, (\pi, e^\pi, 4)^T$ v prostoru $\mathbb{C}^3$ je lineárně závislá. Teď máme kratší zdůvodnění – podle třetího bodu v pozorování nemůže žádná lineárně nezávislá posloupnost v $\mathbb{C}^3$ obsahovat více než 3 vektory.

Podobně můžeme bez jakéhokoliv počítání rozhodnout, že množina $\{(1, 3, i+e^\pi, -10)^T, (i, 2i, 3+2i, -311)^T, (2, \pi, \pi, -4)^T\}$ negeneruje $\mathbb{C}^4$ podle prvního bodu.

Nakonec ukážeme, že podprostor má nejvýše takovou dimenzi jako původní prostor.

Tvrzení 5.59. *Je-li $\mathbf{W}$ podprostor konečně generovaného prostoru $\mathbf{V}$, pak $\mathbf{W}$ je konečně generovaný a platí* $\dim(\mathbf{W}) \leq \dim(\mathbf{V})$*, přičemž rovnost nastane právě tehdy, když $W = V$.*

Důkaz. Nejprve dokážeme, že $\mathbf{W}$ je konečně generovaný. (Pozor, zde se často dělá chyba. Toto „intuitivně zřejmé“ tvrzení je třeba dokázat.) Předpokládejme pro spor, že $\mathbf{W}$ nemá konečnou množinu generátorů. Vezmeme libovolný nenulový vektor $\mathbf{w}_1 \in W$. Protože $\{\mathbf{w}_1\}$ negeneruje W_2, existuje vektor $\mathbf{w}_2 \in W$ takový, že $\mathbf{w}_2 \notin \langle \mathbf{w}_1 \rangle$, atd.: Indukcí najdeme pro libovolné i vektor $\mathbf{w}_i \in W$, který neleží v lineárním obalu předchozích vektorů $\mathbf{w}_1, \dots, \mathbf{w}_{i-1}$. Podle poznámky za tvrzením 5.26 (cvičení **??**) je pro každé i posloupnost $(\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_i)$ lineárně nezávislá (ve $\mathbf{W}$, tedy i ve $\mathbf{V}$), což je spor s bodem (3) předchozího pozorování.

Již víme, že $\mathbf{W}$ je konečně generovaný, takže má bázi B podle důsledku 5.48. Báze B prostoru $\mathbf{W}$ je lineárně nezávislá množina ve $\mathbf{V}$, takže $\dim(\mathbf{W}) = |B| \leq \dim(\mathbf{V})$, opět podle bodu (3). Pokud se dimenze rovnají, pak B je bází $\mathbf{W}$ podle (4), z čehož vyplývá, že $V = W$. (Naopak z $V = W$ triviálně plyne $\dim(V) = \dim(W)$.) □

Příklad 5.60. Podle tvrzení mají podprostory $\mathbb{R}^3$ dimenzi 0 (triviální podprostor $\{\mathbf{o}\}$), 1 (podprostory tvaru $\langle \mathbf{u} \rangle$, kde $\mathbf{u}$ je nenulový vektor, tedy přímky procházející počátkem), 2 (podprostory tvaru $\langle \mathbf{u}, \mathbf{v} \rangle$, kde $(\mathbf{u}, \mathbf{v})$ je lineárně nezávislá, tedy roviny procházející počátkem) nebo 3 (triviální podprostor $\mathbb{R}^3$). Nyní tedy máme precizní důkaz, že diskuze o podprostorech $\mathbb{R}^3$ v části 5.2.1 byla správná.

Obecněji z tvrzení vyplývá, že každý netriviální podprostor $\mathbf{T}^n$ lze zapsat jako lineární obal 1 až $n-1$ (lineárně nezávislých) vektorů.

5.4.3. *Báze jako souřadnicový systém.* Vraťme se teď k pozorování 5.38, které říká, že máme-li bázi $B = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ prostoru $\mathbf{V}$, pak každý vektor $\mathbf{v}$ ve $\mathbf{V}$ lze jednoznačným způsobem vyjádřit jako lineární kombinaci vektorů $\mathbf{v}_1, \ldots, \mathbf{v}_n$. Koeficientům této lineární kombinace říkáme souřadnice $\mathbf{v}$ vzhledem k B.

Definice 5.61. Nechť $B = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ je báze vektorového prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$ a $\mathbf{w} \in \mathbf{V}$. *Souřadnicemi* (též *vyjádřením*) *vektoru* $\mathbf{w}$ *vzhledem k* B rozumíme (jednoznačně určený) aritmetický vektor $(a_1, a_2, \ldots, a_n)^T \in \mathbf{T}^n$ takový, že

$$\mathbf{w} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n \ .$$

Souřadnice $\mathbf{w}$ vzhledem k B značíme $[\mathbf{w}]_B$, tj.

$$[\mathbf{w}]_B = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \ .$$

ZNOVU OBRAZEK

Souřadnice závisí na pořadí vektorů v bázi. Z tohoto důvodu jsme bázi definovali jako posloupnost vektorů, nikoliv množinu.

Zvolíme-li v prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$ dimenze n bázi B, pak předchozí definice jednoznačně přiřazuje každému vektoru $\mathbf{v} \in V$ aritmetický vektor $[\mathbf{v}]_B \in T^n$. Naopak, každý aritmetický vektor v $\mathbf{T}^n$ je roven $[\mathbf{v}]_B$ pro nějaký (jednoznačně určený) vektor $\mathbf{v} \in V$. Zobrazení přiřazující $[\mathbf{v}]_B$ vektoru $\mathbf{v}$ je tedy bijekcí mezi V a T^n.

Příklad 5.62. V příkladu 5.39 jsme si všimli, že pro kanonickou bázi $K = (\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n)$ prostoru $\mathbf{T}^n$ a libovolný vektor $\mathbf{v} \in T^n$ platí

$$[\mathbf{v}]_K = \mathbf{v} \ .$$

Jednou z bází prostoru $\mathbf{V} = \langle (1,2,3)^T, (4,5,6)^T \rangle \leq \mathbb{R}^3$ je posloupnost $B = ((1,2,3)^T, (4,5,6)^T)$ (viz příklad 5.42. Vektor $(9,12,15)^T$ leží v prostoru $\mathbf{V}$, protože $(9,12,15)^T = (1,2,3)^T + 2 \cdot (4,5,6))^T$. Jeho vyjádření v bázi B je podle tohoto vztahu

$$[(9,12,15)]_B = (1,2)^T \ .$$

Posloupnost $B = (x, x^2, 1)$ je bází prostoru reálných polynomů stupně nejvýše dva. Souřadnice vektoru $a+bx+cx^2$ vzhledem k této bázi je

$$[a + bx + cx^2]_B = (b, c, a)^T \ .$$

Příklad 5.63. Uvažujme posloupnost

$$B = (\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) = \left(\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 4 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix} \right)$$

v prostoru $\mathbb{Z}_5^3$. Ověříme, že B je bází a najdeme souřadnice vektoru $\mathbf{w} = (4,0,1)^T$ vzhledem k B.

Obojí uděláme najednou, pokusíme se $\mathbf{w}$ vyjádřit jako lineární kombinaci vektorů v B. Z mnohokrát použitého pohledu na násobení jako na lineární kombinování nahlédneme, že souřadnice $[\mathbf{w}]_B$ jsou řešením soustavy rovnic $A\mathbf{x} = \mathbf{w}$, kde $A = (\mathbf{v}_1|\mathbf{v}_2|\mathbf{v}_3)$ (tj. vektory z báze napíšeme do sloupců). Soustavu vyřešíme.

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

Vidíme, že A je regulární (odstupňovaný tvar je horní trojúhelníková matice s nenulovými prvky na diagonále), takže B je báze podle poznámky za příkladem 5.41. Řešením soustavy je

$$\mathbf{x} = [\mathbf{w}]_B = \begin{pmatrix} 2 \\ 4 \\ 4 \end{pmatrix} \ .$$

Pro kontrolu můžeme ověřit, že skutečně platí $\mathbf{w} = 2\mathbf{v}_1 + 4\mathbf{v}_2 + 4\mathbf{v}_3$.

Korespondence mezi vektory a souřadnicemi ve zvolené bázi je ještě těsnější, zachovává totiž operace vektorového prostoru. Konkrétně, souřadnice součtu vektorů ve $\mathbf{V}$ (vzhledem k B) jsou rovny součtu jejich souřadnic (vzhledem k B) v prostoru $\mathbf{T}^n$. Podobně pro násobení skalárem.

Tvrzení 5.64. *Nechť* $B = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ *je báze vektorového prostoru* $\mathbf{V}$ *nad tělesem* $\mathbf{T}$*, nechť* $\mathbf{u}, \mathbf{w} \in V$ *a* $t \in T$*. Pak platí*

(1) $[\mathbf{u}+\mathbf{w}]_B = [\mathbf{u}]_B + [\mathbf{w}]_B$ *a*
(2) $[t\mathbf{u}]_B = t[\mathbf{u}]_B$

Na levých stranách vystupují operace v prostoru $\mathbf{V}$, na pravých stranách jsou operace v $\mathbf{T}^n$.

Důkaz. Je-li $[\mathbf{u}]_B = (a_1, a_2, \dots, a_n)^T$ a $[\mathbf{w}]_B = (b_1, b_2, \dots, b_n)^T$, pak podle definice souřadnic platí

$$\mathbf{u} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n, \quad \mathbf{w} = b_1\mathbf{v}_1 + b_2\mathbf{v}_2 + \cdots + b_n\mathbf{v}_n \ .$$

Sečtením a úpravou získáme

$$\mathbf{u}+\mathbf{w} = (a_1+b_1)\mathbf{v}_1 + (a_2+b_2)\mathbf{v}_2 + \cdots + (a_n+b_n)\mathbf{v}_n \ ,$$

což podle definice znamená $[\mathbf{u}+\mathbf{w}]_B = (a_1+b_1, a_2+b_2, \dots, a_n+b_n)^T = [\mathbf{u}]_B + [\mathbf{v}]_B$.

Druhá část tvrzení je rovněž snadné cvičení. □

Příklad 5.65. V prostoru $\mathbf{V} = \langle (1,2,3), (4,5,6) \rangle \leq \mathbb{R}^3$ uvažujme bázi $B = ((1,2,3)^T, (4,5,6)^T)$ a vektory $\mathbf{u}, \mathbf{w}$ se souřadnicemi $(1,2)^T$, $(3,-1)^T$ vzhledem k B:

$$\mathbf{u} = \begin{pmatrix} 9 \\ 12 \\ 15 \end{pmatrix}, [\mathbf{u}]_B = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \quad \mathbf{w} = \begin{pmatrix} -1 \\ 1 \\ 3 \end{pmatrix}, [\mathbf{w}]_B = \begin{pmatrix} 3 \\ -1 \end{pmatrix} \ .$$

Součtem $\mathbf{u}$ a $\mathbf{w}$ je vektor $(8,13,18)^T$, jeho souřadnice vzhledem k B jsou $(1,2)^T + (3,-1)^T = (4,1)^T$. Skutečně, $4 \cdot (1,2,3)^T + 1 \cdot (4,5,6)^T = (8,13,18)^T$.

Teď již vidíme přesný význam hesla „všechny konečně generované vektorové prostory jsou v podstatě $\mathbf{T}^n$“. Zvolíme-li v prostoru bázi B, můžeme místo původních vektorů počítat s jejich souřadnicemi vzhledem k B a tím se vše převádí do $\mathbf{T}^n$. Otázku, jak se souřadnice mění při přechodu od báze B k jiné bázi, vyřešíme v kapitole 7 o lineárních zobrazení.

Do $\mathbf{T}^n$ můžeme převádět celé podmnožiny, tj. pro $X \subseteq V$ definujeme

$$[X]_B = \{[\mathbf{v}]_B : \mathbf{v} \in X\} \subseteq T^n \ .$$

Tento přechod také zachovává důležité vlastnosti, jako lineární nezávislost, generování, báze, apod. Důkaz tohoto pozorování přenecháme jako cvičení.

Pozorování 5.66. *Nechť B je báze vektorového prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$ dimenze n. Pak platí*

(1) *posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k)$ je lineárně nezávislá ve $\mathbf{V}$ právě tehdy, když je posloupnost $([\mathbf{v}_1]_B, [\mathbf{v}_2]_B, \dots, [\mathbf{v}_k]_B)$ lineárně nezávislá v $\mathbf{T}^n$;*
(2) *množina X generuje $\mathbf{V}$ právě tehdy, když $[X]_B$ generuje $\mathbf{T}^n$;*
(3) *posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k)$ je báze $\mathbf{V}$ právě tehdy, když je posloupnost $([\mathbf{v}_1]_B, [\mathbf{v}_2]_B, \dots, [\mathbf{v}_k]_B)$ báze $\mathbf{T}^n$.*

5.5. Dimenze podprostorů určených maticí, soustavy rovnic podruhé.

K matici A nad tělesem $\mathbf{T}$ typu $m \times n$ máme přiřazeny řádkový a sloupcový prostor $\operatorname{Im} A^T \leq \mathbf{T}^n$ a $\operatorname{Im} A \leq T^m$. Ukážeme, že mají stejnou dimenzi. Dále dáme do souvislosti dimenzi prostoru $\operatorname{Ker} A \leq \mathbf{T}^n$ a $\operatorname{Im} A$, a podíváme se ještě jednou na řešení soustav lineárních rovnic v terminologii zavedené v této kapitole. V této části budou vystupovat pouze aritmetické vektorové prostory a jejich podprostory.

5.5.1. *Bázové sloupce matice.* Po převodu soustavy lineárních rovnic elementárními řádkovými úpravami do odstupňovaného tvaru jsme rozdělili proměnné na bázové a volné (parametry). Nyní ukážeme, že toto rozdělení nezávisí na konkrétních provedených úpravách, ale pouze na původní soustavě (viz tvrzení 5.71). Výsledek samozřejmě formulujeme v jazyku matic.

Definice 5.67. Nechť A je matice nad $\mathbf{T}$. Říkáme, že i-tý sloupec matice A je *bázový*, pokud není lineární kombinací předchozích sloupců, tj. pokud platí

$$A_{*i} \notin \langle A_{*1}, A_{*2}, \dots, A_{*(i-1)} \rangle \ .$$

Pojmenování ospravedlňuje skutečnost, že bázové sloupce tvoří bázi sloupcového prostoru matice. To si rozmyslete jako cvičení.

Pozorování 5.68. *Pro libovolnou matici A tvoří bázové sloupce bázi sloupcového prostoru. Speciálně, dimenze $\operatorname{Im} A$ je rovna počtu bázových sloupců.*

Příklad 5.69. V matici

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

je bázový druhý a čtvrtý sloupec. První, třetí ani pátý sloupec není bázový. Je to vidět u prvního a třetího sloupce, pátý je součtem druhého a čtvrtého, takže také není bázový.

Za okamžik ukážeme, že řádkové úpravy neovlivňují skutečnost, zda je sloupec bázový nebo ne. Nejdříve ale ukážeme, že bázové sloupce matice v odstupňovaném tvaru jsou právě sloupce obsahující pivoty.

Tvrzení 5.70. *Bázové sloupce matice A nad $\mathbf{T}$ typu $m \times n$ v odstupňovaném tvaru jsou právě sloupce k_1, k_2, …, k_r, kde $r, k_1, \ldots, k_r$ jsou parametry z definice 2.10 odstupňovaného tvaru.*

Důkaz. OBRAZEK

Pro $j = 1, 2, \ldots, n$ označme W_j lineární obal prvních j sloupců, tj. $W_j = \langle A_{*1}, A_{*2}, \ldots, A_{*j} \rangle$. Dále nechť $\mathbf{V}_j$ je následující podprostor $\mathbf{T}^m$:

$$V_j = \{(x_1, x_2, \ldots, x_j, 0, 0, \ldots, 0) : x_1, x_2, \ldots, x_j \in T\} \ .$$

Pro libovolné i je W_{k_i-1} podprostorem prostoru $\mathbf{V}_{i-1}$. Sloupec A_{*k_i} do tohoto prostoru nepatří, takže je bázový.

Zbývá ukázat, že ostatní sloupce bázové nejsou. Za tím účelem si všimneme, že $W_{k_i} = V_i$ pro libovolné i. Je to proto, že za prvé $(A_{*k_1}, A_{*k_2}, \ldots, A_{*k_i})$ je lineárně nezávislá posloupnost (žádný z vektorů v posloupnosti není lineární kombinací předchozích, takže posloupnost je lineárně nezávislá podle cvičení **??**), čili $\dim(W_{k_i}) \geq i$, a za druhé $\dim(V_i) = i$. Prostor $\mathbf{W}_i$ dimenze alespoň i je podprostorem $\mathbf{V}_i$ dimenze i, takže skutečně platí $W_{k_i} = V_i$ podle tvrzení 5.59.

Nyní již důkaz dokončíme snadno. Sloupce $A_{*1}, A_{*2}, \ldots, A_{*k_1-1}$ jsou celé nulové, takže nejsou bázové. Sloupce $A_{*(k_1+1)}, A_{*(k_1+2)}, \ldots, A_{*(k_2-1)}$ nejsou bázové, protože patří do V_2, tedy i do W_{k_1}, atd. □

Tvrzení 5.71. *Nechť A je matice nad tělesem $\mathbf{T}$ typu $m \times n$ a R je regulární matice řádu m. Pak pro libovolné $i \in \{1, 2, \ldots, n\}$ platí, že i-tý sloupec matice A je bázový právě tehdy, když je bázový i-tý sloupec matice RA.*

Důkaz. Tvrzení je důsledkem definice a pozorování, že matice A má stejné lineární závislosti mezi sloupci jako matice RA (toho jsme si všimli v poznámce za tvrzením 5.59). Obšírněji, i-tý sloupec matice A je bázový právě tehdy, když není lineární kombinací předchozích sloupců, tj. právě tehdy, když $A(a_1, \ldots, a_{i-1}, 1, 0, 0, \ldots, 0)^T = \mathbf{o}$ pro nějaké prvky $a_1, \ldots, a_{i-1} \in T$. To nastane právě tehdy, když $RA(a_1, \ldots, a_{i-1}, 1, 0, 0, \ldots, 0)^T = \mathbf{o}$. (Připomeňme, že implikaci zprava doleva v této ekvivalenci lze dokázat například vynásobením zleva maticí R^{-1}.) □

Příklad 5.72. Jako ilustraci provedeme v předchozím příkladu Gaussovu eliminaci a přesvědčíme se, že bázové sloupce jsou právě sloupce obsahující pivoty.

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

5.5.2. *Hodnost.* Z dokázaného tvrzení je již jen krok k důkazu, že sloupcový a řádkový prostor matice mají stejnou dimenzi. Této dimenzi říkáme hodnost matice.

Věta 5.73. *Pro libovolnou matici A platí* $\dim(\operatorname{Im} A) = \dim(\operatorname{Im} A^T)$.

Důkaz. Myšlenka je taková, že pro matice v odstupňovaném tvaru tvrzení platí a ani jedna dimenze se řádkovými úpravami nemění, takže tvrzení platí pro jakoukoliv matici.

Detailněji. Každou matici lze elementárními řádkovými úpravami převést do odstupňovaného tvaru. Jinými slovy, existuje regulární matice R taková, že RA je v odstupňovaném tvaru. Dimenze sloupcového prostoru matice A i RA je počet bázových sloupců (viz pozorování 5.68), tyto dimenze jsou stejné (viz tvrzení 5.71) a rovnají se počtu nenulových řádků matice RA (viz tvrzení 5.70).

Dimenze řádkového prostoru matice RA je také rovna počtu nenulových řádků, protože nenulové řádky tvoří lineárně nezávislou posloupnost (viz tvrzení 5.33), která zřejmě generuje řádkový prostor. Ale násobení regulární maticí zleva nemění lineární obal řádků (viz tvrzení 5.22), speciálně, dimenze řádkového prostoru matice RA je stejná jako dimenze řádkového prostoru matice A. □

Definice 5.74. *Hodností* matice A rozumíme dimenzi řádkového (sloupcového) prostoru matice A. Značíme $\operatorname{rank}(A)$.

Shrneme některé důležité triviální důsledky do pozorování.

Pozorování 5.75. *Pro libovolnou matici A platí* $\operatorname{rank}(A) = \operatorname{rank}(A^T)$. *Hodnost se nemění elementárními řádkovými ani sloupcovými úpravami. Hodnost matice v řádkově odstupňovaném tvaru je rovna počtu nenulových řádků.*

Poslední věta pozorování také vysvětluje volbu písmena r pro počet nenulových řádků v odstupňovaném tvaru.

Příklad 5.76. V závislosti na $a, b \in \mathbb{Z}_3$ určíme dimenzi prostoru

$$\mathbf{V}_{a,b} = \left\langle \begin{pmatrix} a \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ b \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix} \right\rangle \leq \mathbb{Z}_3^3 \ ,$$

přičemž nás nebude zajímat konkrétní báze.

Vektory si napíšeme do řádků nebo sloupců a určíme hodnost matice. Přitom můžeme využívat jak řádkové, tak sloupcové úpravy. Zvolíme například řádky.

$$\begin{pmatrix} a & 1 & 2 \\ 1 & b & 2 \\ 1 & 2 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 1 \\ a & 1 & 2 \\ 1 & b & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 1 \\ 2 & 1 & a \\ 2 & b & 1 \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 1 & 2 & 1 \\ 0 & 0 & a+1 \\ 0 & b+2 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 1 \\ 0 & b+2 & 2 \\ 0 & 0 & a+1 \end{pmatrix}$$

V první úpravě jsme přeuspořádali řádky a v druhé jsem prohodili sloupce. Bývá totiž výhodnější mít parametry co nejvíce vpravo dole, aby se do úprav dostaly co nejpozději. Následně jsme vyeliminovali první sloupec a nakonec ještě prohodili řádky.

Pokud $b \neq 1$ a $a \neq 2$, pak je matice v odstupňovaném tvaru se třemi nenulovými řádky a $\dim(\mathbf{V}_{a,b}) = 3$. Pokud $b \neq 1$ a $a = 2$, pak je matice rovněž v odstupňovaném tvaru tentokrát s dvěma nenulovými řádky a $\dim(\mathbf{V}_{a,b}) = 2$. Pokud $b = 1$, pak můžeme ještě upravit (pozor, v tomto případě je matice v odstupňovaném tvaru pouze když $a = 2$!)

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

a dimenze je 2.

Shrnutí: Pokud $b \neq 1$ a $a \neq 2$ je $\dim(\mathbf{V}_{a,b}) = 3$, ve všech ostatních případech je $\dim(\mathbf{V}_{a,b}) = 2$.

Hodnost matice A je rovná dimenzi obrazu příslušného zobrazení f_A. Máme-li ještě matici B, aby byl definován součin AB, pak hodnost AB je rovná dimenzi obrazu zobrazení f_{AB}. Ale obraz zobrazení $f_{AB} = f_A \circ f_B$ je podprostorem obrazu zobrazení f_A, takže hodnost AB je menší nebo rovna hodnosti A. Tuto nerovnost a obdobnou nerovnost pro násobení zleva dokážeme algebraicky.

Tvrzení 5.77. *Nechť A je matice nad $\mathbf{T}$ typu $m \times n$ a B matice nad $\mathbf{T}$ typu $n \times p$. Pak platí*

$$\operatorname{rank}(AB) \leq \operatorname{rank}(A), \quad \operatorname{rank}(AB) \leq \operatorname{rank}(B) \ .$$

Důkaz. Opět použijeme tvrzení 4.14 o pohledu na násobení jako počítání lineárních kombinací. Dostáváme $\operatorname{Im}(AB) \leq \operatorname{Im}(A)$, takže $\operatorname{rank}(AB) \leq \operatorname{rank}(A)$ (podle tvrzení 5.59 o dimenzi podprostoru). Podobně $\operatorname{Im}(AB)^T \leq \operatorname{Im} B^T$, takže $\operatorname{rank}(AB)^T \leq \operatorname{rank}(B^T)$, z toho plyne $\operatorname{rank}(AB) \leq \operatorname{rank}(B)$. □

Důsledek 5.78. *Nechť A je matice nad $\mathbf{T}$ typu $m \times n$ a R je regulární matice nad $\mathbf{T}$ řádu m. Pak* $\operatorname{rank}(RA) = \operatorname{rank}(A)$. *Podobně pro násobení regulární maticí zprava.*

Důkaz. Podle předchozího tvrzení platí $\operatorname{rank}(RA) \leq \operatorname{rank}(A)$, ale také $\operatorname{rank}(A) = \operatorname{rank}(R^{-1}(RA)) \leq \operatorname{rank}(RA)$. □

Pomocí hodnosti můžeme také doplnit charakterizaci regulárních matic dokázanou ve větě 4.30. Uvažujme čtvercovou matici A nad $\mathbf{T}$ řádu n. Bod (2) ve větě říká, že f_A je zobrazení na, neboli $A\mathbf{x} = \mathbf{b}$ má řešení pro každou pravou stranu, neboli $\operatorname{Im} A = T^n$ (sloupce generují $\mathbf{T}^n$), což nastane podle tvrzení 5.59 právě tehdy, když $\dim(\operatorname{Im} A) = \operatorname{rank}(A) = n$. Bod (4) říká, že $A\mathbf{x} = \mathbf{o}$ má jediné řešení, neboli sloupce A jsou lineárně nezávislé. Protože $\operatorname{rank}(A) = \operatorname{rank}(A^T)$ můžeme podobné charakterizace formulovat i pro řádky. Dostáváme následující pozorování.

Pozorování 5.79. *Nechť A je čtvercová matice nad $\mathbf{T}$ řádu n. Následující tvrzení jsou ekvivalentní.*

(1) *A je regulární.*
(2) $\operatorname{rank}(A) = n$.
(3) *Sloupce (řádky) matice A jsou lineárně nezávislé.*

(4) *Sloupce (řádky) matice A generují $\mathbf{T}^n$.*
(5) *Sloupce (řádky) matice A tvoří bázi $\mathbf{T}^n$.*

Všimněte si, že ekvivalence sloupcových (a řádkových) verzí také plyne z pozorování 5.57.

Příklad 5.80. Ukážeme řešení jedné kombinatorické úlohy pomocí hodnosti matice. Příklad byl převzat ze sbírky *Šestnáct miniatur* Jiřího Matouška, kde jsou popsány některé zajímavé aplikace lineární algebry v jiných oborech. Lze ji najít na domovské stránce autora.

Ve městě žije n občanů, kteří jsou sdruženi v m klubech. Podle vyhlášky městské rady má každý klub lichý počet členů, zatímco pro každé dva různé kluby musí být počet společných členů sudý. Dokážeme, že v této situaci je $m \leq n$, tedy klubů není více než občanů.

Občany označíme čísly $1, 2, \ldots, n$ a kluby čísly $1, 2, \ldots, m$. Utvoříme matici $A = (a_{ij})$ typu $m \times n$ nad tělesem $\mathbb{Z}_2$ tak, že $a_{ij} = 1$, pokud občan j je v klubu i, a $a_{ij} = 0$, jinak. Každý řádek tedy popisuje členy jednoho klubu, má na j-té pozici jedničku právě tehdy, když občan j je jeho členem. Například

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

popisuje situaci, kdy ve městě je 5 občanů a 3 kluby. Členy klubu 1 jsou občané $1, 2, 3$, členy klubu 2 jsou občané $2, 3, 4$ a jediným členem klubu 3 je občan 5. Všimněte si, že tato situace je v souladu s vyhláškou městské rady.

Spočítáme součin matic $AA^T = (b_{kl})$. Prvek na místě kl je součtem n sčítanců $a_{k1}a_{l1} + a_{k2}a_{l2} + \cdots + a_{kn}a_{ln}$. Sčítanec $a_{km}a_{lm}$ je roven jedné právě tehdy, když občan m je v obou klubech k, l, jinak je roven nule. Počítáme v $\mathbb{Z}_2$, takže celý součet je roven jedné, pokud je počet společných členů klubů k a l lichý, jinak je roven nule. Vyhlášku nyní můžeme přeformulovat tak, že $a_{kk} = 1$ a $a_{kl} = 0$ pro libovolná $k \neq l$. Jinými slovy $AA^T = I_m$.

Hodnost matice A je nejvýš n, protože hodnost nemůže být vyšší než počet sloupců. Z tvrzení 5.77 o hodnosti součinu dostaneme

$$\operatorname{rank}(A) \geq \operatorname{rank}(AA^T) = \operatorname{rank}(I_m) = m \ .$$

Celkově $n \geq \operatorname{rank}(A) \geq m$ a jsme hotovi.

5.5.3. *Ještě jednou soustavy rovnic, dimenze jádra a obrazu.* Nyní si zopakujeme různé pohledy na řešení soustav lineárních rovnic a utřídíme již známé skutečnosti o existenci a tvaru řešení. Většina tvrzení již byla dokázána (hlavně ve větě 2.14), přesto některé důkazy stručně zopakujeme, aby vynikla elegance a užitečnost pojmů zavedených v této kapitole. (Navíc věta 2.14 byla formulována jen nad reálnými čísly, formálně jsme ji nedokazovali pro případ libovolného tělesa.)

Budeme předpokládat, že A je matice nad tělesem $\mathbf{T}$ typu $m \times n$ a $\mathbf{b} \in T^m$. Na řešení soustavy $A\mathbf{x} = \mathbf{b}$ se můžeme dívat několika způsoby:

(1) Hledání průniku m „nadrovin“ v prostoru $\mathbf{T}^n$ (každá rovnice, neboli řádek matice A, určuje jednu „nadrovinu“).
(2) Hledání koeficientů lineárních kombinací sloupců matice A, jejímž výsledkem je $\mathbf{b}$.
(3) Určování vzoru vektoru $\mathbf{b}$ při zobrazení f_A.

Pomocí pojmu hodnost můžeme formulovat kritérium řešitelnosti.

Věta 5.81 (Frobeniova věta)**.** *Soustava $A\mathbf{x} = \mathbf{b}$ má řešení právě tehdy, když* $\operatorname{rank}(A) = \operatorname{rank}(A \mid \mathbf{b})$.

Důkaz. Rovnost $A\mathbf{x} = \mathbf{b}$ je pro nějaké $\mathbf{x} \in T^n$ splněna právě tehdy, když $\mathbf{b}$ je lineární kombinací sloupců matice A, což platí právě tehdy, když $\operatorname{Im} A = \operatorname{Im}(A \mid \mathbf{b})$. Uvážíme-li, že $\operatorname{Im} A \leq \operatorname{Im}(A \mid \mathbf{b})$, vidíme, že podprostory jsou rovny právě tehdy, když se rovnají jejich dimenze (viz tvrzení 5.59). □

Prakticky, hodnosti vidíme z odstupňovaného matice soustavy, protože hodnost je rovna počtu nenulových řádků v odstupňovaném tvaru, takže kritérium ve Frobeniově větě se shoduje s předchozím kritériem na řešitelnost (neexistence řádku tvaru $(0, 0, \ldots, 0, a)$, $a \neq 0$ v odstupňovaném tvaru).

Tvar řešení je určený řešením příslušné homogenní soustavy. Řešením je vždy posunutí podprostoru o nějaký vektor, tedy obecný rovný útvar.

Tvrzení 5.82. *Pokud je soustava $A\mathbf{x} = \mathbf{b}$ řešitelná, pak množina všech jejích řešení je rovná množině*

$$\mathbf{u} + \operatorname{Ker} A = \{u + \mathbf{w} : \mathbf{w} \in \operatorname{Ker} A\} \ ,$$

kde $\mathbf{u}$ je libovolné (partikulární) řešení soustavy.

Důkaz. Libovolný vektor tvaru $\mathbf{u}+\mathbf{w}$, $\mathbf{w}\in\operatorname{Ker}A$ je řešením soustavy, protože $A(\mathbf{u}+\mathbf{w})=A\mathbf{u}+A\mathbf{w}=\mathbf{b}+\mathbf{o}=\mathbf{b}$ (dokázali jsme vlastně (p3) z věty 2.14).

Naopak, pokud $\mathbf{v}$ řeší soustavu $A\mathbf{v}=\mathbf{b}$, pak $\mathbf{v}\in\mathbf{u}+\operatorname{Ker}A$, protože $\mathbf{v}=\mathbf{u}+(\mathbf{v}-\mathbf{u})$ a vektor $\mathbf{v}-\mathbf{u}$ leží v $\operatorname{Ker}A$, jak ukazuje výpočet $A(\mathbf{v}-\mathbf{u})=A\mathbf{v}-A\mathbf{u}=\mathbf{b}-\mathbf{b}=\mathbf{o}$ (zde znovu dokazujeme (p4) z věty 2.14). □

Prostor $\operatorname{Ker}A$ můžeme určit nalezením jeho báze. Označme $j_1<j_2<\cdots<j_{n-r}$ nebázové sloupce matice A (příslušným proměnné nazýváme volné). Každý prvek $\mathbf{x}=(x_1,\dots,x_n)\in\operatorname{Ker}A$ (neboli každé řešení homogenní soustavy $A\mathbf{x}=\mathbf{o}$) je jednoznačně určen vektorem $(x_{j_1},x_{j_2},\dots,x_{j_{n-r}})\in T^{n-r}$ (a naopak, libovolný vektor v T^{n-r} určuje jedno řešení). Toto jsme nahlédli v pozorování 2.13 použitím odstupňovaného tvaru, můžeme to ale dokázat přímo z definice bázových sloupců (viz cvičení).

Bázi $\operatorname{Ker}A$ můžeme získat volbou nějaké báze T^{n-r} (ve větě 2.14 jsme použili kanonickou bázi) a dopočítáním zbylých složek (prakticky provedeme z odstupňovaného tvaru; ve větě 2.14 jsme výsledné vektory značili $\mathbf{v}^{(p)}$). Dimenze $n-r$ prostoru $\operatorname{Ker}A$ je rovná počtu nebázových sloupců, ta je rovná počet všech sloupců (to je n) minus počet bázových (to je hodnost r matice A). Po úpravě dostáváme větu o dimenzi jádra a obrazu.

Věta 5.83 (Věta o dimenzi jádra a obrazu)**.** *Pro libovolnou matici A nad $\mathbf{T}$ typu $m\times n$ platí*

$$\dim(\operatorname{Ker}A)+\dim(\operatorname{Im}A)=n\quad(=\dim(\operatorname{Ker}A)+\operatorname{rank}(A))\ .$$

Příklad 5.84. Vrátíme se k soustavě z části 2.3.4.

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

Převodem do odstupňovaného tvaru jsme získali

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

Vidíme, že $\dim(\operatorname{Im}A)=\operatorname{rank}(A)=\operatorname{rank}(A\mid\mathbf{b})=2$, takže soustava je řešitelná. Dimenze $\operatorname{Ker}A$ je $6-2=4$. Partikulární řešení získáme dopočítáním z libovolné volby volných proměnných. V 2.3.4 jsme zvolili nulový vektor a dostali jsme vektor $(-1,0,-3,0,0)^T$. Bázi $\operatorname{Ker}A$ získáme dopočítáním z nějaké báze T^3. V 2.3.4 jsme volili kanonickou bázi T^3 a získali jsme následující bázi $\operatorname{Ker}A$: $((-2,1,0,0,0)^T,(-3,0,0,1,0)^T,(-2,0,-2,0,1)^T)$. Celkově můžeme řešení psát ve tvaru

$$\begin{pmatrix}-1\\0\\-3\\0\\0\end{pmatrix}+\left\langle\begin{pmatrix}-2\\1\\0\\0\\0\end{pmatrix},\begin{pmatrix}-3\\0\\0\\1\\0\end{pmatrix},\begin{pmatrix}-2\\0\\-2\\0\\1\end{pmatrix}\right\rangle.$$

Podívejme se ještě na geometrickou interpretaci věty o dimenzi jádra a obrazu. Matice A určuje zobrazení $f_A:T^n\to T^m$. Dimenze jádra určuje dimenzi prostoru vektorů, které se zobrazí na nulový vektor. To si můžeme představovat jako počet dimenzí, které zobrazení f_A „zkolabuje“ do bodu. Větu lze nyní interpretovat tak, že dimenze obrazu je rovná dimenzi prostoru, který zobrazujeme (n) minus počet zkolabovaných dimenzí. Například pokud $f_A:\mathbb{R}^3\to\mathbb{R}^3$ je projekce na nějakou rovinu, pak $\dim(\operatorname{Ker}A)=1$ a $\operatorname{rank}(A)=\dim(\operatorname{Im}A)=2$. Pro zobrazení $f_A:\mathbb{R}^2\to\mathbb{R}^3$ (viz obrázek **??**), které „věrně“ zobrazuje rovinu do nějaké roviny v $\mathbb{R}^3$, je $\dim(\operatorname{Ker}A)=0$ a $\operatorname{rank}(A)=2$.

5.6. Průnik a součet podprostorů.

Průnik dvou i více podprostorů nějakého vektorového prostoru je vždy podprostor.

Tvrzení 5.85. *Jsou-li $V_i, i\in I$ podprostory vektorového prostoru $\mathbf{V}$, pak $\bigcap_{i\in I}V_i$ je podprostorem $\mathbf{V}$.*

Důkaz. Stačí ověřit, že průnik je neprázdný a je uzavřený na sčítání a násobení skalárem (viz tvrzení 5.6). Průnik je neprázdný, protože obsahuje nulový vektor. Jsou-li $\mathbf{u},\mathbf{w}$ dva vektory z průniku, pak pro každé $i\in I$ platí $\mathbf{u},\mathbf{w}\in V_i$. Protože V_i jsou podprostory, platí $\mathbf{u}+\mathbf{w}\in V_i$ pro každé $i\in I$. To ale znamená, že $\mathbf{u}+\mathbf{w}$ leží v průniku podprostorů V_i. Uzavřenost na násobení skalárem se dokáže podobně. □

Sjednocení dvou podprostorů je zřídkakdy podprostorem. Například sjednocení dvou různých přímek v $\mathbb{R}^2$ zřejmě není podprostorem, protože není uzavřené na sčítání. Nejmenší podprostor obsahující dané podprostory nazýváme jejich součten.

Definice 5.86. Nechť $V_i, i \in I$ jsou podprostory vektorového prostoru $\mathbf{V}$. *Součtem* (též *spojením*) podprostorů $V_i, i \in I$ rozumíme lineární obal jejich sjednocení, značíme jej $\sum_{i\in I} V_i$, tj.

$$\sum_{i\in I} V_i = \left\langle \bigcup_{i\in I} V_i \right\rangle \ .$$

Součet podprostorů $V_1, V_2, \ldots, V_k$ také značíme $V_1 + V_2 + \cdots + V_k$.

Jako cvičení dokažte, že součet je asociativní.

Při tvorbě lineárního obalu stačí sjednocení $V_1 \cup V_2 \cup \cdots \cup V_k$ uzavřít na součty vektorů z různých podprostorů, tj. platí

$$V_1 + V_2 + \cdots + V_k = \{v_1 + v_2 + \cdots + v_k : v_1 \in V_1, v_2 \in V_2, \ldots, v_k \in V_k\} \ .$$

Důkaz přenecháme jako cvičení. Rovněž si všimněme, že sjednocením množiny generátorů prostoru $\mathbf{U}$ a množiny generátorů prostoru $\mathbf{V}$ je množina generátorů prostoru $\mathbf{U} + \mathbf{V}$.

Pro dimenze dvou podprostorů a jejich součtu a průniku platí podobný vztah jako pro počty prvků ve dvou množinách a jejich sjednocení a průniku.

Věta 5.87 (Věta o dimenzi součtu a průniku)**.** *Pro libovolné dva konečně generované podprostory* $\mathbf{U}, \mathbf{V}$ *vektorového prostoru* $\mathbf{W}$ *platí*

$$\dim(\mathbf{U}) + \dim(\mathbf{V}) = \dim(\mathbf{U} \cap \mathbf{V}) + \dim(\mathbf{U} + \mathbf{V}) \ .$$

Důkaz. Prostor $\mathbf{U} \cap \mathbf{V}$ je podprostorem konečně generovaného prostoru $\mathbf{U}$, proto je konečně generovaný (viz tvrzení 5.59). Vezmeme libovolnou bázi $B = (\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k)$ průniku $\mathbf{U} \cap \mathbf{V}$ (báze existuje v libovolném konečně generovaném prostoru podle důsledku 5.48). Množina B je lineárně nezávislá v prostoru $\mathbf{U}$, takže ji můžeme doplnit na bázi $C = (\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k, \mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_l)$ prostoru $\mathbf{U}$ (viz důsledek 5.54). Podobně doplníme B na bázi $D = (\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_m, \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m)$ prostoru $\mathbf{V}$.

Ukážeme, že $E = (\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k, \mathbf{u}_1, \ldots, \mathbf{u}_l, \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m)$ je báze $\mathbf{U} + \mathbf{V}$. Posloupnost E generuje $\mathbf{U} + \mathbf{V}$ podle poznámky nad větou (cvičení **??**). Zbývá ukázat, že E je lineárně nezávislá. Předpokládejme, že

$$\sum_{i=1}^{k} a_i \mathbf{w}_i + \sum_{i=1}^{l} b_i \mathbf{u}_i + \sum_{i=1}^{m} c_i \mathbf{v}_i = \mathbf{o} \ .$$

Chceme dokázat, že všechny koeficienty jsou nutně nulové. Vztah drobně upravíme.

$$\sum_{i=1}^{l} b_i \mathbf{u}_i = -\sum_{i=1}^{m} c_i \mathbf{v}_i - \sum_{i=1}^{k} a_i \mathbf{w}_i$$

Vektor $\mathbf{u} = \sum_{i=1}^{l} b_i \mathbf{u}_i$ leží v prostoru $\mathbf{U}$ a také leží, podle odvozeného vztahu, v lineárním obalu vektorů $\mathbf{v}_1, \ldots, \mathbf{v}_m$, $\mathbf{w}_1, \ldots, \mathbf{w}_k$, čili v prostoru $\mathbf{V}$. Vektor $\mathbf{u}$ tedy leží v průniku $\mathbf{U} \cap \mathbf{V}$ a proto jej lze vyjádřit jako lineární kombinaci vektorů $\mathbf{w}_1, \ldots, \mathbf{w}_k$ báze B.

$$\mathbf{u} = \sum_{i=1}^{k} d_i \mathbf{w}_i$$

Z toho získáme následující vyjádření $\mathbf{o}$ jako lineární kombinaci prvků C:

$$\mathbf{o} = \sum_{i=1}^{k} d_i \mathbf{w}_i - \sum_{i=1}^{l} b_i \mathbf{u}_i \ ,$$

takže $b_1 = b_2 = \cdots = b_l = d_1 = d_2 = \cdots = d_k = 0$, protože C je lineárně nezávislá..

Podobně bychom dokázali, že koeficienty c_1, c_2, …, c_m jsou rovněž všechny nulové. Nyní ale $a_1 = a_2 = \cdots = a_k = 0$, protože B je lineárně nezávislá. □

Věta se geometricky dobře představí, když si ze vztahu vyjádříme dimenzi součtu podprostorů jako součet dimenzí jednotlivých prostorů minus dimenze společné části (průniku). Věta se může hodit třeba při určování dimenze průniku, protože dimenze prostorů a jejich součtu nebývá problém spočítat.

Příklad 5.88. Určíme dimenzi průniku podprostorů $\mathbf{U}, \mathbf{V} \leq \mathbb{Z}_5^4$.

$$U = \left\langle \begin{pmatrix} 2 \\ 1 \\ 0 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \\ 3 \\ 3 \end{pmatrix} \right\rangle, \quad V = \left\langle \begin{pmatrix} 2 \\ 3 \\ 4 \\ 1 \end{pmatrix}, \begin{pmatrix} 4 \\ 4 \\ 0 \\ 1 \end{pmatrix} \right\rangle$$

Dimenzi U a V zjistíme tím, že si vektory napíšeme do řádků a řádkovými úpravami převedeme do odstupňovaného tvaru (víme, že hodnost se nemění ani sloupcovými úpravami, my ale později využijeme toho, že řádkové úpravy nemění lineární obal řádků).

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

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

Vidíme, že $\dim(\mathbf{U}) = 2$ a $\dim(\mathbf{V}) = 2$. Nenulové řádky matice A generují $\mathbf{U}$ a řádky matice B generují $\mathbf{V}$ (protože elementární řádkové úpravy nemění lineární obal), takže dohromady máme množinu generátorů $\mathbf{U} + \mathbf{V}$, která už je částečně upravená. Dokončíme Gaussovu eliminaci.

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

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

Vidíme, že $\dim(\mathbf{U} + \mathbf{V}) = 3$. Z věty o dimenzi součtu a průniku dostáváme

$$\dim(\mathbf{U} \cap \mathbf{V}) = \dim(\mathbf{U}) + \dim(\mathbf{V}) - \dim(\mathbf{U} + \mathbf{V}) = 2 + 2 - 3 = 1 \ .$$

Příklad 5.89. Dokážeme, že průnikem dvou různých podprostorů $\mathbf{U}, \mathbf{V}$ dimenze 2 (rovin) v prostoru $\mathbf{W}$ dimenze 3 (např. $\mathbb{R}^3$) je podprostor dimenze 1 (přímka).

Protože podprostory $\mathbf{U}$ a $\mathbf{V}$ jsou různé, $\mathbf{U}$ je vlastním podprostorem $\mathbf{U} + \mathbf{V}$. Podle tvrzení 5.59 o dimenzi podprostorů máme $2 = \dim \mathbf{U} < \dim(\mathbf{U} + \mathbf{V}) \leq \dim(\mathbf{W}) = 3$, takže dimenze součtu je 3 (součet je podle stejného tvrzení celý prostor $\mathbf{W}$). Z věty o dimenzi součtu a průniku teď můžeme spočítat

$$\dim(\mathbf{U} \cap \mathbf{V}) = \dim(\mathbf{U}) + \dim(\mathbf{V}) - \dim(\mathbf{U} + \mathbf{V}) = 2 + 2 - 3 = 1 \ .$$

Na rozdíl od sjednocení a průniku, pro součet a průnik **neplatí distributivní zákony**. Z toho důvodu také neplatí „přímočaré zobecnění“ věty o dimenzi součtu a průniku na případ tří podprostorů, viz cvičení.

Jak jsme si již všimli, každý vektor v součtu $\mathbf{V} = \mathbf{V}_1 + \mathbf{V}_2 + \cdots + \mathbf{V}_k$ lze psát jakou součet $v_1 + v_2 + \cdots + v_k$. Pokud je tento zápis jednoznačný hovoříme o direktním součtu. Tento pojem je obdobou pojmu báze pro podprostory.

Definice 5.90. Říkáme, že $\mathbf{V}$ je *direktním součtem* podprostorů $\mathbf{V}_1, \mathbf{V}_2, \ldots, \mathbf{V}_k$, pokud jsou splněny dvě podmínky.

(1) $\mathbf{V} = \mathbf{V}_1 + \mathbf{V}_2 + \cdots + \mathbf{V}_k$
(2) $\mathbf{V}_i \cap (\mathbf{V}_1 + \mathbf{V}_2 + \cdots + \mathbf{V}_{i-1} + \mathbf{V}_{i+1} + \mathbf{V}_{i+2} + \cdots + \mathbf{V}_k) = \{\mathbf{o}\}$ pro libovolné $i \in \{1, 2, \ldots, k\}$.

Skutečnost, že $\mathbf{V}$ je direktním součtem $\mathbf{V}_1, \mathbf{V}_2, \ldots, \mathbf{V}_k$ zapisujeme

$$\mathbf{V} = \mathbf{V}_1 \oplus \mathbf{V}_2 \oplus \cdots \oplus \mathbf{V}_k \ .$$

Pro dva podprostory $\mathbf{V}_1, \mathbf{V}_2$ se podmínky zjednoduší na $\mathbf{V}_1 + \mathbf{V}_2 = \mathbf{V}$ a $\mathbf{V}_1 \cap \mathbf{V}_2 = \{\mathbf{o}\}$

Tvrzení 5.91. *Nechť $\mathbf{V}_1, \mathbf{V}_2, \ldots, \mathbf{V}_k$ jsou podprostory vektorového prostoru $\mathbf{V}$. Pak následující tvrzení jsou ekvivalentní.*

(1) $\mathbf{V} = \mathbf{V}_1 \oplus \mathbf{V}_2 \oplus \cdots \oplus \mathbf{V}_k$.
(2) *Každý vektor $\mathbf{v} \in V$ lze zapsat právě jedním způsobem ve tvaru $\mathbf{v} = \mathbf{v}_1 + \mathbf{v}_2 + \cdots + \mathbf{v}_k$, kde $\mathbf{v}_i \in V_i$ pro každé $i \in \{1, 2, \ldots, k\}$.*

Důkaz. Předpokládejme, že $\mathbf{V} = \mathbf{V}_1 + \mathbf{V}_2 + \cdots + \mathbf{V}_k$. Pak $\mathbf{V}$ je součtem podprostorů $\mathbf{V}_1$, $\mathbf{V}_2$, ..., $\mathbf{V}_k$, takže každý vektor $\mathbf{v} \in V$ lze zapsat ve tvaru $v = v_1 + v_2 + \cdots + v_k$, kde $v_i \in V_i$ pro každé $i \in \{1, 2, \ldots, k\}$. K důkazu jednoznačnosti uvažujme dvě taková vyjádření

$$\mathbf{v} = \mathbf{v}_1 + \mathbf{v}_2 + \cdots + \mathbf{v}_k = \mathbf{v}'_1 + \mathbf{v}'_2 + \cdots + \mathbf{v}'_k \ .$$

Pro každé $i \in \{1, 2, \ldots, k\}$ leží vektor $\mathbf{v}_i - \mathbf{v}'_i$ v prostoru $\mathbf{V}_i$, ale také v součtu zbylých podprostorů, jak je vidět z vyjádření

$$\mathbf{v}_i - \mathbf{v}'_i = (\mathbf{v}_1 - \mathbf{v}'_1) + (\mathbf{v}_2 - \mathbf{v}_2)' + \cdots + (\mathbf{v}_{i-1} - \mathbf{v}'_{i-1}) + (\mathbf{v}_{i+1} - \mathbf{v}'_{i+1}) + \cdots + (\mathbf{v}_k - \mathbf{v}'_k) \ .$$

Podle podmínky (2) z definice direktního součtu platí $\mathbf{v}_i - \mathbf{v}'_i$, čili $\mathbf{v}_i = \mathbf{v}'_i$.

Předpokládejme naopak, že platí podmínka (2). Pak $\mathbf{V} = \mathbf{V}_1 + \mathbf{V}_2 + \cdots + \mathbf{V}_k$. Pro spor předpokládejme, že pro nějaké i existuje nenulový vektor $\mathbf{u}$ v průniku $\mathbf{V}_i$ a $\sum_{j\neq i} \mathbf{V}_j$. Pak existují $a_1, a_2, \cdots \in T$ taková, že

$$\begin{aligned}\mathbf{u} &= a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_{i-1}\mathbf{v}_{i-1} + 0\mathbf{v}_i + a_{i+1}\mathbf{v}_{i+1} + \cdots + a_k\mathbf{v}_k \\ &= 0\mathbf{v}_1 + 0\mathbf{v}_2 + \cdots + 0\mathbf{v}_{i-1} + \mathbf{u} + 0\mathbf{v}_{i+1} + \cdots + 0\mathbf{v}_k \ .\end{aligned}$$

Dostali jsme dvě různá vyjádření vektoru $\mathbf{u}$ jako součet vektorů z $V_1, V_2, \ldots, V_k$, spor. □

Direktní součet lze chápat jako rozklad podprostoru na vzájemně nezávislé části. Všimněte si, že $\mathbf{V}$ je direktním součtem jednodimenzionálních podprostorů $\mathbf{V} = \langle\mathbf{v}_1\rangle \oplus \langle\mathbf{v}_2\rangle \oplus \cdots \oplus \langle\mathbf{v}_k\rangle$ právě tehdy, když $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$ je báze.

5.7. **Prostory nekonečné dimenze.**

Pro zjednodušení jsme pojmy lineární nezávislosti a báze definovali pro konečné posloupnosti vektorů, a tím pádem jsme mohli dokazovat některá tvrzení jen pro konečně generované prostory. V této části stručně probereme obecný případ. Příklady prostorů, které nejsou konečně generované, zahrnují prostor reálných funkcí reálné proměnné, nebo reálná čísla chápaná jako vektorový prostor nad $\mathbb{Q}$.

Lineární (ne)závislost a bázi definujeme jako indexovaný soubor vektorů:

Definice (Zobecnění definic 5.24 a 5.37)**.** Soubor $(\mathbf{v}_i : i \in I)$ vektorů ve $\mathbf{V}$ nazýváme *lineárně závislý*, pokud některý z vektorů $\mathbf{v}_i$ je lineární kombinací ostatních vektorů $\mathbf{v}_j, j \neq i$. V opačném případě říkáme, že je soubor *lineárně nezávislý*.

Bází rozumíme lineárně nezávislý soubor generátorů.

Tato definice skutečně rozšiřuje stávající definici, protože posloupnost n vektorů můžeme chápat jako soubor indexovaný množinou $I = \{1, 2, \ldots, n\}$.

Připomeňme, že v lineární kombinaci může mít nenulový koeficient pouze konečně mnoho vektorů, součet nekonečně mnoha vektorů nemáme definován. Tedy například v prostoru $\mathbb{R}^\omega$ všech nekonečných posloupností reálných čísel soubor $(\mathbf{e}_i : i \in \mathbb{N})$, kde $\mathbf{e}_i = (0, 0, \ldots, 1, 0, 0, \ldots)$ s jedničkou na i-tém místě, negeneruje $\mathbb{R}^\omega$. Tento soubor generuje podprostor $\mathbb{R}^{(\omega)}$ všech posloupností s konečným počtem nenulových členů a je jeho bází.

Mnoho dokázaných tvrzení lze zobecnit, konkrétně platí obdoby následujících tvrzení. Důkazy dělat nebudeme.

- Tvrzení 5.26 charakterizující lineární nezávislost.
- Pozorování 5.38, které říká, že každý vektor lze vyjádřit jako lineární kombinaci prvků báze. To umožňuje zavést souřadnice vektoru vzhledem k bázi. Roli aritmetických vektorových prostorů hrají prostory $\mathbf{T}^{(I)}$: Vektory jsou „skoro všude nulové“ I-tice prvků tělesa I, formálněji, soubory $(a_i : i \in I)$, takové, že všechna $a_i \in T$ až na konečný počet jsou nulové. Operace jsou definovány po složkách. Obdoba tvrzení 5.64 o souřadnicích a operacích i obdoba pozorování 5.66 o zachovávání důležitých vlastností jako lineární nezávislost platí.
- Minimální soubor generátorů je vždy báze (obdoba tvrzení 5.46). Obdoba důsledku 5.47, tj. že z každé množiny generátorů lze vybrat bázi platí, ale není to zřejmé, protože není apriori jasné, že minimální generující podmnožina existuje. Speciálně, každý konečně generovaný vektorový prostor má bázi (obdoba důsledku 5.48). Poznamenejme, že důkaz vyžaduje axiom výběru.
- Všechny báze mají stejnou mohutnost (obdoba důsledku 5.51), takže má smysl zavést dimenzi jako mohutnost libovolné báze. Rovněž platí obdoba důsledku 5.54, že libovolný lineárně nezávislý soubor lze doplnit do báze vektory z libovolné množiny generátorů. Z toho plyne obdoba důsledku 5.55, že maximální lineárně nezávislý soubor je báze.
- Obdoba tvrzení 5.59 platí jen částečně. Je pravda, že podprostor má vždy dimenzi menší nebo rovnou dimenzi původního prostoru. Není ale pravda, že rovnost nastane pouze tehdy, když se prostory rovnají. Například dimenze prostoru $\mathbb{R}^{(\omega)}$ skoro všude nulových posloupností je stejná jako dimenze jeho vlastního podprostoru tvořeného posloupnostmi, které začínají nulou.

5.8. **Samoopravné kódy.** Představíme základní pojmy teorie samoopravných kódů a ukážeme si, jak se v ní uplatňuje lineární algebra.

5.8.1. *Kódy neformálně.* V roce 1947 byl v Bellových laboratořích v provozu jeden z prvních reléových počítačů. Relé byla uspořádána do pětic. Jednotlivé cifry $0, 1, \ldots, 9$ byly reprezentovány tak, že vždy dvojice z pěti relé byla sepnuta a zbylá tři nikoliv. Protože existuje deset možných výběrů dvojice prvků z pěti, každá z dvojic reprezentovala právě jednu cifru.

Pokud během výpočtu došlo k nějaké chybě, projevila se tak, že v nějaké pětici relé byl počet sepnutých relé různý od dvou. Počítač to zaregistroval a zastavil se. V té chvíli nastoupila obsluha, nějakým způsobem zjistila, jaká dvojice relé má být správně sepnuta, ručně to zařídila, a spustila pokračování výpočtu.

V režimu bez obsluhy (mimo pracovní dobu) počítač výpočet ukončil a ze zásobníku programů vzal ten následující. Toto ukončování výpočtu bez náhrady motivovalo Richarda W. Hamminga (1915-1998) k návrhu prvních *samoopravných kódů*.

Bellův počítač pracoval s desetiprvkovou abecedou $0, 1, \ldots, 9$. Každou z těchto cifer reprezentoval pomocí posloupnosti pěti nul a jednotek: 00110, 01010, atd. *Binární* vyjádření prvků nějaké abecedy jako posloupnosti nul a jednotek je v současnosti tak běžné, že je považujeme za samozřejmé. Tak například odpovědi v testu s výběrem ze čtyř možností a, b, c, d můžeme přeložit do binárního vyjádření třeba následovně:

$$a = 00,\ b = 01,\ c = 10,\ d = 11.$$

Vyplněný test s 90 otázkami a nabídkou čtyř možných odpovědí je pak totéž, co posloupnost 180 nul a jednotek. Analogicky můžeme zapsat celý genetický kód člověka, použijeme-li překlad

$$G = 00,\ C = 01,\ T = 10,\ H = 11.$$

Zápis bude jenom o něco delší.

Morseova abeceda je příklad jiného kódování. Používá sice také jenom dva symboly - tečka, čárka - ale mezi symboly do abecedy je třeba také zařadit mezeru. To je cena, kterou je nutné zaplatit za to, že posloupnosti teček a čárek reprezentující různá písmena abecedy mohou mít různou délku a Morseova volba byla taková, že vyjádření jednoho písmene může být počátečním úsekem jiného písmene. Např. $e = \cdot$, $a = \cdot -$.

My se budeme v dalším zabývat pouze kódováním, které každému symbolu původní abecedy přiřazuje posloupnost n nul a jedniček pro nějaké pevné n.

Definice 5.92. *Binární blokový kód* délky n je libovolná podmnožina C aritmetického vektorového prostoru $\mathbb{Z}_2^n$. Prvkům C říkáme *slova* nebo také *bloky* kódu C. *Zprávou* v kódu C potom rozumíme posloupnost slov kódu C.

Tak například, je-li $C = \{000, 001, 010, 001, 110, 111\}$ kód délky 3, pak posloupnost

$$000\ 111\ 110\ 010\ 001$$

je zpráva v tomto kódu. Mezery mezi jednotlivými slovy kódu děláme pro pohodlí. Také vynecháváme závorky při zápisu vektorů a čárky mezi jejich složkami, jak je v teroii kódování běžné. Stejná délka jednotlivých bloků v binárním kódu umožňuje jednoznačně interpretovat tutéž zprávu zapsanou bez mezer

$$000111110010001.$$

Zprávu zapsanou v jakékoliv abecedě s konečným počtem symbolů můžeme jednoznačně zakódovat pomocí bloků binárního kódu vhodné délky n. Stačí pouze, aby bylo číslo 2^n aspoň tak velké jako počet znaků v původní abecedě.

V této "digitalizované"podobě můžeme zprávu přenést nějakým *komunikačním kanálem*. Pokud je kanál bez jakéhokoliv šumu, neni žádné nebezpečí, že přijímající strana přijme zprávu v jiné podobě, než v jaké byla vyslána. Takové kanály ale v reálném světě neexistují, vždy je nenulová pravděpodobnost, že některá z cifer 0 nebo 1 se během přenosu změní na opačnou. Pro kanály se šumem nejsou blokové kódy typu $C = \mathbb{Z}_2^n$ vhodné. Skutečnost, že každý blok z n cifer 0 nebo 1 je kódovým slovem, znamená že přijímající strana nemá možnost poznat, že během přenosu zprávy byl nějaký blok pozměněn. Každý přijatý blok mohl být také vyslán.

Řešením je nepoužívat jako kódová slova všechny bloky dané délky n, ale pouze některé. Pokud jsou kódová slova dobře vybrána, může přijímající strana poznat, že během přenosu bloku zprávy došlo k nějaké chybě díky tomu, že přijme posloupnost délky n, která není kódovým slovem. Takový blok vysílající strana nemohla vyslat. Daní, kterou je nutné za to zaplatit, je snížení *rychlosti přenosu informace*, množství informace, kterou kanálem přeneseme za jednotku času. Do kódu vnášíme *nadbytečnost*, cizím slovem *redundanci* - pro přenášení informace používáme více symbolů, než kolik je potřeba. nadbytečnost ale umožňuje odhalovat a opravovat chyby při přenosu dat.

Nejjednodušší způsob jak bojovat se šumem, je vyslat každý blok dvakrát po sobě. Příkladem takového *opakovacího kódu* je následující kód délky 4:

$$C = \{0000, 0101, 1010, 1111\}.$$

Každé slovo má dvě části. První dva symboly jsou *informační symboly*, zbylé dva jsou *kontrolní symboly*. Kontrolní symboly nenesou žádnou informaci, pouze opakují předchozí dva symboly. Z každých čtyř symbolů vyslaného slova pouze první dva nesou informaci. Rychlost přenosu informace pomocí takového kódu je poloviční oproti rychlosti přenosu informace kódem $D = \{00, 01, 10, 11\}$.

Narozdíl od kódu D ale kód C umožňuje přijímající straně poznat, pokud během přenosu slova došlo k jedné chybě. První a druhá polovina přijatého čtyřprvkového bloku se v takovém případě liší. Říkáme, že kód C *odhalí jednu chybu*.

V opakovacím kódu můžeme počáteční informační část opakovat vícekrát. Kód

$$\{000, 111\} \subseteq \mathbb{Z}_2^3$$

obsahuje pouze dva bloky, v každém z nich se první symbol opakuje třikrát. Je to příklad *3-opakovacího kódu*. Jiným příkladem 3-opakovacího kódu je

$$\{000000, 010101, 101010, 111111\} \subseteq \mathbb{Z}_2^6,$$

ve kterém opakujeme třikrát vždy první dva informační symboly. Rychlost přenosu informace kterýmkoliv z těchto dvou kódů je 1/3. V každém bloku je pouze jedna třetina symbolů informačních, zbylé dvě třetiny jsou kontrolní.

Každý 3-opakovací kód odhalí jednu chybu – změníme-li v libovolném bloku jeden symbol, dostaneme slovo, které do kódu nepatří. Oproti prostému opakovacímu kódu ale dokáže navíc *lokalizovat (opravit) jednu chybu*. Ukážeme si to na příkladu, kdy vyslaný blok 010101 přijme přijímající strana jako 010001. Graficky to znázorníme takto:

$$010101 \longrightarrow 010001.$$

Rozdělíme-li libovolné slovo 3-opakovacího kódu na tři stejně dlouhé úseky, jsou tyto úseky stejné. Tak jsou kódová slova definována. Pokud tomu tak u přijatého slova není, došlo během přenosu informace k nějaké chybě. Pokud došlo k jedné chybě, dva z těchto úseků zůstanou stejné, třetí (ten, ve kterém se chyba vyskytla) se od nich liší. Předpokládáme, že vysláno bylo to kódové slovo, ve kterém se všechny tři úseky rovnají těm dvěma stejným přijatým. Je to jediná možnost, jak z přijatého slova dostat kódové slovo změnou jediného symbolu. V našem případě změníme čtvrtý přijatý symbol z 0 na 1 a dostaneme kódové slovo. Jakékoliv jiné kódové slovo dostaneme z přijatého pomocí změny aspoň dvou symbolů. Například tak, že obě přijaté 1 změníme na 0.

Pokud předpokládáme, že pravděpodobnost změny symbolu vlivem šumu je $p < 1/2$, a tedy pravděpodobnost, že symbol byl přijatý správně (tj. tak jak byl vyslán) je $1 - p > 1/2 > p$, pak v případě přijetí nekódového slova je nejpravděpodobnější, že bylo vysláno to slovo, které se od přijatého liší v co nejméně symbolech.

5.8.2. *Hammingova vzdálenost.* Pro teorii samoopravných kódů je následující definice klíčová.

Definice 5.93. Jsou-li $\mathbf{a} = a_1a_2\cdots a_n$ a $\mathbf{b} = b_1b_2\cdots b_n$ libovolné dva prvky $\mathbb{Z}_2^n$, pak jejich *Hammingova vzdálenost* $h(\mathbf{a}, \mathbf{b})$ se rovná počtu indexů $i \in \{1, 2, \ldots, n\}$, pro které platí $a_i \neq b_i$. *Hammingova váha* slova $\mathbf{a} \in \mathbb{Z}_2^n$ je definována jako Hammingova vzdálenost $h(\mathbf{a}, \mathbf{o})$ slova $\mathbf{a}$ od nulového slova $\mathbf{o}$.

Hammingova vzdálenost je tak definována pro posloupnosti téže délky a rovná se počtu míst (indexů), na kterých se obě posloupnosti liší. Hammingova váha slova $\mathbf{a}$ se pak rovná počtu cifer 1 ve slově $\mathbf{a}$. Pro Hammingovu vzdálenost zřejmě platí $h(\mathbf{a}, \mathbf{a}) = 0$ a $h(\mathbf{a}, \mathbf{b}) = h(\mathbf{b}, \mathbf{a})$ pro libovolná dvě slova $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_2^n$. Platí také trojúhelníková nerovnost

$$h(\mathbf{a}, \mathbf{c}) \leq h(\mathbf{a}, \mathbf{b}) + h(\mathbf{b}, \mathbf{c})$$

pro libovolná tři slova $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{Z}_2^n$. Snadno si to ověříte sami. Pokud totiž pro nějaký index $i \in \{1, 2, \ldots, n\}$ platí $a_i \neq c_i$, platí také $a_i \neq b_i$ nebo $b_i \neq c_i$. Jestliže index i přispívá ke vzdálenosti $h(\mathbf{a}, \mathbf{c})$, přispívá také k aspoň jedné ze vzdáleností $h(\mathbf{a}, \mathbf{b})$ nebo $h(\mathbf{b}, \mathbf{c})$.

Hammingovu vzdálenost si můžeme také představit pomocí délky (počtu hran) cest v nějakém neorientovaném grafu. Jeho vrcholy jsou prvky $\mathbb{Z}_2^n$ a dva vrcholy $\mathbf{a}, \mathbf{b}$ jsou spojené hranou pokud se liší v právě jednom symbolu, tj. pokud je jejich Hammingova vzdálenost rovná 1. Pro $n = 2$ se tento graf rovná čtverci, pro $n = 3$ je jím třídimenzionální krychle. Hammingova vzdálenost libovolných dvou vrcholů $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_2^n$ se pak rovná délce (tj. počtu hran) v nejkratší cestě z $\mathbf{a}$ do $\mathbf{b}$. Proto se také někdy tomuto grafu říká *Hammingova krychle* i v případě libovolného n.

Pro schopnost kódu odhalovat a lokalizovat chyby je důležitý pojem minimální vzdálenost kódu.

Definice 5.94. Je-li $C \subseteq \mathbb{Z}_2^n$ binární blokový kód délky n, pak definujeme *minimální vzdálenost* kódu C jako číslo

$$h(C) = \min\{h(\mathbf{a}, \mathbf{b}); \mathbf{a}, \mathbf{b} \in \mathbb{C}, \mathbf{a} \neq \mathbf{b}\}.$$

Příklad 5.95.
- Minimální vzdálenost 3-opakovacího kódu $\{000, 111\}$ se rovná 3.
- Minimální vzdálenost opakovacího kódu $\{0000, 0101, 1010, 1111\}$ se rovná 2.
- Minimální vzdálenost kódu používaného v roce 1947 v reléovém počítači v Bellových laboratořích se rovná 2.
- Minimální vzdálenost kódu $C = \mathbb{Z}_2^n$ se rovná 1.

Nyní můžeme přesně formulovat, co myslíme tím, že nějaký kód $C \subseteq \mathbb{Z}_2^n$ odhalí jednu chybu. Pokud při přenosu slova $\mathbf{a} \in C$ dojde k jedné chybě, přijímající strana to pozná, přijme-li v takovém případě slovo, které není prvkem C. Znamená to, že žádné slovo $\mathbf{b} \in C$, jehož Hammingova vzdálenost od $\mathbf{a}$ se rovná 1, není blokem kódu C. Jinak řečeno, Hammingova vzdálenost libovolných dvou různých kódových slov $\mathbf{a}, \mathbf{b} \in C$ je aspoň 2, a to znamená, že minimální vzdálenost kódu C je aspoň 2.

Každý kód C, jehož minimální vzdálenost je $d > 1$, odhalí až $d - 1$ chyb. Pokud při přenosu slova $\mathbf{a} \in C$ dojde k nejvýše $d - 1$ chybám, přijímající strana přijme slovo $\mathbf{c}$, jehož Hammingova vzdálenost od vyslaného slova $\mathbf{a}$ je

nejvýše $d-1$. Slovo $\mathbf{c}$ tak nepatří do kódu C, a přijímající strana proto odhalí, že při přenosu došlo k nějakým chybám. Počet chyb ale jednoznačně nezjistí stejně jako kde k nim došlo.

Předpokládejme nyní, že minimální vzdálenost nějakého kódu $C \subseteq \mathbb{Z}_2^n$ se rovná 3. Pokud při přenosu slova $\mathbf{a}$ dojde k jedné chybě, přijímající strana přijme slovo $\mathbf{c}$, které má od slova $\mathbf{a}$ Hammingovu vzdálenost $h(\mathbf{c},\mathbf{a}) = 1$. Vzdálenost přijatého slova $\mathbf{c}$ od jakéhokoliv jiného slova $\mathbf{b} \in C$ je v důsledku trojúhelníkové nerovnosti

$$h(\mathbf{c},\mathbf{b}) \geq h(\mathbf{a},\mathbf{b}) - h(\mathbf{a},\mathbf{c}) \geq 3 - 1 = 2,$$

použili jsme navíc skutečnost, že minimální vzdálenost kódu C je 3, a tedy $h(\mathbf{a},\mathbf{b}) \geq 3$ pro jakékoliv dva různé bloky $\mathbf{a},\mathbf{b} \in C$.

Vyslané slovo $\mathbf{a}$ je tedy ze všech možných vyslaných slov $\mathbf{b} \in C$ nejblíže (vzhledem k Hammingově vzdálenosti) k přijatému slovu $\mathbf{c}$. Předpokládáme, že pravděpodobnost poškození přenášeného symbolu šumem v kanálu je $p < 1/2$ a tedy menší než pravděpodobnost $1-p$ že k poškození symbolu nedošlo. V případě přijetí slova $\mathbf{c}$ je nejpravděpodobnější, že bylo vysláno slovo $\mathbf{a} \in C$, které je ze všech slov kódu C nejblíže k přijatému slovu $\mathbf{c}$. V tomto smyslu tedy kód s minimální vzdáleností 3 dokáže opravit (lokalizovat) jednu chybu.

Zcela analogicky lze odůvodnit, že kód s minimální vzdáleností $2d+1$ dokáže opravit d chyb. Schopnost kódu odhalovat a opravovat daný počet chyb je tak dána jeho minimální vzdáleností.

5.8.3. *Paritní kód, lineární kódy.* Nejjednodušší příklad kódu, který je schopen odhalit jednu chybu, je *paritní kód*.

Definice 5.96. *Paritní kód* délky n je podmnožina $S \subseteq \mathbb{Z}_2^n$ tvořená všemi slovy, které obsahují sudý počet jednotek.

Minimální vzdálenost paritního kódu S je 2, paritní kód tedy dokáže odhalit jednu chybu. Známe-li $a_1a_2\cdots a_{n-1}$, existuje právě jedno $a_n \in \{0,1\}$ takové, že slovo $\mathbf{a} = a_1a_2\cdots a_{n-1}a_n \in S$. Prvních $n-1$ symbolů ve slově $\mathbf{a}$ tak můžeme považovat za informační symboly, zatímco poslední symbol a_n je kontrolní. Nenese žádnou dodatečnou informaci, lze jej doplnit na základě znalosti $a_1a_2\cdots a_{n-1}$. Proto se kontrolnímu bitu říká také *paritní bit* nebo *paritní kontrola*. Samozřejmě můžeme za kontrolní bit považovat kterýkoliv symbol ve slově $\mathbf{a}$ a zbylé symboly za informační. Obvyklé ale bývá seřadit symboly v kódovém slově tak, že informační symboly jsou na začátku a kontrolní symboly následují po nich. Rychlost přenosu informace paritním kódem je tak $n-1/n$.

Kódy, které dokážou nejen odhalit, ale i opravit chyby se konstruují kombinací více paritních kontrol.

Paritní kód S délky n má jednu důležitou vlastnost. Tvoří nejenom podmnožinu $\mathbb{Z}_2^n$, ale dokonce podprostor. Obsahuje totiž nulové slovo $\mathbf{o}$, je proto uzavřený na násobení skaláry ze $\mathbb{Z}_2$ a zřejmě také na sčítání. Takové kódy jsou důležité a zaslouží si zvláštní pojmenování.

Definice 5.97. Binární blokový kód $C \subseteq \mathbb{Z}_2^n$ délky n se nazývá *lineární kód*, je-li C podprostor $\mathbb{Z}_2^n$. Je-li dimenze C rovna r, říkáme také, že jde o *lineární* (n,r)-kód.

Minimální vzdálenost lineárních kódů lze zjistit snáze než u obecných kódů.

Tvrzení 5.98. *Minimální vzdálenost lineárního kódu C se rovná*

$$\min\{h(\mathbf{a},\mathbf{o}); \mathbf{a} \in C, \mathbf{a} \neq \mathbf{o}\},$$

tj. rovná se minimální Hammingově váze nenulových prvků C.

Důkaz. Připomeňme si, že minimální vzdálenost kódu C označujeme $h(C)$. Je-li C lineární kód, platí $\mathbf{o} \in C$ a $h(\mathbf{a},\mathbf{o}) \geq h(C)$ pro libovolné nenulové slovo $\mathbf{a} \in C$. Dále platí pro libovolná dvě slova $\mathbf{a},\mathbf{b} \in C$, že

$$h(\mathbf{a},\mathbf{b}) = h(\mathbf{a}+\mathbf{b},\mathbf{o}).$$

Je-li tedy $h(C) = h(\mathbf{a},\mathbf{b})$, platí, že $h(C)$ se rovná Hammingové váze vektoru $\mathbf{a}+\mathbf{b}$. □

Je-li C lineární (n,r)-kód, má prostor C dimenzi r. Zvolíme-li v něm nějakou bázi $\mathbf{a}_1,\ldots,\mathbf{a}_r$, je každý prvek $\mathbf{b}$ kódu (podprostoru) C jenoznačně určen r-ticí jeho souřadnic vzhledem ke zvolené bázi. K jeho jednoznačnému určení nám tedy stačí posloupnost koeficientů lineární kombinace, která vyjadřuje $\mathbf{b}$ pomocí prvků zvolené báze. Naopak, každá posloupnost r nul a jednotek určuje jednoznačně nějaký prvek kódu C. To jenom jinak vyjadřujeme skutečnost, že C je izomorfní aritmetickému prostoru $\mathbb{Z}_2^r$. K předání informace o bloku $\mathbf{b}$ nám tedy stačí předat r koeficientů vyjádřujících $\mathbf{b}$ jako lineární kombinaci báze $\mathbf{a}_1,\ldots,\mathbf{a}_r$. Kód C ale předává celý vektor $\mathbf{b}$ délky n. Intuitivně tak můžeme říct, že rychlost přenosu informace lineárním (n,r)-kódem je r/n.

5.8.4. *Hammingovy kódy.* Hamming předložil tři konstrukce kódů, které opravují jednu chybu. Všechny tři jsou založené na kombinaci několika paritních testů. Všechny tři návrhy jsou lineární kódy. Jejich konstrukci si ukážeme na příkladu, který má čtyři informační symboly. Protože kódy mají opravovat jednu chybu, musí být jejich minimální vzdálenost 3.

Příklad 5.99. V první konstrukci si čtyři informační symboly a, b, c, d napíšeme do prvních dvou řádků a prvních dvou sloupců čtvercové matice řádu 3.

$$\left(\begin{array}{cc|c} a & b & ? \\ c & d & ? \\ \hline ? & ? & ? \end{array}\right)$$

Místo otazníků doplníme další prvky tak, aby v každém řádku a každém sloupci byl sudý počet jednotek. Doplněná matice je

$$\left(\begin{array}{cc|c} a & b & r_1 \\ c & d & r_2 \\ \hline s_1 & s_2 & t \end{array}\right),$$

kde

$$r_1 = a + b,\ r_2 = c + d,\ s_1 = a + c,\ s_2 = b + d,\ t = s_1 + s_2 = a + b + c + d = r_1 + r_2.$$

Celé kódové slovo je potom $abr_1cdr_2s_1s_2t$. Informační symboly jsou na prvním, druhém, čtvrtém a pátém místě, zbylé symboly jsou kontrolní.

Kód C je tvořen všemi slovy $\mathbf{a} = a_1a_2\cdots a_9 \in \mathbb{Z}_2^9$, pro která platí

$$\begin{aligned} a_3 &= a_1 + a_2 \\ a_6 &= a_4 + a_5, \\ a_7 &= a_1 + a_4, \\ a_8 &= a_2 + a_5, \\ a_9 &= a_1 + a_2 + a_4 + a_5. \end{aligned}$$

Prvky a_1, a_2, a_4, a_5 můžeme zvolit libovolně a právě uvedené rovnosti ukazují, že matice

$$\left(\begin{array}{cc|c} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ \hline a_7 & a_8 & a_9 \end{array}\right)$$

splňuje všechny požadované paritní testy, tj. každý řádek a každý sloupec obsahuje sudý počet jednotek.

Z kostrukce kódu také snadno nahlédneme, že kód C opravuje jednu chybu. Pokud totiž při přenosu slova $\mathbf{a} = a_1a_2\cdots a_9 \in C$ dojde k jedné chybě, přijaté slovo nebude splňovat dva paritní testy, jeden pro řádek a druhý pro sloupec, ve kterých leží chybně přijatý symbol. Tyto dva neplatné paritní testy tak přesně určují polohu poškozeného symbolu.

Kód C je lineární, protože jeho prvky jsou právě všechna řešení $x_1x_2\cdots x_9$ homogenní soustavy lineárních rovnic s maticí

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

Třetí sloupec spolu s posledními čtyřmi sloupci jsou lineárně nezávislé, hodnost matice A je tedy aspoň 5, řádky matice A jsou tedy lineárně nezávislé, $\operatorname{rank}(A) = 5$, dimenze $\operatorname{Ker}(A)$ je tudíž podle věty o dimenzi jádra a obrazu rovna $9 - 5 = 4$ a počet prvků kódu C je 16.

Přijímající strana tak snadno ověří, patří-li přijaté slovo $\mathbf{c} = c_1c_2\cdots c_9$ do kódu C. Stačí ověřit rovnost $A\mathbf{c}^T = \mathbf{o}^T$.

Poslední pozorování vede k následující důležité definici.

Definice 5.100. Je-li C lineární (n, r)-kód a pro matici A typu $(n - r) \times n$ platí, že $C = \operatorname{Ker} A$, pak matici A nazýváme *kontrolní matice* kódu C.

Z definice kontrolní matice a z věty o dimenzi jádra a obrazu matice plyne, že $\operatorname{rank}(A) = \dim(\operatorname{Im}(A)) = n - r$, tj. že posloupnost řádků matice A je lineárně nezávislá. Později si ukážeme obecné tvrzení, ze kterého plyne existence kontrolní matice pro jakýkoliv lineární kód. Ve skutečnosti jsou lineární kódy zadávány tak, že napíšeme jejich kontrolní matici.

Pomocí kontrolní matice můžeme snadno zjistit, jaká je minimální vzdálenost lineárního kódu.

Tvrzení 5.101. *Nechť C je (n,r)-lineární kód a A jeho kontrolní matice. Minimální vzdálenost kódu C se rovná d právě když libovolná $(d-1)$-prvková podposloupnost sloupců matice A je lineárně nezávislá a existuje d-prvková podposloupnost sloupců A, která je lineárně závislá.*

Důkaz. Kontrolní matice A kódu C je typu $(n-r)\times n$. Nechť $\mathbf{x}=x_1x_2\cdots x_n$ je nenulový prvek kódu C. Pak platí $A\mathbf{x}^T=\mathbf{o}^T$, neboli

$$x_1A_{*1}+x_2A_{*2}+\cdots x_nA_{*n}=\mathbf{o}^T.$$

Je-li l Hammingova váha prvku $\mathbf{x}$ a $x_{j_1},x_{j_2},\dots,x_{j_l}$ jsou všechny nenulové složky vektoru $\mathbf{x}$, pak platí rovněž

$$x_{j_1}A_{*j_1}+x_{j_2}A_{*j_2}+\cdots x_{j_l}A_{*j_l}=\mathbf{o}^T,$$

l-prvková podposloupnost sloupcových vektorů $A_{*j_1},\dots,A_{*j_l}$ je tedy lineárně závislá.

Jestliže naopak existuje lineárně závislá podposloupnost $A_{*i_1},A_{*i_2},\dots,A_{*i_m}$ sloupcových vektorů matice A, existují prvky $x_{i_j}\in\mathbb{Z}_2$, ne všechny nulové, takové, že

$$x_{i_1}A_{*i_1}+x_{i_2}A_{*i_2}+\cdots+x_{i_m}A_{*i_m}=\mathbf{o}^T.$$

Doplníme tuto lineární kombinaci zbývajícími sloupcovými vektory matice A s koeficienty $x_i=0$. Vektor $\mathbf{x}=x_1\cdots x_n$ pak splňuje $A\mathbf{x}^T=\mathbf{o}^T$, je tedy blokem kódu C a jeho Hammingova váha je nejvýše m.

Je-li tedy minimální vzdálenost kódu C rovna d, je podle Tvrzení 5.98 minimální Hammingova váha nenulových vektorů v C rovna d. Každá podposloupnost $d-1$ sloupcových vektorů matice A je tedy lineárně nezávislá a existuje podposloupnost d sloupcových vektorů matice A, která je lineárně závislá.

Jestliže naopak je každá podposloupnost $d-1$ sloupcových vektorů matice A lineárně nezávislá, neobsahuje C nenulový vektor, který by měl Hammingovu váhu menší nebo rovnou $d-1$. Pokud je navíc nějaká d-prvková podposloupnost sloupcových vektorů A lineárně závislá, existuje v $C=\operatorname{Ker}A$ nenulový vektor, jehož Hammingova váha je nejvýše d. Minimální Hammingova váha nenulových vektorů v C je tedy rovna d. □

Příklad 5.102. Kontrolní matice A kódu C z Příkladu 5.99 neobsahuje nulový sloupcový vektor, každá jednoprvková podposloupnost sloupcových vektorů matice A je tedy lineárně nezávislá. Libovolné dva sloupcové vektory matice A jsou různé, lineárně nezávislá je proto rovněž každá dvouprvková podposloupnost sloupcových vektorů v A. Platí dokonce, že žádný ze sloupcových vektorů se nerovná součtu jiných dvou sloupcových vektorů, a tak každá tříprvková podposloupnost sloupců matice A je lineárně nezávislá. Naproti tomu první sloupcový vektor se rovná součtu jiných tří sloupcových vektorů, existuje tedy čtyřprvková lineárně závislá podposloupnost sloupcových vektorů matice A. Minimální vzdálenost kódu C je tedy 4.

Kód C tak opraví jednu chybu a odhalí až tři chyby. Rychlost přenosu informace tímto kódem je 4/9, což je zlepšení oproti 3-opakovacímu kódu, který také dokáže opravit jednu chybu.

Příklad 5.103. Druhý kód, který Hamming navrhnul, se od toho prvního liší v tom, že nepoužívá paritní kontrolu třetího řádku a třetího sloupce, tj. nepotřebuje prvek t. Matici

$$\left(\begin{array}{cc|c} a & b & ? \\ c & d & ? \\ \hline ? & ? & ? \end{array}\right)$$

doplní na matici

$$\left(\begin{array}{cc|c} a & b & r_1 \\ c & d & r_2 \\ \hline s_1 & s_2 & \end{array}\right),$$

kde

$$r_1=a+b,\ r_2=c+d,\ s_1=a+c,\ s_2=b+d.$$

Jde opět o lineární kód, označme jej D. Kontrolní matici tohoto kódu dostaneme tak, že z kontrolní matice původního kódu vynecháme poslední řádek a poslední sloupec. Dostaneme tak matici

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

Libovolná dvouprvková podposloupnost sloupců matice B je lineárně nezávislá ze stejného důvodu, jako v případě prvního Hammingova návrhu. Existují lineárně závislé tříprvkové podposloupnosti sloupců v B. Minimální vzdálenost kódu D je tak rovna 3, kód dokáže opravit jednu chybu a odhalit až dvě chyby. Rychlost přenosu informace kódem D je 1/2, což je další vylepšení.

Může kód se čtyřmi informačními symboly opravovat jednu chybu a současně přenášet informaci rychlostí větší než 1/2? Ukážeme si tvrzení, které ukazuje, že by to mohlo jít ještě o něco rychleji.

Tvrzení 5.104. *Předpokládejme, že kód délky n má r informačních symbolů a $n-r$ kontrolních symbolů. Pokud opravuje jednu chybu, musí platit*

$$\frac{2^n}{n+1} \geq 2^r.$$

Důkaz. Kód C délky n, který má r informačních symbolů, musí obsahovat aspoň 2^r různých slov. Každá volba informačních symbolů musí vést k nějakému kódovému slovu, různé volby k různým slovům. Jinak by dekódování nebylo jednoznačné.

Využijeme geometrické představy kódu jako podmnožiny vrcholů Hammingovy krychle. Pro každý vektor $\mathbf{a} \in \mathbb{Z}_2^n$ nazveme 1-okolí slova $\mathbf{a}$ množinu

$$V_1(\mathbf{a}) = \{\mathbf{x} \in \mathbb{Z}_2^n; h(\mathbf{a}, \mathbf{x}) \leq 1\}.$$

Snadno nahlédneme, že 1-okolí každého vektoru $\mathbf{a}$ obsahuje přesně $n+1$ prvků.

Má-li kód C opravovat jednu chybu, musí být jeho minimální vzdálenost aspoň 3. To znamená, že pro libovolná dvě různá kódová slova $\mathbf{a}, \mathbf{b} \in C$ musí být jejich 1-okolí disjunktní. V opačném případě by totiž v důsledku trojúhelníkové nerovnosti pro Hammingovu vzdálenost platilo $h(\mathbf{a}, \mathbf{b}) \leq 2$, což je spor s tím, že minimální vzdálenost kódu je aspoň 3.

Sjednotíme-li všechna 1-okolí všech slov $\mathbf{a} \in C$, bude mít toto sjednocení aspoň $2^r(n+1)$ prvků. Tento počet musí být menší nebo rovný počtu všech prvků (vrcholů Hammingovy krychle) $\mathbb{Z}_2^n$, tj. 2^n. Odtud po snadné úpravě vyplývá dokazovaná nerovnost. □

Analogickou nerovnost můžeme dokázat pro kódy, které opravují d chyb, podrobnosti ve cvičeních.

Pro $r = 4$ a $n = 6$ platí $2^4 \cdot 7 > 2^6$, kód délky 6 se čtyřmi informačními symboly, který by opravoval jednu chybu proto neexistuje.

V případě $n = 7$ platí rovnost $2^4 \cdot 8 = 2^7$, existence kódu délky 7 se čtyřmi informačními symboly, který opravuje jednu chybu, tak vyloučena není. Všimněme si, že pokud by takový kód $C \subseteq \mathbb{Z}_2^7$ existoval, platila by rovnost

$$\mathbb{Z}_2^7 = \bigcup_{\mathbf{a} \in C} V_1(\mathbf{a}).$$

To znamená, že pro takový kód by každý vrchol Hammingovy krychle $\mathbb{Z}_2^7$ měl vzdálenost 1 od nějakého (jednoznačně určeného) kódového slova $\mathbf{a}$. Všechny vrcholy Hammingovy krychle $\mathbb{Z}_2^7$ by tak byly pokryté 1-okolími kódových slov. Takový kód by byl optimální v tom smyslu, že množina $\mathbb{Z}_2^7$ by neobsahovala žádná "zbytečná"slova, každé ze slov délky 7 by se vyskytovalo ve vzdálenosti nejvýše 1 od nějakého kódového slova.

Definice 5.105. Kód délky n, který má r informačních symbolů a opravuje jednu chybu, se nazývá *perfektní kód*, pokud platí rovnost

$$2^r(n+1) = 2^n.$$

Jako poslední příklad kódu si ukážeme perfektní lineární $(7,4)$-kód, který opravuje jednu chybu.

Příklad 5.106. Kód H_3 definujeme pomocí kontrolní matice

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

Prvky C jsou prvky jádra $\mathrm{Ker}\,(A)$ matice A. Tato matice je v řádkově odstupňovaném tvaru, její hodnost se tedy rovná 3, a dimenze kódu $H_3 = \mathrm{Ker}\,(A)$ je tedy rovna 4. Platí-li $A\mathbf{x}^T = \mathbf{o}^T$ pro $\mathbf{x} = x_1x_2\cdots x_7$, jsou neznámé x_4, x_5, x_6, x_7 volné, můžeme je zvolit libovolně a považujeme je za informační symboly. Neznámé x_1, x_2, x_3 jsou volbou x_4, x_5, x_6, x_7 určené jednoznačně:

$$x_1 = x_4 + x_5 + x_7,\ x_2 = x_4 + x_6 + x_7,\ x_3 = x_5 + x_6 + x_7.$$

Neznámé x_1, x_2, x_3 jsou tedy kontrolní (paritní) bity. I tento kód H_3 je založen na kombinací tří paritních kontrol.

Sloupce matice A tvoří všechny nenulové vektory z prostoru Z_2^3. Každá dvouprvková podposloupnost sloupců matice A je tedy lineárně nezávislá a minimální vzdálenost kódu C je tak aspoň 3, (ve skutečnosti je právě 3), a kód H_3 tak opravuje jednu chybu.

Jak najdeme kódové slovo $x_1x_2\cdots x_7$, jsou-li dány informační symboly x_4, x_5, x_6, x_7, jsme si už řekli. Pokud přijímající strana přijme slovo $\mathbf{y} = y_1y_2\cdots y_7$, spočítá součin $A\mathbf{y}^T$. Platí-li $A\mathbf{y}^T = \mathbf{o}^T$, je $\mathbf{y}$ kódové slovo a bylo tedy přeneseno bez chyby.

Je-li $A\mathbf{y}^T \neq \mathbf{o}^T$, došlo během přenosu k chybě a zbývá určit, který symbol v přijatém slově $\mathbf{y} = y_1 y_2 \cdots y_7$ je ten poškozený. Označme $A\mathbf{y}^T = (s_1 s_2 s_3)^T$.

Protože matice A obsahuje všechny nenulové vektory $\mathbb{Z}_2^3$ jako sloupce, existuje jednoznačně určený sloupec $A_{*j} = (s_1 s_2 s_3)^T$. Platí $A_{*j} = A\mathbf{e}_j^T$ pro j-tý vektor $\mathbf{e}_j$ standardní báze v $\mathbb{Z}_2^7$. Slovo $\mathbf{y} + \mathbf{e}_j$ se od $\mathbf{y}$ liší pouze v j-tém symbolu. Platí navíc

$$A(\mathbf{y}^T + \mathbf{e}_j^T) = A\mathbf{y}^T + A\mathbf{e}_j^T = (s_1 s_2 s_3)^T + A_{*j} = (s_1 s_2 s_3)^T + (s_1 s_2 s_3)^T = \mathbf{o}^T.$$

Slovo $\mathbf{y} + \mathbf{e}_j$ tak patří do kódu H_3 a má Hammingovu vzdálenost 1 od přijatého slova $\mathbf{y}$. Je to tedy to slovo, které bylo vysláno a při přenosu byl poškozen j-tý symbol.

Příklad 5.107. Při použití Hammingova kódu H_3 bylo přijato slovo 1010101. Došlo během přenosu k chybě a pokud ano, jaké slovo bylo vysláno?

Vynásobíme kontrolní matici A vektorem $(1010101)^T$. Dostaneme

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

Vektor $(0,1,1)^T$ je šestý sloupcový vektor matice A_3, poškozen byl tedy šestý symbol ve slově 1010101, vysláno bylo slovo 1010111.

Definice 5.108. *Hammingův kód* H_r je binární blokový kód délky $n = 2^r - 1$ určený kontrolní maticí typu $r \times n$, jejíž sloupce tvoří všechny nenulové aritmetické vektory dimenze r nad $\mathbb{Z}_2$.

Detaily důkazu následujícího tvrzení přenecháme do cvičení.

Tvrzení 5.109. *Hammingův kód H_r je perfektní lineární kód délky $2^r - 1$ a dimenze $2^r - r - 1$, jehož minimální vzdálenost je 3.*

Cvičení

1. Vysvětlete, proč množina všech polynomů stupně právě 173 s reálnými koeficienty s běžnými operacemi sčítání polynomů a násobení polynomu reálným číslem není vektorovým prostorem.

2. Pro libovolné těleso $\mathbf{T}$ a libovolnou množinu X definujeme vektorový prostor $\mathbf{T}^{(X)}$ jako množinu těch zobrazení f z X do T, pro který je množina $\{x : f(x) \neq 0\}$ je konečná. Sčítání a násobení definujeme po souřadnicích, tj. $(f+g)(x) = f(x)+g(x)$ a $(af)(x) = af(x)$. Dokažte, že $\mathbf{T}^{(X)}$ je vektorový prostor.

Tímto způsobem bychom zobecnili definici 5.2 na případ nekonečné dimenze – prostor $\mathbf{T}^{(X)}$ může být nazýván aritmetickým vektorovým prostorem nad $\mathbf{T}$ dimenze $|X|$.

3. U všech příkladů vektorových prostorů za definicí ověřte, že se skutečně jedná o vektorové prostory.

4. $\mathbb{Q}(\sqrt{2})$ DOKONCIT

5. Množina všech podmnožin množiny $\{1, 2, 3, \ldots, n\}$ (nebo jiné dané množiny X) spolu s operací symetrické diference, tj. $A + B = (A \setminus B) \cup (B \setminus A)$, je vektorový prostor nad $\mathbb{Z}_2$. (Násobení skalárem je jednoznačně dané axiomy.) Dokažte a vysvětlete, proč je tento prostor „v podstatě“ $\mathbb{Z}_2^n$.

6. Dokažte tvrzení 5.4 a formulujte a dokažte obdoby vlastností (8) a (9) z tvrzení 3.3.

7. Dokažte, že $\mathbf{T}$ jako vektorový prostor nad $\mathbf{T}$ má pouze triviální podprostory.

8. Dokažte, že jedinými netriviálními podprostory prostoru $\mathbf{T}^2$ jsou množinu tvaru $\{t\mathbf{x} : t \in T\}$, kde $\mathbf{o} \neq \mathbf{x} \in \mathbf{T}^2$.

9. Nechť A je matice nad $\mathbf{T}$ typu $m \times n$ a $\mathbf{b} \in T^m$. Dokažte, že množina $\{\mathbf{x} : A\mathbf{x} = \mathbf{b}\}$ je podprostorem $\mathbf{T}^n$ právě tehdy, když $\mathbf{b} = \mathbf{o}$.

10. Zjistěte lineární obal množiny X z příkladu 5.18 a dokažte, že množina Y tvoří podprostor.

11. Dokažte, že posloupnost vektorů $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ ve vektorovém prostoru $\mathbf{V}$ nad $\mathbf{T}$ je lineárně nezávislá právě tehdy, když žádný z vektorů není v lineárním obalu předchozích (tj. pro každé i platí $\mathbf{v}_i \notin \langle \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{i-1} \rangle$).

12. Dokažte, že sloupce matice v řádkově odstupňovaném tvaru jsou lineárně nezávislé právě tehdy, když příslušná homogenní soustava nemá žádné volné proměnné.

13. Dokončete příklad 5.44 o Fibonacciho posloupnostech.

14. Dokažte, že sloupce (řádky) čtvercové matice A nad $\mathbf{T}$ řádu n tvoří bázi $\mathbf{T}^n$ právě tehdy, když A je regulární.

15. Dokažte:

- Dimenze prostoru všech matic nad $\mathbf{T}$ typu $m \times n$ je mn.
- Dimenze prostoru reálných polynomů stupně nejvýše n je n.
- Dimenze prostoru $\mathbb{C}$ jako vektorového prostoru nad $\mathbb{R}$ je 2.

16. Najděte bázi podprostoru $\mathbb{R}^\omega$ tvořeného posloupnostmi $(a_1, a_2, \dots)$, pro které platí $a_n = 2a_{n-1} - a_{n-2}$ (pro každé $n \geq 3$). Pomocí nalezené báze najděte vzorec pro výpočet a_n, když $a_1 = 3$, $a_2 = 7$.

17. Dokažte, že z každé množiny generátorů konečně generovaného prostoru lze vybrat bázi.

18. Dokažte, že důsledek 5.54 platí bez předpokladu konečnosti G. Předpoklad tedy změníme na „G je množina generátorů konečně generovaného prostoru $\mathbf{V}$“.

19. Spočítejte počet všech různých bází $\mathbf{V}$ vybraných z vektorů $\mathbf{v}_1, \dots, \mathbf{v}_5$ z příkladu 5.56.

20. Dokažte druhou část tvrzení 5.64.

21. Dokažte, že bázové sloupce tvoří bázi sloupcového prostoru matice.

22. Přímo z definice bázových sloupců dokažte, že řešení $\mathbf{x} = (x_1, x_2, \dots, x_n) \in T^n$ soustavy $A\mathbf{x} = \mathbf{b}$ je jednoznačně určeno vektorem $(x_{i_1}, x_{i_2}, \dots, x_{i_k}) \in T^k$, kde $i_1, i_2, \dots, i_k$ je seznam nebázových sloupců matice A, a naopak, že každý vektor $(x_{i_1}, x_{i_2}, \dots, x_{i_k})$ v T^k vzniká z nějakého řešení $(x_1, x_2, \dots, x_n)$.

23. Dokažte, že pro libovolné tři podprostory $\mathbf{V}_1, \mathbf{V}_2, \mathbf{V}_3$ prostoru $\mathbf{V}$ platí

$$(V_1 + V_2) + V_3 = V_1 + (V_2 + V_3) \ .$$

24. Dokažte, že

$$V_1 + V_2 + \cdots + V_k = \{v_1 + v_2 + \cdots + v_k : v_1 \in V_1, v_2 \in V_2, \dots, v_k \in V_k\} \ .$$

25. Nechť $\mathbf{V}_i, i \in I$ jsou podprostory vektorového prostoru $\mathbf{W}$ a G_i je množina generátorů prostoru $\mathbf{V}_i$ pro každé $i \in I$. Dokažte, že $\bigcup_{i\in I} G_i$ generuje $\bigvee_{i\in I} \mathbf{V}_i$.

26. Najděte podprostory $\mathbf{U}, \mathbf{V}, \mathbf{W}$ prostoru $\mathbb{R}^3$ takové, že $\mathbf{U}\cap(\mathbf{V}+\mathbf{W}) \neq (\mathbf{U}\cap\mathbf{V})+(\mathbf{U}\cap\mathbf{W})$, $\mathbf{U}+(\mathbf{V}\cap\mathbf{W}) \neq (\mathbf{U}+\mathbf{V})\cap(\mathbf{U}+\mathbf{W})$.

27. Jedna inkluze v obou (neplatných) distributivních zákonech vždy platí. Zjistěte které a dokažte.

28. Dokažte, že rovnosti v distributivních zákonech platí za předpokladu $\mathbf{U} \leq \mathbf{W}$ nebo $\mathbf{W} \leq \mathbf{U}$.

29. Rozhodněte, zda pro podprostory $\mathbf{U}, \mathbf{V}, \mathbf{W}$ vektorového prostoru $\mathbf{Z}$ platí

$$\begin{aligned}\dim(\mathbf{U}) + \dim(\mathbf{V}) + \dim(\mathbf{W}) = \dim(\mathbf{U}+\mathbf{V}+\mathbf{W}) + \dim(\mathbf{U}\cap\mathbf{V}) + \dim(\mathbf{V}\cap\mathbf{W}) + \\ + \dim(\mathbf{U}\cap\mathbf{W}) - \dim(\mathbf{U}\cap\mathbf{V}\cap\mathbf{W})\end{aligned}$$

30. Jakou dimenzi může mít průnik podprostoru dimenze 3 a podprostoru dimenze 4 v $\mathbb{Z}_{37}^6$? Pro každou z možností uveďte příklad.

31. Při komunikaci byl použit Hammingův kód H_3. Přijímající strana přijala slova

$$0101011, 0011111, 1011100, 1111110, 011111, 0001110, 1100101.$$

Rozhodněte, která z nich byla během přenosu poškozena a u každého z poškozených slov rozhodněte, který ze symbolů byl přenesen nesprávně a jaké slovo bylo vysláno.

32. Dokažte Tvrzení 5.109.

33. Definujeme d-okolí slova $\mathbf{a} \in \mathbb{Z}_2^n$ jako množinu

$$V_d(\mathbf{a}) = \{\mathbf{x} \in \mathbb{Z}_2^n; h(\mathbf{x}, \mathbf{a}) \leq d\}.$$

Dokažte, že počet prvků $V_d(\mathbf{a})$ se rovná

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{d} = \sum_{i=1}^{d} \binom{n}{i}.$$

34. Dokažte, že je-li C kód dimenze n s r informačními symboly, který opravuje d chyb, pak platí nerovnost

$$2^r\left(\binom{n}{0} + \binom{n}{1} + \cdots \binom{n}{d}\right) \leq 2^n.$$

35. Hamming svůj lineární $(7, 4)$-kód D definoval pomocí kontrolní matice

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

Pokud bylo přijaté slovo $\mathbf{y}$ a $B\mathbf{y}^T = (s_1 s_2 s_3)^T \neq \mathbf{o}^T$, dokažte že $s_3 s_2 s_1$ je binární vyjádření indexu poškozeného symbolu.

36. Dokažte, že existuje permutace π na množině $\{1, 2, \dots, 7\}$ taková, že platí $a_1 a_2 \cdots a_7 \in H_3$ právě když $a_{\pi(1)} a_{\pi(2)} \cdots a_{\pi(7)} \in D$, kde D je kód z předchozího cvičení. Jak souvisí permutace π s permutací sloupců, pomocí které dostaneme z kontrolní matice A kódu H_3 kontrolní matici B kódu D.

6. Determinant

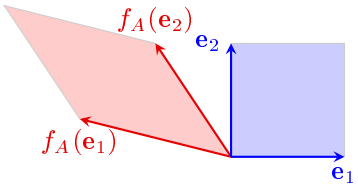
Cíl. *Budeme se věnovat pojmu determinantu matice. Motivací je porozumění, jak zobrazení určené maticí mění obsah (v $\mathbb{R}^2$) a objem (v $\mathbb{R}^3$). K definici budeme potřebovat permutace, naučíme se je různými způsoby zapisovat a určovat znaménko.*

6.1. **Motivace.** Čtvercová matice A řádu n nad $\mathbb{R}$ určuje zobrazení $f_A : \mathbb{R}^n \to \mathbb{R}^n$. Tato zobrazení mají tu vlastnost, že násobí n-dimenzionální objemy (obsahy v případě $n = 2$, objemy v případě $n = 3$) konstantním číslem. Toto číslo je rovno absolutní hodnotě tzv. determinantu, který zavedeme v této kapitole. Znaménko determinantu určuje, zda zobrazení mění „orientaci prostoru“. Například pokud je determinant matice A řádu 2 rovný 1,3, příslušné zobrazení násobí obsah každého útvaru číslem 1,3 a nemění orientaci. To, že se orientace nemění si lze představit tak, že obraz lze dostat spojitou deformací roviny z původního útvaru. Pokud je determinant A rovný $-1{,}3$, pak zobrazení násobí obsah každého útvaru číslem 1,3 a orientaci mění.

$A = I_2$ $\qquad$ $\det A = 1{,}3$ $\qquad$ $\det A = -1{,}3$

Odvodíme si vzorec na výpočet determinantu v případě reálných čtvercových matic řádu $n = 2$ a $n = 3$. V obecné definici pro větší n a nad jinými tělesy vizuální představa chybí, ale determinant můžeme definovat stejně a bude mít podobné vlastnosti.

6.1.1. *Determinant v $\mathbb{R}^2$.* Budeme se snažit odvodit vzorec pro determinant čtvercových matic A řádu 2. Matici se sloupci $\mathbf{u}$, $\mathbf{v}$ budeme značit $(\mathbf{u}|\mathbf{v})$ a její determinant $\det(\mathbf{u}|\mathbf{v})$. Číslo $\det(A)$, kde $A = (\mathbf{u}|\mathbf{v})$, má vyjadřovat změnu obsahu a orientace při zobrazení f_A. Protože zobrazení f_A zobrazuje vektor $\mathbf{e}_1 = (1, 0)^T$ na vektor $A\mathbf{e}_1 = \mathbf{u}$ a vektor $\mathbf{e}_2 = (0, 1)^T$ na vektor $A\mathbf{e}_2 = \mathbf{v}$, f_A zobrazuje jednotkový čtverec se stranami $\mathbf{e}_1, \mathbf{e}_2$ na rovnoběžník se stranami $\mathbf{u}$, $\mathbf{v}$.



Obsah tohoto rovnoběžníku můžeme vyjádřit vhodným doplněním na obdélník a znaménko určit diskuzí možné vzájemné polohy vektorů $\mathbf{u}$ a $\mathbf{v}$ podle obrázku (viz cvičení).

OBRAZEK

Podíváme se na jiný postup, který se nám rovněž bude hodit v obecnější situaci.

Když vynásobíme jeden z vektorů číslem $t \in \mathbb{R}$, pak se obsah výsledného rovnoběžníku zvětší (nebo zmenší) $|t|$-krát. Přitom orientace se pro kladné t nezmění a pro záporná t změní. Dostáváme vztahy

$$\det(t\mathbf{u}|\mathbf{v}) = t\det(\mathbf{u}|\mathbf{v}) = \det(\mathbf{u}|t\mathbf{v}) \quad .$$

OBRAZEK (zvetseni rovnobezniku)

Z následujícího obrázku můžeme nahlédnout (stačí přesunout trojúhelník ...), že platí

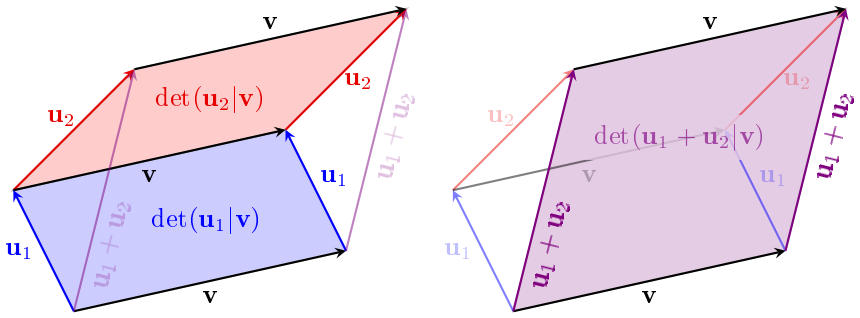
$$\det(\mathbf{u}_1 + \mathbf{u}_2|\mathbf{v}) = \det(\mathbf{u}_1|\mathbf{v}) + \det(\mathbf{u}_2|\mathbf{v})$$

a podobný vztah platí, když součet je v druhém sloupci.

$$\det(\mathbf{u}|\mathbf{v}_1 + \mathbf{v}_2) = \det(\mathbf{u}|\mathbf{v}_1) + \det(\mathbf{u}|\mathbf{v}_2)$$

Ještě si uvědomíme, že

$$\det(\mathbf{e}_1, \mathbf{e}_2) = 1, \quad \det(\mathbf{e}_2, \mathbf{e}_1) = -1 \quad , \quad \det(\mathbf{e}_1, \mathbf{e}_1) = \det(\mathbf{e}_2, \mathbf{e}_2) = 0$$



protože první matice odpovídá identickému zobrazení, které nemění obsah ani orientaci, druhá matice odpovídá překlopení kolem osy prvního kvadrantu, která nemění obsah a mění orientaci, třetí a čtvrtá matice odpovídá zobrazení, která čtverci přiřadí „zdegenerovaný rovnoběžník“ – úsečku.

Z odvozených vztahů již jde spočítat determinant obecné matice

$$A = (\mathbf{u}|\mathbf{v}) = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} .$$

$$\begin{aligned} \det(A) &= \det(\mathbf{u}|\mathbf{v}) = \det(a_{11}\mathbf{e}_1 + a_{21}\mathbf{e}_2 | a_{12}\mathbf{e}_1 + a_{22}\mathbf{e}_2) \\ &= \det(a_{11}\mathbf{e}_1 | a_{12}\mathbf{e}_1 + a_{22}\mathbf{e}_2) + \det(a_{21}\mathbf{e}_2 | a_{12}\mathbf{e}_1 + a_{22}\mathbf{e}_2) = \\ &= \det(a_{11}\mathbf{e}_1 | a_{12}\mathbf{e}_1) + \det(a_{11}\mathbf{e}_1 | a_{22}\mathbf{e}_2) + \\ &\quad + \det(a_{21}\mathbf{e}_2 | a_{12}\mathbf{e}_1) + \det(a_{21}\mathbf{e}_2 | a_{22}\mathbf{e}_2) = \\ &= a_{11}a_{12}\det(\mathbf{e}_1|\mathbf{e}_1) + a_{11}a_{22}\det(\mathbf{e}_1|\mathbf{e}_2) + \\ &\quad + a_{21}a_{12}\det(\mathbf{e}_2|\mathbf{e}_1) + a_{21}a_{22}\det(\mathbf{e}_2|\mathbf{e}_2) = \\ &= a_{11}a_{22} - a_{21}a_{12} \end{aligned}$$

Determinant jsme odvodili použitím jednotkového čtverce. Obecně obsah a orientace obrazu libovolného útvaru (u nějž lze měřit obsah) se změní tak, jak udává determinant. Tento fakt nebudeme odvozovat.

6.1.2. *Determinant v* $\mathbb{R}^3$. Pro matice řádu 3 udává determinant změnu objemu a orientace. Pro zobrazení f_A určené maticí $A = (\mathbf{u}|\mathbf{v}|\mathbf{w})$ je obrazem jednotkové krychle se stranami $\mathbf{e}_1$, $\mathbf{e}_2$, $\mathbf{e}_3$ rovnoběžnostěn se stranami $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w}$. Z geometrického náhledu dostáváme podobné vztahy jako v případě $\mathbb{R}^2$.

$$\det(t\mathbf{u}|\mathbf{v}|\mathbf{w}) = \det(\mathbf{u}|t\mathbf{v}|\mathbf{w}) = \det(\mathbf{u}|\mathbf{v}|t\mathbf{w}) = \det(\mathbf{u}|\mathbf{v}|\mathbf{w})$$

$$\det(\mathbf{u}_1 + \mathbf{u}_2 + \mathbf{u}_3|\mathbf{v}|\mathbf{w}) = \det(\mathbf{u}_1|\mathbf{v}|\mathbf{w}) + \det(\mathbf{u}_2|\mathbf{v}|\mathbf{w}) + \det(\mathbf{u}_3|\mathbf{v}|\mathbf{w})$$

Podobný vztah platí, když součet je ve druhém nebo třetím sloupci.

K výpočtu ještě potřebujeme determinanty matic, jejichž sloupce jsou vektory v kanonické bázi. Pokud jsou dva ze sloupců stejné, pak příslušné zobrazení degeneruje krychli na čtverec, nebo dokonce úsečku, takže determinant je 0. Dále

$$\det(\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3) = \det(\mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_1) = \det(\mathbf{e}_3, \mathbf{e}_1, \mathbf{e}_2) \quad ,$$

protože příslušná zobrazení jsou rotace, které orientaci nemění. Zbývají tři matice, jejichž determinant je -1, protože příslušná zobrazení jsou zrcadlení a ta orientaci mění.

$$\det(\mathbf{e}_1, \mathbf{e}_3, \mathbf{e}_2) = \det(\mathbf{e}_2, \mathbf{e}_1, \mathbf{e}_3) = \det(\mathbf{e}_3, \mathbf{e}_2, \mathbf{e}_1) \quad ,$$

Determinant teď můžeme spočítat jako v případě $n = 2$, výrazy ale budou poněkud delší.

$$A = (\mathbf{u}|\mathbf{v}|\mathbf{w}) = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} .$$

$$\begin{aligned}\det(A) &= \det(\mathbf{u}|\mathbf{v}|\mathbf{w}) = \\ &= \det(a_{11}\mathbf{e}_1 + a_{21}\mathbf{e}_2 + a_{31}\mathbf{e}_3 | a_{12}\mathbf{e}_1 + a_{22}\mathbf{e}_2 + a_{32}\mathbf{e}_3 | a_{13}\mathbf{e}_1 + a_{23}\mathbf{e}_2 + a_{33}\mathbf{e}_3) \\ &= \sum_{k=1}^{3}\sum_{l=1}^{3}\sum_{m=1}^{3} a_{k1}a_{l2}a_{m3}\det(\mathbf{e}_k, \mathbf{e}_l, \mathbf{e}_m) = \\ &= a_{11}a_{22}a_{33}\det(\mathbf{e}_1,\mathbf{e}_2,\mathbf{e}_3) + a_{11}a_{32}a_{23}\det(\mathbf{e}_1,\mathbf{e}_3,\mathbf{e}_2) + \\ &\quad + a_{21}a_{12}a_{33}\det(\mathbf{e}_2,\mathbf{e}_1,\mathbf{e}_3) + a_{21}a_{32}a_{13}\det(\mathbf{e}_2,\mathbf{e}_3,\mathbf{e}_1) + \\ &\quad + a_{31}a_{12}a_{23}\det(\mathbf{e}_3,\mathbf{e}_1,\mathbf{e}_2) + a_{31}a_{22}a_{13}\det(\mathbf{e}_3,\mathbf{e}_2,\mathbf{e}_1) = \\ &= a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} + a_{31}a_{12}a_{23} - a_{11}a_{32}a_{23} - a_{31}a_{22}a_{13} - a_{21}a_{12}a_{33}\end{aligned}$$

Každý sčítanec je součinem třech prvků matice $a_{k1}a_{l2}a_{m3}$, kde k,l,m jsou navzájem různé, se znaménkem odpovídajícím orientaci trojice $\mathbf{e}_k, \mathbf{e}_l, \mathbf{e}_m$. Jeden sčítanec tedy odpovídá výběru jednoho prvku s prvního sloupce, jednoho prvku z druhého sloupce a jednoho prvku z třetího sloupce, kde prvky vybíráme s navzájem různých řádků (ostatní členy budou nulové).

6.2. **Permutace.** Výpočet vzorce pro „vícerozměrný objem“ by probíhal podobně. Museli bychom zjistit, která pořadí vektorů kanonické báze odpovídají kladné orientaci a která záporné. To lze pomocí pojmu znaménka permutace, které definujeme v této části. Děláme tím malý výlet z lineární algebry do algebry obecné.

Permutaci definujeme jako bijekci množiny na sebe samu.

Definice 6.1. *Permutací* množiny X rozumíme bijekci $X \to X$. Množinu všech permutací na množině X značíme S_X. Pro množinu permutací na množině $X = \{1, 2, \dots, n\}$, kde n je přirozené číslo, také používáme značení S_n.

Nejčastěji budeme používat permutace na konečné množině, konkrétně množině $\{1, 2, \dots, n\}$. Pro konečnou množinu X je každé prosté zobrazení $X \to X$ již bijekcí, a také každé zobrazení $X \to X$ na je bijekcí. (Připomeňme, že ani jedna z těchto implikací není pravdivá pro nekonečné množiny.)

Význačnou permutací na X je identické zobrazení $\mathrm{id}_X : X \to X$, pro něž $\mathrm{id}_X(x) = x$ pro každé $x \in X$. Protože inverzní zobrazení k bijekci je bijekce, je inverzní zobrazení π^{-1} k permutaci π na X opět permutace na X. Složením permutací je rovněž permutace. Složení permutací ρ a σ značíme $\sigma \circ \rho$ nebo $\sigma\rho$, tj. $\sigma\rho(x) = \sigma(\rho(x))$. Množina S_X spolu s těmito operacemi opět splňuje vlastnosti podobné sčítání v tělese, nebo sčítání ve vektorovém prostoru, **s výjimkou komutativity**:

(1) Pro libovolné $\pi, \rho, \sigma \in S_X$ platí $\pi(\rho\sigma) = (\pi\rho)\sigma$.
(2) Pro libovolné $\pi \in S_X$ platí $\mathrm{id}_X\,\pi = \pi\,\mathrm{id}_X = \pi$.
(3) Pro libovolné $\pi \in S_X$ platí $\pi\pi^{-1} = \pi^{-1}\pi = \mathrm{id}_X$.

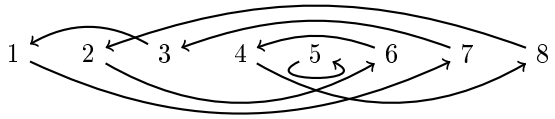
Tím pádem nemusíme při skládání psát závorky a také můžeme řešit jednoduché rovnice typu $\alpha\rho\beta = \gamma$, kde α, β, γ jsou dané permutace, podobným způsobem jako pro čísla, akorát musíme dát pozor na nekomutativitu.

6.2.1. *Zápis permutace.* Permutaci π na konečné množině X můžeme zapsat tabulkou, kdy do horního řádku napíšeme v nějakém pořadí prvky množiny X a pod každý prvek $x \in X$ napíšeme jeho obraz $\pi(x)$. Například permutaci $\pi \in S_8$ danou vztahy $\pi(1) = 7$, $\pi(2) = 6$, $\pi(3) = 1$, $\pi(4) = 8$, $\pi(5) = 5$, $\pi(6) = 4$, $\pi(7) = 3$, $\pi(8) = 2$ můžeme zapsat

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 6 & 1 & 8 & 5 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 6 & 4 & 7 & 2 & 8 & 1 & 3 & 5 \\ 4 & 8 & 3 & 6 & 2 & 7 & 1 & 5 \end{pmatrix}.$$

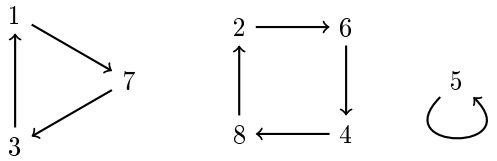
Tabulkou můžeme zapsat libovolné zobrazení z X do X (nebo i do jiné množiny). To, že π je permutace, se v tabulce projeví tak, že v druhém řádku bude každý prvek množiny X právě jednou.

Další možností je si permutaci nakreslit. Prvky X si nakreslíme jako body (tzv. vrcholy) a pro každé $x \in X$ si nakreslíme šipku (tzv. hranu) z x do $\pi(x)$. Takovému obrázku říkáme *graf* permutace π. Protože π je zobrazení, vede z každého bodu právě jedna šipka, a protože je to bijekce, vede do každého bodu právě jedna šipka.



Obrázek 6. Obrázek permutace

Když graf trochu překreslíme, vidíme, že permutace je sjednocením nezávislých cyklů.



OBRÁZEK 7. Lepší obrázek permutace

To není náhoda, každá permutace je složením nezávislých cyklů.

Definice 6.2. *Cyklus délky k* je permutace na X splňující $\pi(x_1) = x_2$, $\pi(x_2) = x_3$, ..., $\pi(x_{k-1}) = x_k$, $\pi(x_k) = x_1$ a $\pi(y) = y$ pro každé $y \in X \setminus \{x_1, x_2, \ldots, x_k\}$, kde x_1, x_2, ..., x_k jsou po dvou různé prvky X. Zapisujeme $\pi = (x_1\ x_2\ \ldots\ x_k)$.

Cykly nazýváme *nezávislé*, pokud jsou množiny prvků vyskytující se v cyklech disjunktní.

Transpozice je cyklus délky 2, tj. permutace tvaru $\pi = (x\ y)$.

Všimněte si, že pořadí prvků v cyklu můžeme cyklicky otočit a dostaneme stejnou permutaci:

$$(x_1\ x_2\ \ldots\ x_k) = (x_2\ \ldots\ x_k\ x_1) = \cdots = (x_k\ x_1\ x_2\ \ldots\ x_{k-1})$$

Jak najít pro danou permutaci π rozklad na nezávislé cykly aniž bychom kreslili obrázek? Zvolíme libovolný výchozí prvek x_1 a podíváme se na jeho obraz $x_2 = \pi(x_1)$, pak se podíváme na jeho obraz $x_3 = \pi(x_2)$, atd. Když poprvé narazíme na prvek, který se již vyskytl, tj. $x_{k+1} = x_i$ pro nějaké $i \leq k$, pak nutně $i = 1$, jinak by π zobrazovala dva různé prvky x_{i-1} a x_k na stejný prvek x_i. Takže máme $\pi(x_k) = x_1$ a můžeme cyklus uzavřít. Pokud jsou v množině X ještě jiné prvky, vybereme kterýkoliv z nich a nalezneme další cykly. Tyto cykly musí být nezávislé, jinak bychom opět měli dva prvky, které se zobrazí do stejného prvku, a zobrazení π by nebylo prosté. Naznačili jsme důkaz, že rozklad na nezávislé cykly je možný. Pořadí skládání nezávislých cyklů můžeme libovolně měnit (na rozdíl od obecných cyklů) a až na tuto skutečnost je rozklad jednoznačný. Detaily si rozmyslete jako cvičení.

Tvrzení 6.3. *Každou permutaci na konečné množině X lze zapsat jako složení nezávislých cyklů. Tento zápis je jednoznačný až na pořadí cyklů (a cykly délky 1).*

Příklad 6.4. Podle návodu rozložíme naší permutaci π na nezávislé cykly. Začneme například s prvkem 1. Jeho obraz je $\pi(1) = 7$, obraz 7 je $\pi(7) = 3$ a obraz 3 je $\pi(3) = 1$. Nalezli jsme první cyklus (1 7 3). Nyní vezmeme nějaký prvek, který se doposud neobjevil, třeba 2. Spočítáme $\pi(2) = 6$, $\pi(6) = 4$, $\pi(4) = 8$, $\pi(8) = 2$ a nalezli jsme další cyklus (2 6 4 8). Zbývá prvek 5, který je *pevným bodem*, tj. $\pi(5) = 5$, což můžeme zapsat cyklem (5) délky 1 (to je identická permutace), chceme-li tento fakt zdůraznit. Celkově tedy máme

$$\pi = (1\ 7\ 3)(2\ 6\ 4\ 8)\ .$$

Pořadí skládání můžeme díky nezávislosti prohodit a rovněž můžeme v tomto zápisu cyklicky otáčet prvky v závorkách, protože tím vznikají pouze různé zápisy stejné permutace. Takže například také

$$\pi = (6\ 4\ 8\ 2)(3\ 1\ 7)\ .$$

Cyklickým zápisem rozumíme rozumíme zápis pomocí nezávislých cyklů s vyznačenými pevnými body, například

$$\pi = (1\ 7\ 3)(2\ 6\ 4\ 8)(5)\ .$$

Pokud pevné body neuvádíme, hovoříme o *redukovaném cyklickém zápisu.*

Cyklický (nebo redukovaný cyklický) zápis je většinou daleko výhodnější než zápis tabulkou, protože lépe vidíme, co permutace „dělá“. Zápis tabulkou budeme dále používat jen zřídka.

Na příkladu si rozmyslíme, jak permutace invertovat a skládat v cyklickém zápisu.

Příklad 6.5. Inverzní permutace přiřadí každému prvku jeho vzor. Pro permutaci $\pi = (1\ 7\ 3)(2\ 6\ 4\ 8)$ je například $\pi^{-1}(3) = 7$, protože $\pi(7) = 3$. Stačí tedy převrátit pořadí prvků v cyklu. Na obrázku bychom otočili směr šipek.

$$\pi^{-1} = (1\ 3\ 7)(2\ 8\ 4\ 6)$$

Na tomto místě si rovněž uvědomme, že inverzní permutace k transpozici je tatáž transpozice.

$$(i\ j)^{-1} = (i\ j)\ (\ = (j\ i)\ )$$

Vypočítáme složení permutace π a permutace $\rho = (1\ 7\ 4\ 6)(2\ 8)(3\ 5)$:

$$\rho\pi = (1\ 7\ 4\ 6)(2\ 8)(3\ 5)(1\ 7\ 3)(2\ 6\ 4\ 8) = (1\ 4\ 2)(3\ 7\ 5)$$

Cyklový zápis tvoříme jako pro samotnou permutaci: vyjdeme z libovolného prvku, podíváme se, kam ho složená permutace zobrazí a takto pokračujeme. Vyšli jsme z prvku 1, permutace π ho zobrazí na 3 a permutace ρ prvek 3 zobrazí na 5, takže složená permutace $\rho\pi$ zobrazí prvek 1 na prvek 5, tj. za 1 napíšeme číslo 5. Číslo 5 permutace π zobrazí na 5 a permutace ρ zobrazí číslo 5 na 3, takže píšeme 3, atd.

Ještě jednou připomeňme, že skládání komutativní není (ale třeba nezávislé cykly spolu komutují). Složením ρ a π vyjde permutace

$$\pi\rho = (1\ 3\ 5)(6\ 7\ 8)\ ,$$

což je jiná permutace než $\pi\rho$. Má ale stejnou strukturu – má stejně jako $\rho\pi$ jeden dva cykly délky 3. To není náhoda, viz cvičení.

Každý cyklus lze zapsat jako složení transpozic, například

$$(x_1\ x_2\ \dots\ x_k) = (x_1\ x_2)(x_2\ x_3)\dots(x_{k-1}\ x_k)$$

nebo

$$(x_1\ x_2\ \dots\ x_k) = (x_1\ x_k)\dots(x_1\ x_3)(x_1\ x_2)\ .$$

Ověřte obě rovnosti! Protože každá permutace je složením cyklů (dokonce nezávislých), můžeme každou permutaci napsat jako složení transpozic. Dokázali jsme

Tvrzení 6.6. *Každá permutace na konečné množině je složením transpozic.*

Tvrzení vlastně říká, že jakkoliv promícháme prvky množiny, lze původní uspořádání dostat postupným prohazováním dvojic. Zápis permutace jako složení transpozic není samozřejmě jednoznačný, například

$$(1\ 2\ 3) = (1\ 3)(1\ 2) = (1\ 2)(2\ 3) = (1\ 2)(2\ 3)(1\ 2)(1\ 2) = (1\ 2)(1\ 3)(2\ 3)(1\ 2) = \dots$$

6.2.2. *Znaménko.* I když každou permutaci můžeme zapsat jako složení transpozic mnoha způsoby, parita počtu transpozic (tj. zda je počet sudý nebo lichý) se nemění. K důkazu tohoto tvrzení si nejdřív všimneme jak se mění počet cyklů v cyklovém zápisu při složení s transpozicí. V následujícím tvrzení počítáme i cykly délky jedna.

Tvrzení 6.7. *Nechť X je konečná množina, $\pi \in S_X$ a $(x\ y) \in S_X$. Pak počet cyklů v permutaci $(x\ y)\pi$ a π se liší o 1 a počet sudých cyklů v permutaci $(x\ y)\pi$ a π se rovněž liší o 1.*

Důkaz. Rozebereme dva případy. Nejprve předpokládejme, že x a y leží ve stejném cyklu ($x = x_1\ x_2\ \dots\ x_k\ y = y_1\ y_2\ \dots\ y_l$) permutace π. Pak

$$(x\ y)\pi = (x\ y)\dots(x\ x_2\ \dots\ x_k\ y\ y_2\ \dots\ y_l)\dots = \dots(x\ x_2\ \dots\ x_k)(y\ y_2\ \dots\ y_l)\dots\ ,$$

kde ostatní cykly permutace π zůstanou beze změny. Počet cyklů se v tomto případě zvýší o 1. Rozborem případů dostaneme druhou část tvrzení (například pokud k i l je sudé, pak se počet sudých cyklů zvětší o jedna, pokud k je sudé a l je liché, pak se počet sudých cyklů také zvětší o jedna, atd.).

Pokud jsou prvky x a y v různých cyklech ($x = x_1\ x_2\ \dots\ x_k$), ($y = y_1\ y_2\ \dots\ y_l$), pak

$$(x\ y)\pi = (x\ y)\dots(x\ x_2\ \dots\ x_k)(y\ y_2\ \dots\ y_l)\dots = \dots(x\ x_2\ \dots\ x_k\ y\ y_2\ \dots\ y_l)\dots\ ,$$

takže se počet cyklů sníží o 1. Druhou část získáme opět rozborem případů. □

Důsledkem je, že parita počtu transpozic je stejná v libovolném zápisu permutace jako složení transpozic. Tuto paritu navíc poznáme podle počtu cyklů sudé délky v cyklickém zápisu permutace.

Důsledek 6.8. *Pro libovolnou permutaci π na konečné množině X nastane jedna z následujících možností:*

(1) *Každý zápis π jako složení transpozic obsahuje sudý počet transpozic. To nastane právě tehdy, když počet cyklů sudé délky v (redukovaném) cyklickém zápisu permutace π je sudý.*
(2) *Každý zápis π jako složení transpozic obsahuje lichý počet transpozic. To nastane právě tehdy, když počet cyklů sudé délky v (redukovaném) cyklickém zápisu permutace π je lichý.*

Důkaz. Je-li π složením transpozic $\rho_1\rho_2\dots\rho_k$, pak několikanásobnou aplikací předchozího tvrzení dostaneme, že parita počtu cyklů sudé délky v permutaci π je rovná paritě k: Počet cyklů sudé délky v permutaci ρ_k je lichý (jeden cyklus délky 2), v permutaci $\rho_{k-1}\rho_k$ je sudý, atd. □

Tento důsledek nám umožňuje zavést znaménko permutace.

Definice 6.9. Permutace π na konečné množině X se nazývá *sudá*, pokud nastane možnost (1) v důsledku 6.8. Rovněž říkáme, že *znaménko* π *je* 1 a píšeme $\operatorname{sgn}(\pi) = 1$.

V opačném případě je π *lichá*, má znaménko -1 a definujeme $\operatorname{sgn}(\pi) = -1$.

Znaménko snadno vypočteme z (redukovaného) cyklického zápisu. Stačí spočítat počet cyklů sudé délky. Znaménko lze také určit podle počtu všech cyklů v cyklickém zápisu, viz cvičení.

Příklad 6.10.

$$\operatorname{sgn}\left((1\ 2\ 3\ 4)(5\ 6\ 7)(8\ 9)(10\ 11)\right) = -1$$

protože má permutace v cyklickém zápisu 3 cykly sudé délky.

Znaménko inverzní permutace a složené permutace je určené znaménkem původních permutací.

Tvrzení 6.11. *Nechť X je konečná množina a $\pi, \rho \in S_X$. Pak platí*

(1) $\operatorname{sgn}(\mathrm{id}_X) = 1$,
(2) $\operatorname{sgn}(\pi^{-1}) = \operatorname{sgn}(\pi)$ *a*
(3) $\operatorname{sgn}(\pi\rho) = \operatorname{sgn}(\pi)\operatorname{sgn}(\rho)$.

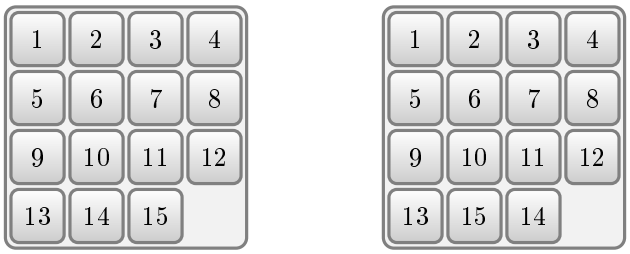
Důkaz.

(1) Identická permutace má 0 cyklů sudé délky.
(2) Inverzní permutace má stejný počet cyklů sudé délky.
(3) Pokud π lze zapsat jako složení k transpozic, tj. $\operatorname{sgn}(\pi) = (-1)^k$, a ρ lze zapsat jako složení l transpozic, tj. $\operatorname{sgn}(\rho) = (-1)^l$, pak $\pi\rho$ lze zapsat jako složení $k + l$ transpozic, tj. $\operatorname{sgn}(\pi\rho) = (-1)^{k+l} = (-1)^k(-1)^l = \operatorname{sgn}(\pi)\operatorname{sgn}(\rho)$.

□

Slovy, identická permutace je sudá, inverzní permutace k sudé (resp. liché) je sudá (resp. lichá), složením dvou sudých nebo dvou lichých permutací je sudá permutace a složením liché a sudé permutace v libovolném pořadí je lichá permutace.

Příklad 6.12. Ve hře „15“ máme čtvercovou krabičku se 4×4 políčky, v níž jsou kostičky číslované 1 až 15 a jedno prázdné políčko, pomocí něhož jdou kostičky vodorovně nebo svisle přesouvat. Ukážeme, že základní pozici na obrázku vlevo nelze získat z pozice na obrázku vpravo.



Obrázek 8. Hra 15

Místa v krabičce si očíslujeme podle základní pozice. Místo vpravo dole očíslujeme 16. Libovolnou pozici zapíšeme pomocí permutace $\pi \in S_{16}$ tak, že definujeme $\pi(i) = j$, pokud se na místě i nalézá kostička s číslem j. Jeden tah je vlastně prohozením umístění prázdného políčka a nějaké kostičky $i \in \{1, 2, \ldots, 15\}$. Nová pozice tedy odpovídá permutaci $(16\ i)\pi$.

Budeme si všímat parity permutace π a parity pozice prázdného políčka. Na začátku vyjdeme z pozice odpovídající liché permutaci (14 15) a prázdné políčko je na sudém místě 16. Po provedení jednoho tahu permutace π změní paritu a rovněž se změní parita pozice prázdného políčka, protože sudá místa sousedí pouze s lichými a naopak. Z toho plyne, že

- po provedení sudého počtu tahů bude π lichá a prázdné políčko bude na sudém místě;
- po provedení lichého počtu tahů bude π sudá a prázdné políčko bude na lichém místě.

Ani v jednom z obou případů nemůžeme získat základní pozici, pro kterou je permutace π sudá (je to identická permutace) a prázdné políčko je na sudém místě (16).

6.2.3. *Počet permutací.* Jak již asi víte, počet permutací na n-prvkové množině $X = \{x_1, x_2, \dots, x_n\}$ je $n!$. Máme totiž n možností, kam zobrazit x_1, pak $n-1$ možností, kam zobrazit x_2, atd. Dohromady $n(n-1)\dots 1 = n!$.

Počet lichých permutací spočítáme z následujícího pozorování, které také použijeme pro důkazy tvrzení o determinantech.

Tvrzení 6.13. *Nechť X je konečná množina a $\pi \in S_X$. Pak platí:*

(1) *Soubor $(\rho^{-1} : \rho \in S_X)$, soubor $(\pi\rho : \rho \in S_X)$ i soubor $(\rho\pi : \rho \in S_X)$ obsahuje každou permutaci v S_X právě jednou.*
(2) *Pokud π je lichá, pak soubor $(\pi\rho : \rho \in S_X, \operatorname{sgn}(\rho) = 1)$ i soubor $(\rho\pi : \rho \in S_X, \operatorname{sgn}(\rho) = 1)$ obsahuje pouze liché permutace v S_X, každou právě jednou.*

Důkaz. Rovnice $\sigma = \rho^{-1}$ má pro dané σ právě jedno řešení $\rho = \sigma^{-1}$. (Rozmyslete si podrobně toto i další tvrzení použitá v tomto důkazu. Zdůvodnění je podobné jako v tvrzení 3.3 o vlastnostech těles.) To znamená, že každou permutaci σ lze zapsat ve tvaru ρ^{-1} právě jedním způsobem, tj. soubor $(\rho^{-1} : \rho \in S_X)$ obsahuje každou permutaci v S_X právě jednou.

Rovnice $\sigma = \pi\rho$ má pro dané σ a π právě jedno řešení $\rho = \pi^{-1}\sigma$. Z toho plyne, že v souboru $(\pi\rho : \rho \in S_X)$ je každá permutace právě jednou. Podobně pro třetí soubor v části (1). Pokud jsou permutace σ a π liché, pak $\rho = \pi^{-1}\sigma$ je sudá, protože $\operatorname{sgn}(\pi^{-1}\sigma) = \operatorname{sgn}(\pi^{-1})\operatorname{sgn}(\sigma) = \operatorname{sgn}(\pi)\operatorname{sgn}(\sigma) = (-1)(-1) = 1$ (viz tvrzení 6.11). Každou lichou permutaci lze tedy zapsat ve tvaru $\pi\rho$, kde ρ je sudá, právě jedním způsobem. Navíc $\pi\rho$ je lichá, pokud π je lichá a ρ je sudá. Z toho plyne první část bodu (2). Druhá část se dokáže podobně. □

Tvrzení můžeme formulovat v jazyku zobrazení. Například druhá část tvrzení v bodě (1) říká, že zobrazení $f : S_X \to S_X$ definované $f(\rho) = \pi\rho$ je bijekce. První část bodu (2) říká, že je-li π lichá, pak zobrazení f definované stejným předpisem je bijekcí z množiny všech sudých permutací v S_X na množinu všech lichých permutací v S_X.

Důsledkem je, že počet lichých permutací na n-prvkové množině X je stejný jako počet sudých permutací na X, kdykoliv na X nějaká lichá permutace existuje, tj. v případě $n > 1$. Pro $n > 1$ je tedy počet lichých i sudých permutací $n!/2$.

6.3. **Definice determinantu a základní vlastnosti.** Připomeňme, že determinant reálné čtvercové matice $A = (\mathbf{u}|\mathbf{v}|\mathbf{w})$ řádu 3 určuje, jak zobrazení f_A mění objem a orientaci. Jeho absolutní hodnota je rovna objemu rovnoběžnostěnu o stranách $\mathbf{u}, \mathbf{v}, \mathbf{w}$. Odvodili jsme vzorec

$$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} =$$
$$= a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} + a_{31}a_{12}a_{23} - a_{11}a_{32}a_{23} - a_{31}a_{22}a_{13} - a_{21}a_{12}a_{33} \ .$$

Každý člen součtu je součin třech prvků $a_{k1}a_{l2}a_{m3}$, kde k, l, m jsou navzájem různé, a znaménko udává orientaci trojice vektorů $(\mathbf{e}_k, \mathbf{e}_l, \mathbf{e}_m)$. Každý člen lze tedy zapsat jako $a_{\pi(1)1}a_{\pi(2)2}a_{\pi(3)3}$, kde $\pi \in S_3$ je permutace $\pi(1) = k$, $\pi(2) = l$, $\pi(3) = m$ a všimněte si, že znaménko členu je rovno znaménku permutace π. To geometricky odpovídá tomu, že prohodíme-li dva vektory kanonické báze, orientace se změní.

6.3.1. *Definice.* Podobně definujeme determinant libovolné **čtvercové** matice nad libovolným tělesem.

Definice 6.14. Je-li $A = (a_{ij})$ čtvercová matice nad tělesem $\mathbf{T}$ řádu n, pak definujeme *determinant* matice A předpisem

$$\det(A) = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) a_{\pi(1),1}a_{\pi(2),2}\dots a_{\pi(n),n} \ .$$

Determinant tedy přiřadí čtvercové matici nad $\mathbf{T}$ prvek tělesa $\mathbf{T}$. Součet má $n!$ členů, jeden pro každou permutaci $\pi \in S_n$. Sčítanec odpovídající permutaci π je součinem n prvků matice, z každého sloupce i obsahuje součin prvek $a_{\pi(i),i}$, znaménko sčítance je rovné znaménku permutace π. (Pro přehlednost oddělujeme indexy prvků matice čárkou.)

Pro determinant matice A se také užívá značení $|A|$.

Příklad 6.15. V případě $n = 2$ máme dvě permutace v S_2 – identickou permutaci a transpozici (1 2). Identická permutace je sudá a odpovídající sčítanec je $a_{11}a_{22}$, transpozice je lichá a odpovídající sčítanec je $-a_{21}a_{12}$. Dostáváme stejný vzorec jako dříve:

$$\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{21}a_{12}$$

OBRAZEK (diagonaly)

Například

$$\begin{vmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{vmatrix} = \cos^2(\alpha) + \sin^2(\alpha) = 1 \ ,$$

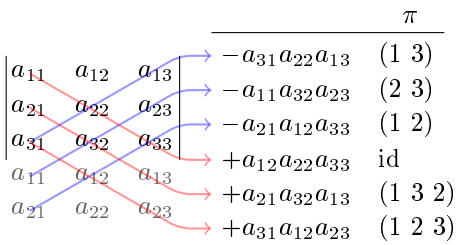
což není překvapivé, protože rotace o α nemění ani obsah ani orientaci.

(Při zápisu determinantu pomocí svislých čar vynecháváme kulaté závorky.)

Příklad 6.16. V případě $n = 3$ máme šest permutací v S_3 – identické permutace a trojcykly jsou sudé, transpozice jsou liché. Odpovídající sčítanci jsou:

π	
id	$a_{11}a_{22}a_{33}$
(1 2 3)	$a_{21}a_{32}a_{13}$
(1 3 2)	$a_{31}a_{12}a_{23}$
(2 3)	$-a_{11}a_{32}a_{23}$
(1 3)	$-a_{31}a_{22}a_{13}$
(1 2)	$-a_{21}a_{12}a_{33}$

a opět dostáváme vzorec odvozený výše. Mnemotechnickou pomůckou je tzv. *Sarrusovo pravidlo* na obrázku.



Obrázek 9. Sarrusovo pravidlo

Počítat matice z definice není vhodné už pro matice řádu 3, je lepší využít jiné metody. Sarrusovo pravidlo tedy nebudeme používat. V případě $n = 4$ má již výraz 24 členů (vypište je jako cvičení) a definice je pro výpočet již zcela nevhodná. Všimněte si, že **pravidlo podobné Sarrusovu pro matice řádu $n > 3$ neplatí**.

6.3.2. *Základní vlastnosti.* Pro horní trojúhelníkové matice vypočítáme determinant jako součin prvků na diagonále.

Tvrzení 6.17. *Je-li A horní trojúhelníková matice, pak* $\det(A) = a_{11}a_{22}\dots a_{nn}$.

Důkaz. Podívejme se na jeden sčítanec $\operatorname{sgn}(\pi)a_{\pi(1),1}a_{\pi(2),2}\dots a_{\pi(n),n}$ v definici determinantu. Pokud je jeden z činitelů v tomto součinu nulový, celý sčítanec je roven nule a můžeme jej ignorovat. První sloupec matice A je celý nulový, až na hodnotu a_{11}, která může být nenulová. Pokud tedy $\pi(1) > 1$, pak $a_{\pi(1),1} = 0$ a sčítanec je nulový. Předpokládejme proto $\pi(1) = 1$. Podobně, pokud $\pi(2) > 2$ můžeme na sčítanec zapomenout, protože $a_{\pi(2),2} = 0$. Takže můžeme předpokládat $\pi(2) \leq 2$. Ale $\pi(2)$ nemůže být 1, protože máme $\pi(1) = 1$ a π je prosté zobrazení, čili $\pi(2) = 2$. Postupně dostáváme $\pi(3) = 3$, $\pi(4) = 4$, …, $\pi(n) = n$.

Jediný možná nenulový sčítanec tedy odpovídá identické permutaci, ta je sudá, takže $\det A = a_{11}a_{22}\dots a_{nn}$. □

Pro matice 2×2 nad $\mathbb{R}$ je geometrické vysvětlení na obrázku **??**. Rovnoběžník o stranách $(a_{11}, 0)^T$, $(a_{21}, a_{22})^T$ má stejný obsah jako obdélník o stranách $(a_{11}, 0)^T$ a $(0, a_{22})^T$, protože oba rovnoběžníky mají stejnou výšku. Také mají stejnou orientaci.

OBRAZEK

Podobně bychom mohli dokázat, že determinant dolní trojúhelníkové matice je součin prvků na diagonále. Dělat to ale nebudeme, dokážem obecněji, že determinant se nezmění transponováním.

Tvrzení 6.18. *Pro libovolnou čtvercovou matici A platí* $\det(A) = \det\left(A^T\right)$.

Důkaz. Sčítanec v definici $\det\left(A^T\right)$ odpovídající permutaci π je

$$\operatorname{sgn}(\pi)a_{1,\pi(1)}a_{2,\pi(2)}\dots a_{n,\pi(n)} \ .$$

Součin lze přeuspořádat na

$$\operatorname{sgn}(\pi)a_{\pi^{-1}(1),1}a_{\pi^{-1}(2),2}\dots a_{\pi^{-1}(n),n} \ ,$$

protože $\pi^{-1}(i)$-tý činitel v původním součinu je roven $a_{\pi^{-1}(i)\pi(\pi^{-1}(i))} = a_{\pi^{-1}(i),i}$. Tento činitel jsme přesunuli na i-té místo. Máme

$$\begin{aligned}
\det\left(A^T\right) &= \sum_{\pi\in S_n} \operatorname{sgn}(\pi) a_{1,\pi(1)} a_{2,\pi(2)} \dots a_{n,\pi(n)} \\
&= \sum_{\pi\in S_n} \operatorname{sgn}(\pi) a_{\pi^{-1}(1),1} a_{\pi^{-1}(2),2} \dots a_{\pi^{-1}(n),n} \\
&= \sum_{\pi\in S_n} \operatorname{sgn}(\pi^{-1}) a_{\pi^{-1}(1),1} a_{\pi^{-1}(2),2} \dots a_{\pi^{-1}(n),n} \\
&= \sum_{\pi\in S_n,\ \rho=\pi^{-1}} \operatorname{sgn}(\rho) a_{\rho(1),1} a_{\rho(2),2} \dots a_{\rho(n),n} \\
&= \sum_{\rho\in S_n} \operatorname{sgn}(\rho) a_{\rho(1),1} a_{\rho(2),2} \dots a_{\rho(n),n} = \det(A) \quad .
\end{aligned}$$

Ve třetí úpravě jsme použili vztah $\operatorname{sgn}(\pi^{-1}) = \operatorname{sgn}(\pi)$ (viz tvrzení 6.11) a v páté úpravě jsme začali sčítat přes inverzy permutací, což výsledek nezmění, protože soubor $(\pi^{-1} : \pi \in S_n)$ obsahuje všechny permutace v S_n právě jednou (viz tvrzení 6.13). □

Dokázané tvrzení jinými slovy říká, že

$$\det(A) = \sum_{\pi\in S_n} \operatorname{sgn}(\pi) a_{1,\pi(1)} a_{2,\pi(2)} \dots a_{n,\pi(n)} \quad ,$$

což je trochu tradičnější verze definice.

Tvrzení se hodí se k tomu, že věty, které dokážeme pro řádky, budeme moci použít i pro sloupce.

Teď dokážeme vlastnosti determinantu použité při odvození vzorců v dimenzi 2 a 3 nad $\mathbb{R}$, jsou to body (1) a (2) v následujícím tvrzení. Zároveň spočítáme, jak se mění determinant při elementárních sloupcových úpravách, to jsou body (2), (3) a (4).

Tvrzení 6.19. *Nechť* $\mathbf{T}$ *je těleso,* $n \in \mathbb{N}$, $i, j \in \{1, 2, \dots, n\}$, $i \neq j$, $\mathbf{u}$, $\mathbf{v}_1$, $\mathbf{v}_2$, …, $\mathbf{v}_n \in T^n$, $t \in T$ *a* $\rho \in S_n$. *Pak platí.*

(1) $\det(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_{i-1}|\ \mathbf{v}_i + \mathbf{u}\ |\mathbf{v}_{i+1}|\dots|\mathbf{v}_n)$
$= \det(\mathbf{v}_1|\dots|\mathbf{v}_{i-1}|\ \mathbf{v}_i\ |\mathbf{v}_{i+1}|\dots|\mathbf{v}_n) + \det(\mathbf{v}_1|\dots|\mathbf{v}_{i-1}|\ \mathbf{u}\ |\mathbf{v}_{i+1}|\dots|\mathbf{v}_n)$
(2) $\det(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_{i-1}|\ t\mathbf{v}_i\ |\mathbf{v}_{i+1}|\dots|\mathbf{v}_n) = t\ \det(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_n)$
(3) $\det\left(\mathbf{v}_{\rho(1)}|\mathbf{v}_{\rho(2)}|\dots|\mathbf{v}_{\rho(n)}\right) = \operatorname{sgn}(\rho)\det(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_n)$
(4) $\det(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_{i-1}|\mathbf{v}_i + t\mathbf{v}_j|\mathbf{v}_{i+1}|\dots|\mathbf{v}_n) = \det(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_n)$

Důkaz. Označíme $A = (a_{ij}) = (\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_n)$, čili a_{ij} je i-tá složka vektoru $\mathbf{v}_j$.

(1) Označíme-li $\mathbf{u} = (b_1, b_2, \dots, b_n)$, platí

$$\begin{aligned}
&\det(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_{i-1}|\ \mathbf{v}_i + \mathbf{u}\ |\mathbf{v}_{i+1}|\dots|\mathbf{v}_n) \\
&= \sum_{\pi\in S_n} \operatorname{sgn}(\pi) a_{\pi(1),1} a_{\pi(2),2} \dots a_{\pi(i-1),i-1} (a_{\pi(i),i} + b_{\pi(i)}) a_{\pi(i+1),i+1} \dots a_{\pi(n),n} \\
&= \sum_{\pi\in S_n} (\operatorname{sgn}(\pi) a_{\pi(1),1} a_{\pi(2),2} \dots a_{\pi(n),n} + \\
&\qquad + \operatorname{sgn}(\pi) a_{\pi(1),1} a_{\pi(2),2} \dots a_{\pi(i-1),i-1} b_{\pi(i)} a_{\pi(i+1),i+1} \dots a_{\pi(n),n}) \\
&= \sum_{\pi\in S_n} \operatorname{sgn}(\pi) a_{\pi(1),1} a_{\pi(2),2} \dots a_{\pi(n),n} \\
&\qquad + \sum_{\pi\in S_n} \operatorname{sgn}(\pi) a_{\pi(1),1} a_{\pi(2),2} \dots a_{\pi(i-1),i-1} b_{\pi(i)} a_{\pi(i+1),i+1} \dots a_{\pi(n),n} \\
&= \det(\mathbf{v}_1|\dots|\mathbf{v}_{i-1}|\ \mathbf{v}_i\ |\mathbf{v}_{i+1}|\dots|\mathbf{v}_n) + \det(\mathbf{v}_1|\dots|\mathbf{v}_{i-1}|\ \mathbf{u}\ |\mathbf{v}_{i+1}|\dots|\mathbf{v}_n) \quad .
\end{aligned}$$

V úpravách jsme roznásobili závorku a rozdělili sumu na dvě části.

(2) K důkazu tohoto bodu stačí vytknout t před sumu:

$$\begin{aligned}
&\det\left(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_{i-1}|\ t\mathbf{v}_i\ |\mathbf{v}_{i+1}|\dots|\mathbf{v}_n\right)\\
&=\sum_{\pi\in S_n}\operatorname{sgn}(\pi)a_{\pi(1),1}a_{\pi(2),2}\dots a_{\pi(i-1),i-1}(ta_{\pi(i),i})a_{\pi(i+1),i+1}\dots a_{\pi(n),n}\\
&=t\sum_{\pi\in S_n}\operatorname{sgn}(\pi)a_{\pi(1),1}a_{\pi(2),2}\dots a_{\pi(n),n}\\
&=t\ \det\left(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_n\right)\ .
\end{aligned}$$

(3) Uvědomíme si, že prvek na místě (i,j) v matici $(\mathbf{v}_{\rho(1)}|\mathbf{v}_{\rho(2)}|\dots|\mathbf{v}_{\rho(n)})$ je $a_{i,\rho(j)}$. K rozepsání determinantu použijeme alternativní definici.

$$\begin{aligned}
&\det\left(\mathbf{v}_{\rho(1)}|\mathbf{v}_{\rho(2)}|\dots|\mathbf{v}_{\rho(n)}\right)\\
&=\sum_{\pi\in S_n}\operatorname{sgn}(\pi)a_{1,\rho(\pi(1))}a_{2,\rho(\pi(2))}\dots a_{n,\rho(\pi(n))}\\
&=\sum_{\pi\in S_n}\operatorname{sgn}(\rho)\operatorname{sgn}(\rho\pi)a_{1,\rho\pi(1)}a_{2,\rho\pi(2)}\dots a_{n,\rho\pi(n)}\\
&=\operatorname{sgn}(\rho)\sum_{\pi\in S_n}\operatorname{sgn}(\rho\pi)a_{1,\rho\pi(1)}a_{2,\rho\pi(2)}\dots a_{n,\rho\pi(n)}\\
&=\operatorname{sgn}(\rho)\sum_{\pi\in S_n,\sigma=\rho\pi}\operatorname{sgn}(\sigma)a_{1,\sigma(1)}a_{2,\sigma(2)}\dots a_{n,\sigma(n)}\\
&=\operatorname{sgn}(\rho)\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)a_{1,\sigma(1)}a_{2,\sigma(2)}\dots a_{n,\sigma(n)}\\
&=\operatorname{sgn}(\rho)\det\left(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_n\right)
\end{aligned}$$

V předposlední úpravě jsme začali sčítat přes permutace $\sigma=\pi\rho$ místo π, což výsledek nezmění, protože soubor $(\rho\pi:\pi\in S_n)$ obsahuje všechny permutace v S_n právě jednou (viz tvrzení 6.13).

(4) Nejprve dokážeme pomocné tvrzení: Determinant matice $B=(b_{kl})$ řádu n, která má dva sloupce i,j $(i\neq j)$ stejné, je nula.

Pro většinu těles bychom mohli použít předchozí bod: Protože (i,j) je lichá permutace a prohozením sloupců i a j se matice nezmění, platí $\det(B)=-\det(B)$. Bohužel z toho plyne $\det(B)=0$ pouze pro tělesa charakteristiky různé od 2. Proto obecně musíme postupovat jinak. V sumě

$$\det(B)=\sum_{\pi\in S_n}b_{1,\pi(1)}b_{2,\pi(2)}\dots b_{n,\pi(n)}$$

k sobě seskupíme pro každou sudou permutaci π sčítanec odpovídající π a sčítanec odpovídající permutaci $(i\ j)\pi$. Toto seskupení můžeme provést a vyčerpáme jím všechny sčítance, protože soubor $((i\ j)\pi:\pi\in S_n,\operatorname{sgn}(\pi)=1)$ obsahuje všechny liché permutace v S_n právě jednou (viz tvrzení 6.13). Dostaneme

$$\begin{aligned}
\det(B)=&\sum_{\pi\in S_n,\operatorname{sgn}(\pi)=1}(\operatorname{sgn}(\pi)b_{1,\pi(1)}b_{2,\pi(2)}\dots b_{n,\pi(n)}+\\
&\qquad+\operatorname{sgn}((i\ j)\pi)b_{1,(i\ j)\pi(1)}b_{2,(i\ j)\pi(2)}\dots b_{n,(i\ j)\pi(n)})\\
=&\sum_{\pi\in S_n,\operatorname{sgn}(\pi)=1}(\operatorname{sgn}(\pi)b_{1,\pi(1)}b_{2,\pi(2)}\dots b_{n,\pi(n)}-\\
&\qquad-\operatorname{sgn}(\pi)b_{1,\pi(1)}b_{2,\pi(2)}\dots b_{n,\pi(n)})\\
=&\,0\ ,
\end{aligned}$$

kde jsme použili $\operatorname{sgn}((i\ j)\pi)=-\operatorname{sgn}(\pi)$ a fakt, že B má shodný i-tý a j-tý sloupec.

Tím jsem dokázali pomocné tvrzení a důkaz čtvrtého bodu snadno dokončíme užitím předchozích.

$$\begin{aligned}
&\det\left(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_{i-1}|\mathbf{v}_i+t\mathbf{v}_j|\mathbf{v}_{i+1}|\dots|\mathbf{v}_n\right)\\
&=\det\left(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_n\right)+\det\left(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_{i-1}|\ t\mathbf{v}_j\ |\mathbf{v}_{i+1}|\dots|\mathbf{v}_n\right)\\
&=\det\left(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_n\right)+t\det\left(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_{i-1}|\ \mathbf{v}_j\ |\mathbf{v}_{i+1}|\dots|\mathbf{v}_n\right)\\
&=\det\left(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_n\right)
\end{aligned}$$

□

Protože determinant matice se shoduje s determinantem transponované matice (tvrzení 6.18), podobné tvrzení můžeme formulovat pro řádky. Bod (2) říká, že vynásobíme-li některý sloupec (nebo řádek) prvkem $t \in T$, determinant se zvětší t-krát. Další bod ukazuje, že prohodíme-li sloupce (řádky) podle nějaké permutace π, pak determinant nanejvýš změní znaménko, a to v případě, že π je lichá. Speciálně, pokud prohodíme dva sloupce (řádky), determinant změní znaménko. Poslední bod můžeme formulovat tak, že přičteme-li t-násobek některého sloupce (resp. řádku) k jinému sloupci (resp. řádku), determinant se nezmění.

Protože víme, jak spočítat determinant horní (dolní) trojúhelníkové matice (tvrzení 6.17), můžeme k výpočtu determinantu obecné matice použít Gaussovu eliminaci. Přitom si můžeme pomoci také sloupcovými úpravami.

Geometricky jsme si již zdůvodnili vlastnosti (1) a (2) v případě $\mathbf{T} = \mathbb{R}$ a $n = 2, 3$. Prohození dvou sloupců odpovídá zrcadlení podle přímky nebo roviny, takže determinant změní znaménko. To odůvodňuje (3). Následující obrázek vysvětluje čtvrtou vlastnost pro $n = 2$. Přičteme-li k jednomu z vektorů násobek druhého, příslušný rovnoběžníky budou mít stejnou jednu ze stran a stejnou výšku na tuto stranu jako původní rovnoběžník.

OBRAZEK

Příklad 6.20. Spočítáme determinant reálné matice

$$A = \begin{pmatrix} 2 & 4 & 2 \\ 7 & -1 & 4 \\ 5 & 0 & -6 \end{pmatrix} .$$

V prvních dvou úpravách vynásobíme pro pohodlí poslední sloupec číslem $1/2$ a prohodíme první a třetí sloupec, abychom dostali na pozici $(1,1)$ prvek 1. Dále budeme používat už jen řádkové úpravy. V jedné z nich vynásobíme druhý řádek číslem $1/3$. Musíme dát pozor na to, že prohazování a násobení determinant mění. Na násobení se můžeme v tomto kontextu dívat jako na vytýkání inverzního skaláru před determinant.

$$\begin{vmatrix} 2 & 4 & 2 \\ 7 & -1 & 4 \\ 5 & 0 & -6 \end{vmatrix} = 2 \cdot \begin{vmatrix} 2 & 4 & 1 \\ 7 & -1 & 2 \\ 5 & 0 & -3 \end{vmatrix} = -2 \cdot \begin{vmatrix} 1 & 4 & 2 \\ 2 & -1 & 7 \\ -3 & 0 & 5 \end{vmatrix}$$

$$= -2 \cdot \begin{vmatrix} 1 & 4 & 2 \\ 0 & -9 & 3 \\ 0 & 12 & 11 \end{vmatrix} = -2 \cdot 3 \cdot \begin{vmatrix} 1 & 4 & 2 \\ 0 & -3 & 1 \\ 0 & 12 & 11 \end{vmatrix} = -6 \cdot \begin{vmatrix} 1 & 4 & 2 \\ 0 & -3 & 1 \\ 0 & 0 & 15 \end{vmatrix}$$

$$= -6 \cdot 1 \cdot (-3) \cdot 15 = 270$$

Výpočet budeme umět provést šikovněji pomocí elementárních úprav kombinovaných s rozvojem.

Příklad 6.21. Prohozením sloupců spočítáme determinant reálné matice.

$$\begin{vmatrix} 2 & 1 & 3 & 5 \\ -3 & 8 & 0 & -2 \\ 7 & 5 & 0 & 0 \\ 4 & 0 & 0 & 0 \end{vmatrix} = \operatorname{sgn}((1\ 4\ 2\ 3)) \cdot \begin{vmatrix} 3 & 5 & 1 & 2 \\ 0 & -2 & 8 & -3 \\ 0 & 0 & 5 & 7 \\ 0 & 0 & 0 & 4 \end{vmatrix}$$

$$= \operatorname{sgn}((1\ 4\ 2\ 3)) \cdot 3 \cdot (-2) \cdot 5 \cdot 4 = 120$$

Provedli jsme prohození sloupců odpovídající permutaci $\rho = (1\ 4\ 2\ 3)$ – sloupec 1 jsme přesunuli na místo 4, sloupec 4 na místo 2, atd. Tato permutace je lichá. Alternativně bychom postupně mohli prohazovat sloupce po dvou.

6.3.3. *Další kriterium regularity.* Z tvrzení 6.19 můžeme odvodit další kriterium pro regulárnost matice: matice je regulární právě tehdy, když má nenulový determinant. Geometricky to pro reálné matice řádu 3 můžeme odůvodnit tak, že f_A nuluje objemy právě tehdy, když obraz $f_A(\mathbb{R}^3)$ je obsažen v nějaké rovině (tj. zobrazení zkolabuje prostor do roviny nebo dokonce přímky či bodu).

Tvrzení 6.22. *Čtvercová matice je regulární právě tehdy, když* $\det(A) \neq 0$.

Důkaz. Elementární řádkové úpravy sice determinant mění, ale nemění „nulovost“ determinantu: prohozením řádků determinant změní znaménko, vynásobením nenulovým číslem t se determinant zvětší t-krát a přičtení násobku nějakého řádku k jinému determinant nezmění. Takže označíme-li B odstupňovaný tvar matice A, pak $\det(A) = 0$ právě tehdy, když $\det(B) = 0$. Matice B je v horním trojúhelníkovém tvaru, takže $\det(B)$ je součinem prvků na diagonále (tvrzení 6.17). Tento součin je nulový právě tehdy, když má B nulový řádek, což se stane právě tehdy, když A je singulární podle bodu (5) věty 4.30 charakterizující regulární matice. □

Implikace zprava doleva zobecňuje fakt dokázaný v důkazu bodu (4), že determinant matice, která má dva sloupce stejné, je nulový.

Obecněji lze hodnost libovolné matice určit podle determinantů čtvercových podmatic.

Definice 6.23. *Minorem* řádu k matice A rozumíme determinant matice vzniklé z A výběrem k řádků a k sloupců.

Příklad 6.24. Jedním ze minorů řádu 2 matice

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{pmatrix}$$

je

$$\det(B) = \det \begin{pmatrix} 6 & 8 \\ 10 & 12 \end{pmatrix} .$$

Matice B vznikne z A výběrem řádků 2 a 3 a výběrem sloupců 2 a 4.

Tvrzení 6.25. *Hodnost libovolné matice A je rovna největšímu číslu r takovému, že existuje nenulový minor matice A řádu r.*

Důkaz. Pro odstupňovaný tvar se tvrzení nahlédne snadno a číslo r se řádkovými úpravami nemění. Detaily si rozmyslete jako cvičení. □

Například hodnost matice A je rovna 2 právě tehdy, když každý subdeterminant řádu 3 je nulový a existuje nenulový subdeterminant řádu 2.

6.3.4. *Determinant součinu.* Další aplikací tvrzení 6.19 je věta o determinantu součinu matic. K tomu si nejprve všimneme, jaké jsou determinanty elementárních matic:

- Matice odpovídající prohození dvou řádků má determinant -1, protože vznikne z jednotkové matice prohozením těchto řádků (můžeme použít například bod (3) z tvrzení na jednotkovou matici, nebo přímo definici).
- Matice odpovídající vynásobení nějakého řádku prvkem $t \in T$ má determinant t, například podle věty o determinantu horní trojúhelníkové matice, nebo podle bodu (2).
- Matice odpovídající přičtení t-násobku nějakého řádku k jinému má determinant 1, například opět podle věty o determinantu horní nebo dolní trojúhelníkové matice, nebo podle bodu (4).

Z bodů (2),(3),(4) nyní vyplývá, že pro libovolnou elementární matici E a libovolnou čtvercovou matici B stejného řádu platí $\det(EB) = \det(E)\det(B)$. Každá regulární matice R je součinem elementárních matic $R = E_1 E_2 \dots E_k$ (podle tvrzení 4.39), takže dostáváme

$$\begin{aligned} \det(RB) &= \det(E_1 E_2 \dots E_k B) = \det(E_1)\det(E_2 \dots E_k B) = \dots \\ &= \det(E_1)\det(E_2)\dots\det(E_k)\det(B) = \dots = \det(R)\det(B) \end{aligned}$$

Tento vztah platí i pro singulární matice R, tedy obecně platí, že determinant součinu je součin determinantů.

Věta 6.26 (věta o determinantu součinu)**.** *Pro libovolné matice A, B řádu n nad stejným tělesem platí* $\det(AB) = \det(A)\det(B)$.

Důkaz. Pro regulární matici A jsme větu dokázali. Pokud A je singulární, pak AB je rovněž singulární. To lze zdůvodnit například pomocí tvrzení 5.77 o hodnosti součinu: $\operatorname{rank}(AB) \leq \operatorname{rank}(A) < n$. Obě strany rovnosti jsou proto rovny nule. □

Věta má opět názorný geometrický význam. Pro reálné matice řádu tři udávají determinanty matic A, B koeficienty změny objemu a orientace pro zobrazení f_A, f_B. Matice AB odpovídá složenému zobrazení $f_A \circ f_B$, jeho koeficient změny objemu a orientace je zřejmě součinem těchto koeficientů pro matice A, B. Například, je-li $\det(A) = 2$ a $\det(B) = 3$, zobrazení f_B jakýkoliv útvar zvětší třikrát a f_A pak ještě dvakrát, takže dohromady se útvar zvětší šestkrát.

Pro součet podobná věta neplatí, například proto, že součet dvou singulárních matic může být regulární. Pro determinant inverzní matice dostaneme vzorec z věty o determinantu součinu.

Důsledek 6.27. *Je-li A regulární matice, pak* $\det\left(A^{-1}\right) = \det(A)^{-1}$.

Důkaz. Podle věty o determinantu součinu je

$$1 = \det(I) = \det\left(AA^{-1}\right) = \det(A)\det\left(A^{-1}\right) \quad ,$$

z čehož dostaneme vzorec vydělením $\det(A)$. (Determinant matice A je nenulový podle tvrzení 6.22.) □

6.3.5. *Cramerovo pravidlo.* Jako poslední aplikaci základních vlastností determinantu dokážeme *Cramerovo pravidlo* pro řešení soustav lineárních rovnic s regulární maticí.

Věta 6.28 (Cramerovo pravidlo)**.** *Nechť A je regulární matice řádu n a $j \in \{1,2,\dots,n\}$. Pak j-tá složka vektoru řešení $\mathbf{x} = (x_1, x_2, \dots, x_n)$ soustavy $A\mathbf{x} = \mathbf{b}$ je*

$$x_j = \frac{\det(A_j)}{\det(A)} \ ,$$

kde A_j je matice, která vznikne z A nahrazením j-tého sloupce vektorem $\mathbf{b}$, tj.

$$A_j = (A_{*1}|A_{*2}|\dots|A_{*(j-1)}|\mathbf{b}|A_{*(j+1)}|\dots|A_{*n}) \ .$$

Důkaz. Vztah $A\mathbf{x} = \mathbf{b}$ můžeme zapsat jako

$$x_1A_{*1} + x_2A_{*2} + \cdots + x_nA_{*n} = \mathbf{b} \ .$$

Dostáváme

$$\begin{aligned}
\det(A_j) &= \det\left(A_{*1}|A_{*2}|\dots|A_{*(j-1)}|\mathbf{b}|A_{*(j+1)}|\dots|A_{*n}\right) \\
&= \det\left(A_{*1}|A_{*2}|\dots|A_{*(j-1)}|\sum_{k=1}^{n} x_kA_{*k}|A_{*(j+1)}|\dots|A_{*n}\right) \\
&= \det\left(A_{*1}|A_{*2}|\dots|A_{*(j-1)}|x_jA_{*j}|A_{*(j+1)}|\dots|A_{*n}\right) \\
&= x_j\det\left(A_{*1}|A_{*2}|\dots|A_{*(j-1)}|A_{*j}|A_{*(j+1)}|\dots|A_{*n}\right) = x_j\det(A) \ ,
\end{aligned}$$

kde ve třetí úpravě jsme využili toho, že přičtením lineárním kombinace sloupců různých od j k sloupci j se determinant nezmění (to plyne z bodu (4) v tvrzení 6.19) a ve čtvrté úpravě jsme použili (2).

Z toho ihned vidíme dokazovaný vztah. □

Cramerovo pravidlo můžeme použít pouze pro regulární matice, tj. pro čtvercové matice s nenulovým determinantem (viz tvrzení 6.22). Spíše než pro praktické počítání se využívá ve výpočtech a úvahách, kdy se může hodit explicitní vzorec pro nějakou složku řešení.

Příklad 6.29. Vypočítáme třetí složku řešení soustavy $A\mathbf{x} = \mathbf{b}$ nad $\mathbb{Z}_5$.

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

Spočítáme determinant matice A.

$$\begin{vmatrix} 1 & 3 & 2 \\ 2 & 4 & 1 \\ 0 & 2 & 2 \end{vmatrix} = \begin{vmatrix} 1 & 3 & 2 \\ 0 & 3 & 2 \\ 0 & 2 & 2 \end{vmatrix} = \begin{vmatrix} 1 & 3 & 2 \\ 0 & 3 & 2 \\ 0 & 0 & 4 \end{vmatrix} = 2$$

Matice A je tedy regulární a můžeme použít Cramerovo pravidlo. Spočítáme ještě determinant matice A_3.

$$\begin{vmatrix} 1 & 3 & 0 \\ 2 & 4 & 2 \\ 0 & 2 & 4 \end{vmatrix} = \begin{vmatrix} 1 & 3 & 0 \\ 0 & 3 & 2 \\ 0 & 2 & 4 \end{vmatrix} = \begin{vmatrix} 1 & 3 & 0 \\ 0 & 3 & 2 \\ 0 & 0 & 1 \end{vmatrix} = 3$$

Třetí složka řešení je

$$x_3 = \frac{3}{2} = 4 \ .$$

6.4. **Rozvoj, adjungovaná matice.**

Vezmeme-li v definici všechny členy obsahující vybraný prvek a_{ij} a vytkneme jej, v závorce dostaneme tzv. *algebraický doplněk* prvku a_{ij}. Až na znaménko je roven determinantu matice, která vznikne vynecháním řádku a sloupce obsahující a_{ij}. To dokážeme ve větě o rozvoji podle sloupce. Nejprve potřebný pojem.

Definice 6.30. Nechť $A = (a_{ij})$ je čtvercová matice řádu n a $i,j \in \{1,2,\dots,n\}$. *Algebraickým doplňkem* (též *kofaktorem*) prvku a_{ij} matice A rozumíme skalár

$$A_{ij} = (-1)^{i+j}\det(M_{ij}) \ ,$$

kde M_{ij} je matice řádu $n-1$, která vznikne z A vynecháním i-tého řádku a j-tého sloupce.

Definice má smysl pro matice řádu $n > 1$. Pro matici řádu 1 definujeme $A_{11} = 1$. Tento případ je potřeba v některých tvrzeních této kapitoly rozebrat zvlášť, ale explicitně na to upozorňovat nebudeme.

Příklad 6.31. Algebraickým doplňkem prvku a_{12} v reálné matici

$$A = (a_{ij}) = \begin{pmatrix} 2 & 4 & 7 \\ 3 & -2 & -4 \\ 5 & 1 & -3 \end{pmatrix}$$

je

$$A_{12} = (-1)^{1+2} \begin{vmatrix} 3 & -4 \\ 5 & -3 \end{vmatrix} = (-1)(-9 - (-20)) = -11 \ .$$

Věta 6.32 (o rozvoji podle sloupce)**.** *Je-li A čtvercová matice řádu n a $j \in \{1, 2, \dots, n\}$, pak*

$$\det(A) = \sum_{i=1}^{n} a_{ij} A_{ij} = a_{1j}A_{1j} + a_{2j}A_{2j} + \cdots + a_{nj}A_{nj} \ .$$

Důkaz. Potřebujeme dokázat, že koeficient u a_{ij}, vytkneme-li tento prvek ze všech členů, které jej obsahují, je rovný A_{ij}. Pro pohodlnost zvolíme trochu jiný postup důkazu.

1. krok. Pokud $a_{nn} = 1$ a všechny ostatní prvky v n-tém sloupci jsou nulové, pak $\det(A) = A_{nn}$.

Platí

$$\begin{aligned} \det(A) &= \sum_{\pi \in S_n} \operatorname{sgn}(\pi) a_{\pi(1),1} a_{pi(2),2} \dots a_{\pi(n),n} \\ &= \sum_{\pi \in S_n, \pi(n)=n} \operatorname{sgn}(\pi) a_{\pi(1),1} a_{pi(2),2} \dots a_{\pi(n),n} \\ &= \sum_{\pi \in S_n, \pi(n)=n} \operatorname{sgn}(\pi) a_{\pi(1),1} a_{pi(2),2} \dots a_{\pi(n-1),n-1} = \\ &= (-1)^{n+n} \sum_{\pi \in S_{n-1}} \operatorname{sgn}(\pi) a_{\pi(1),1} a_{pi(2),2} \dots a_{\pi(n-1),n-1} = A_{nn} \ . \end{aligned}$$

V druhé úpravě jsme vynechali nulové sčítance, ve třetí jsme použili $a_{nn} = 1$, ve čtvrté jsme použili $(-1)^{(n-1)+(n-1)} = 1$ a skutečnost, že znaménko permutace $\pi \in S_n$, pro kterou $\pi(n) = n$, je stejné jako znaménko permutace π zúžené na množinu $\{1, 2, \dots, n-1\}$ (to platí, protože tyto dvě permutace mají stejný redukovaný cyklický zápis).

2. krok. Pro libovolné $i, j \in \{1, 2, \dots, n\}$, pokud $a_{ij} = 1$ a všechny ostatní prvky v j-tém sloupci jsou nulové, pak $\det(A) = A_{ij}$.

Posuneme-li v matici A řádek i na poslední místo a potom sloupec j na poslední místo, dostaneme matici B, jejíž determinant je B_{nn} podle 1. kroku. Posunutí i-tého řádku na n-té místo odpovídá permutaci řádků $\sigma = (n\ (n-1)\ \dots\ i)$ a posunutí j-tého sloupce na n-té místo odpovídá permutaci sloupců $\rho = (n\ (n-1)\ \dots\ j)$. Podle bodu (3) tvrzení 6.19 o změně determinantu při permutaci sloupců a analogického tvrzení pro řádky máme

$$\det(A) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\rho)\det(B) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\rho)B_{nn} = (-1)^{i+j}B_{nn} = A_{ij} \ ,$$

kde $\operatorname{sgn}(\sigma)\operatorname{sgn}(\rho) = (-1)^{i+j}$ je vidět z toho, že parita délek cyklů σ,ρ je stejná právě tehdy, když parita i a j je stejná.

3. krok. Pomocí 2.kroku a bodů (1) a (2) z tvrzení 6.19 nyní výpočet dokončíme.

$$\begin{aligned} \det(A) &= \det(A_{*1}|A_{*2}|\dots|A_{*n}) \\ &= \det\left(A_{*1}|A_{*2}|\dots|A_{*(j-1)}|\ \sum_{i=1}^{n} a_{ij}\mathbf{e}_i\ |A_{*(j+1)}|\dots|A_{*n}\right) \\ &= \sum_{i=1}^{n} a_{ij} \det\left(A_{*1}|A_{*2}|\dots|A_{*(j-1)}|\ \mathbf{e}_i\ |A_{*(j+1)}|\dots|A_{*n}\right) \\ &= \sum_{i=1}^{n} a_{ij}A_{ij} \ . \end{aligned}$$

(Rovněž jsme využili triviální skutečnosti, že algebraický doplněk prvku a_{ij} se nezmění, změníme-li j-tý sloupec.) □

Díky tvrzení 6.18 o transponování můžeme provádět rozvoj podle řádku:

$$\det(A) = \sum_{j=1}^{n} a_{ij}A_{ij} = a_{i1}A_{i1} + a_{i2}A_{i2} + \cdots + a_{in}A_{in} \ .$$

Příklad 6.33. Provedeme rozvoj podle druhého řádku.

$$\begin{vmatrix} 2 & 4 & 7 \\ 3 & -2 & -4 \\ 5 & 1 & -3 \end{vmatrix} = 3 \cdot (-1)^{1+2} \begin{vmatrix} 4 & 7 \\ 1 & -3 \end{vmatrix} + (-2) \cdot (-1)^{2+2} \begin{vmatrix} 2 & 7 \\ 5 & -3 \end{vmatrix} +$$

$$+(-4) \cdot (-1)^{3+2} \begin{vmatrix} 2 & 4 \\ 5 & 1 \end{vmatrix}$$

Všimněte si, že se znaménka v algebraickém doplňku střídají, stačí tedy určit první.

Rozvoj podle sloupce (řádku) vznikne pouhým přeskupením výrazu z definice determinantu. Kdybychom provedli rozvoj pro matici řádu n, na vzniklé matice provedli rozvoj, atd., po $n-1$ krocích bychom dostali znovu výraz z definice determinantu. Pro praktické počítání se rozvoj hodí v situaci, že některý řádek nebo sloupec je skoro celý nulový, nejlépe, když obsahuje jen jeden nenulový prvek. Pak je totiž většina sčítanců v rozvoji nulová a nemusíme počítat menší determinanty. Efektivní postup je vyeliminovat jeden řádek nebo sloupec, provést rozvoj a pokračovat s jedním menším determinantem.

Příklad 6.34. Spočítáme znovu determinant v příkladu 6.20.

$$\begin{vmatrix} 2 & 4 & 2 \\ 7 & -1 & 4 \\ 5 & 0 & -6 \end{vmatrix} = \begin{vmatrix} 30 & 0 & 18 \\ 7 & -1 & 4 \\ 5 & 0 & -6 \end{vmatrix} = (-1)^{2+2} \begin{vmatrix} 30 & 18 \\ 5 & -6 \end{vmatrix}$$

$$= -180 - 90 = -270$$

V první úpravě jsme 4-násobek druhého řádku přičetli k prvnímu, pak jsme provedli rozvoj podle 2. sloupce a zbylý determinant jsme spočítali z definice.

Příklad 6.35. Vypočítáme determinant větší matice.

$$\begin{vmatrix} -3 & -1 & -3 & 4 & -3 \\ -7 & -1 & -10 & 5 & -2 \\ 4 & 0 & 6 & -4 & -1 \\ 5 & 1 & 10 & -4 & 5 \\ 5 & 3 & 4 & -4 & 3 \end{vmatrix} = \begin{vmatrix} 2 & 0 & 7 & 0 & 2 \\ -2 & 0 & 0 & 1 & 3 \\ 4 & 0 & 6 & -4 & -1 \\ 5 & 1 & 10 & -4 & 5 \\ -10 & 0 & -26 & 8 & -12 \end{vmatrix}$$

$$= \begin{vmatrix} 2 & 7 & 0 & 2 \\ -2 & 0 & 1 & 3 \\ 4 & 6 & -4 & -1 \\ -10 & -26 & 8 & -12 \end{vmatrix} = \begin{vmatrix} 2 & 7 & 0 & 2 \\ 0 & 0 & 1 & 0 \\ -4 & 6 & -4 & 11 \\ 6 & -26 & 8 & -36 \end{vmatrix}$$

$$= - \begin{vmatrix} 2 & 7 & 2 \\ -4 & 6 & 11 \\ 6 & -26 & -36 \end{vmatrix} = - \begin{vmatrix} 2 & 7 & 2 \\ 0 & 20 & 15 \\ 0 & -47 & -42 \end{vmatrix}$$

$$= -2 \cdot \begin{vmatrix} 20 & 15 \\ -47 & -42 \end{vmatrix} = 10 \cdot \begin{vmatrix} 4 & 3 \\ 47 & 42 \end{vmatrix} = 10(168 - 141) = 270.$$

Nejprve jsme téměř vynulovali 2. sloupec eliminací, užitím 4. řádku. Potom jsme determinant rozvinuli podle 2. sloupce, máme jediný nenulový člen se znaménkem $(-1)^{2+4} = 1$. Dále jsme vyeliminovali 2. řádek (pomocí 3. sloupce). Následoval rozvoj podle 2. řádku, nenulový člen má znaménko $(-1)^{3+2} = -1$, atd.

6.4.1. *Adjungovaná matice.* Rozvoj podle j-tého sloupce probíhá tak, že vezmeme první prvek v j-tém sloupci, vynásobíme znaménkem $(-1)^{j+1}$ a determinantem matice, která vznikne vynecháním prvního řádku a j-tého sloupce. Pak postupujeme obdobně s dalšími prvky v j-tém sloupci a všechny takové výrazy sečteme. Pokud „omylem“ vždy vynecháváme jiný sloupec k, dostaneme nulový prvek tělesa.

Věta 6.36 (o falešném rozvoji)**.** *Je-li A čtvercová matice řádu n a $j,k \in \{1,2,\dots,n\}$, $j \neq k$, pak*

$$0 = \sum_{i=1}^{n} a_{ij} A_{ik} = a_{1j}A_{1k} + a_{2j}A_{2k} + \cdots + a_{nj}A_{nk} \ .$$

Důkaz. Označme B matici, která vznikne nahrazením k-tého sloupce matice A sloupcem A_{*j}. Protože B má dva sloupce stejné, je B singulární (má lineárně závislé sloupce, takže můžeme použít bod (3) pozorování 5.79), a proto $\det(B) = 0$ podle kritéria v tvrzení 6.22. Na B použijeme rozvoj podle k-tého sloupce a využijeme toho, že $B_{ik} = A_{ik}$, protože algebraický doplněk prvku b_{ik} na k-tém sloupci nezávisí.

$$0 = \det(B) = b_{1k}B_{1k} + b_{2k}B_{2k} + \cdots + b_{nk}B_{nk} = a_{1j}A_{1k} + a_{2j}A_{2k} + \cdots + a_{nj}A_{nk}$$

□

Z algebraických doplňků matice $A = (a_{ij})$ vytvoříme tzv. *adjungovanou matici* tak, že prvek na místě (i, j) bude algebraický doplněk prvku a_{ji}. **Pozor na změnu pořadí indexů.**

Definice 6.37. *Adjungovanou maticí* ke čtvercové matici A rozumíme matici $\operatorname{adj}(A)$ stejného řádu, která má na místě (i, j) prvek A_{ji}.

Řádkovou i sloupcovou verzi vět o rozvoji a falešném rozvoji jde formulovat maticovým vztahem.

Věta 6.38. *Pro libovolnou čtvercovou matici A platí*

$$\operatorname{adj}(A)\, A = A \operatorname{adj}(A) = \det(A)\, I_n \ .$$

Speciálně, pokud A je regulární, pak

$$A^{-1} = \frac{\operatorname{adj}(A)}{\det(A)} \ .$$

Důkaz. Prvek na místě (i, j) v součinu $\operatorname{adj}(A)\ A$ je $A_{1i}a_{1j} + A_{2i}a_{2j} + \ldots A_{ni}a_{nj}$. Pokud $i = j$ je výsledkem $\det A$, protože výraz je roven rozvoji podle i-tého sloupce. Pokud $i \neq j$ je výsledkem 0 podle věty o falešném rozvoji. Dohromady dostáváme $\operatorname{adj}(A)\, A = \det(A)\, I_n$. Rovnost $A \operatorname{adj}(A) = \det(A)\, I_n$ dostaneme obdobně podle vět o rozvoji a falešném rozvoji podle řádku. □

Věta nám také dává explicitní vyjádření inverzní matice. Inverzní matici pro řády 2 a 3 lze její pomocí počítat rychle bez eliminace.

Příklad 6.39. Pro regulární matici A řádu 2 dostáváme

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}^{-1} = \frac{1}{a_{11}a_{22} - a_{12}a_{21}} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$$

Příklad 6.40. Spočítáme inverzní matici k reálné matici

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

Nejdřív spočítáme adjungovanou matici.

$$\operatorname{adj}(A) = \begin{pmatrix} \begin{vmatrix} 4 & -2 \\ 2 & 5 \end{vmatrix} & -\begin{vmatrix} 1 & -3 \\ 2 & 5 \end{vmatrix} & \begin{vmatrix} 1 & -3 \\ 4 & -2 \end{vmatrix} \\ -\begin{vmatrix} 3 & -2 \\ 0 & 5 \end{vmatrix} & \begin{vmatrix} -2 & -3 \\ 0 & 5 \end{vmatrix} & -\begin{vmatrix} -2 & -3 \\ 3 & -2 \end{vmatrix} \\ \begin{vmatrix} 3 & 4 \\ 0 & 2 \end{vmatrix} & -\begin{vmatrix} -2 & 1 \\ 0 & 2 \end{vmatrix} & \begin{vmatrix} -2 & 1 \\ 3 & 4 \end{vmatrix} \end{pmatrix}$$
$$= \begin{pmatrix} 24 & -11 & 10 \\ -15 & -10 & -13 \\ 6 & 4 & -11 \end{pmatrix}$$

Determinant matice A by teď bylo neefektivní počítat zvlášť. Stačí spočítat například prvek na místě $(3, 3)$ v součinu $A \operatorname{adj}(A)$.

$$\det(A) = 0 \cdot 10 + 2 \cdot (-13) + 5 \cdot (-11) = -81.$$

Vidíme, že A je regulární a platí

$$A^{-1} = -\frac{1}{81} \begin{pmatrix} 24 & -11 & 10 \\ -15 & -10 & -13 \\ 6 & 4 & -11 \end{pmatrix} = \frac{1}{81} \begin{pmatrix} -24 & 11 & -10 \\ 15 & 10 & 13 \\ -6 & -4 & 11 \end{pmatrix} \ .$$

6.5. **Vandermondův determinant.**

Tzv. *Vandermondova matice* vzniká při interpolaci polynomem. Budeme hledat polynom f nad tělesem $\mathbf{T}$ stupně nejvýše $n-1$, tj.

$$f = k_0 + k_1 x + \cdots + k_{n-1}x_{n-1}, \quad k_0, k_1, \dots k_{n-1} \in T \ ,$$

který splňuje podmínky

$$f(a_1) = b_1,\ f(a_2) = b_2,\ \dots\ , f(a_n) = a_n \ ,$$

kde $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n$ jsou dané prvky tělesa $\mathbf{T}$, přičemž $a_1, a_2, \dots, a_n$ jsou navzájem různé. Pro koeficienty dostáváme soustavu rovnic

$$\begin{pmatrix} 1 & a_1 & a_1^2 & \dots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \dots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \dots & a_n^{n-1} \end{pmatrix} \begin{pmatrix} k_0 \\ k_1 \\ \vdots \\ k_{n-1} \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

Matice této soustavy se nazývá *Vandermondova matice* a její determinant *Vandermondův determinant*. Indukcí podle n dokážeme, že je roven

$$V(a_1, a_2, \dots, a_n) = \begin{vmatrix} 1 & a_1 & a_1^2 & \dots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \dots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \dots & a_n^{n-1} \end{vmatrix} = \prod_{1 \le i < j \le n} a_j - a_i \ .$$

Z toho mimo jiné vyplývá, že Vandermondova matice je regulární (za předpokladu, že $a_1, a_2, \dots, a_n$ jsou po dvou různé) a tedy hledaný polynom f existuje a je jednoznačně určený; nazývá se Lagrangeův interpolační polynom.

Vzorec snadno ověříme pro $n = 2$ (pro $n = 1$ by vzorec platil, pokud bychom definovali prázdný součin jako 1). Předpokládejme $n > 2$ a že vzorec platí pro menší hodnoty n. Začneme tím, že vyeliminujeme první sloupec, tj. (-1)-násobek prvního řádku přičteme ke všem ostatním, a pak provedeme rozvoj podle prvního sloupce. .

$$\begin{vmatrix} 1 & a_1 & a_1^2 & \dots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \dots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \dots & a_n^{n-1} \end{vmatrix} = \begin{vmatrix} 1 & a_1 & a_1^2 & \dots & a_1^{n-1} \\ 0 & a_2 - a_1 & a_2^2 - a_1^2 & \dots & a_2^{n-1} - a_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & a_n - a_1 & a_n^2 - a_1^2 & \dots & a_n^{n-1} - a_1^{n-1} \end{vmatrix}$$

$$= \begin{vmatrix} a_2 - a_1 & a_2^2 - a_1^2 & \dots & a_2^{n-1} - a_1^{n-1} \\ a_3 - a_1 & a_3^2 - a_1^2 & \dots & a_3^{n-1} - a_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_n - a_1 & a_n^2 - a_1^2 & \dots & a_n^{n-1} - a_1^{n-1} \end{vmatrix}$$

Vytkneme z prvního řádku výraz $a_2 - a_1$, z druhého výraz $a_3 - a_2$, atd., a využijeme vzorce

$$c^k - d^k = (c-d)(c^{k-1} + c^{k-2}d + c^{k-3}d^2 + \cdots + cd^{k-2} + d^{k-1}) \ .$$

$$\begin{vmatrix} a_2 - a_1 & a_2^2 - a_1^2 & \dots & a_2^{n-1} - a_1^{n-1} \\ a_3 - a_1 & a_3^2 - a_1^2 & \dots & a_3^{n-1} - a_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_n - a_1 & a_n^2 - a_1^2 & \dots & a_n^{n-1} - a_1^{n-1} \end{vmatrix} = (a_2 - a_1)(a_3 - a_1) \dots (a_n - a_1) \cdot$$

$$\cdot \begin{vmatrix} 1 & a_2 + a_1 & a_2^2 + a_2 a_1 + a_1^2 & \dots & a_2^{n-2} + a_2^{n-3}a_1 + \cdots + a_1^{n-2} \\ 1 & a_3 + a_1 & a_3^2 + a_3 a_1 + a_1^2 & \dots & a_3^{n-2} + a_3^{n-3}a_1 + \cdots + a_1^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n + a_1 & a_n^2 + a_n a_1 + a_1^2 & \dots & a_n^{n-2} + a_n^{n-3}a_1 + \cdots + a_1^{n-2} \end{vmatrix}$$

Dále přičteme $(-a_1)$-násobek předposledního sloupce k poslednímu, ..., $(-a_1)$-násobek druhého sloupce ke třetímu, a nakonec $(-a_1)$-násobek prvního sloupce ke druhému.

$$\begin{vmatrix} 1 & a_2 + a_1 & a_2^2 + a_2 a_1 + a_1^2 & \dots & a_2^{n-2} + a_2^{n-3}a_1 + \cdots + a_1^{n-2} \\ 1 & a_3 + a_1 & a_3^2 + a_3 a_1 + a_1^2 & \dots & a_3^{n-2} + a_3^{n-3}a_1 + \cdots + a_1^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n + a_1 & a_n^2 + a_n a_1 + a_1^2 & \dots & a_n^{n-2} + a_n^{n-3}a_1 + \cdots + a_1^{n-2} \end{vmatrix}$$

$$= \begin{vmatrix} 1 & a_2+a_1 & a_2^2+a_2a_1+a_1^2 & \dots & a_2^{n-2} \\ 1 & a_3+a_1 & a_3^2+a_3a_1+a_1^2 & \dots & a_3^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n+a_1 & a_n^2+a_na_1+a_1^2 & \dots & a_n^{n-2} \end{vmatrix} = \dots = \begin{vmatrix} 1 & a_2+a_1 & a_2^2 & \dots & a_2^{n-2} \\ 1 & a_3+a_1 & a_3^2 & \dots & a_3^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n+a_1 & a_n^2 & \dots & a_n^{n-2} \end{vmatrix}$$

$$= \begin{vmatrix} 1 & a_2 & a_2^2 & \dots & a_2^{n-2} \\ 1 & a_3 & a_3^2 & \dots & a_3^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \dots & a_n^{n-2} \end{vmatrix} = V(a_2,\dots,a_n)$$

Vznikne Vandermondův determinant pro $a_2, a_3, \dots, a_n$, takže výpočet můžeme dokončit užitím indukčního předpokladu.

$$V(a_1,\dots,a_n) = (a_2-a_1)(a_3-a_1)\dots(a_n-a_1)V(a_2,\dots,a_n)$$
$$= (a_2-a_1)(a_3-a_1)\dots(a_n-a_1)\prod_{2\le i<j\le n} a_j-a_i = \prod_{1\le i<j\le n} a_j-a_i$$

Odvozený vzorec platí i v případě, že $a_1,\dots,a_n$ nejsou navzájem různé, protože pak má Vandermondova matice dva stejné řádky, takže její determinant je nulový, stejně jako výraz $\prod_{1\le i<j\le n} a_j-a_i$.

Cvičení

1. Vypočtěte obsah rovnoběžníku určeného vektory $\mathbf{u}, \mathbf{v}$ podle obrázku **??**.

2. Promyslete si detailně důkaz tvrzení 6.3.

3. Najděte všechna řešení rovnic $\alpha\pi = \beta$, $\pi\alpha = \beta$ a $\alpha\pi\gamma = \beta$, kde $\alpha, \beta, \gamma \in S_{10}$.

$$\alpha = (1\ 5\ 3\ 2\ 7)(4\ 6),\ \beta = (2\ 3\ 9\ 10\ 4)(7\ 8),\ \gamma = (1\ 7)(2\ 6)(4\ 5)$$

4. Dokažte, že pro libovolné $k \in \mathbb{N}$ permutace na konečné množině X má permutace $\pi\rho\pi^{-1}$ v zápisu pomocí nezávislých cyklů stejný počet cyklů délky k jako permutace ρ. Odvoďte z toho, že stejné tvrzení platí pro permutace $\pi\rho$ a $\rho\pi$.

5. Označme k počet cyklů v cyklickém zápisu permutace $\pi \in S_n$ (počítáme i cykly délky 1!). Dokažte, že $\operatorname{sgn}(\pi) = (-1)^{n+k}$.

6. Vypište z definice výraz pro determinant matice řádu 4.

7. Najděte vzorec pro determinant čtvercových matic $A = (a_{ij})$ řádu n takových, že $a_{ij} = 0$ kdykoliv $i > n+1-j$.

8. Nechť A je blokově horní trojúhelníková matice, tj. matice tvaru

$$A = \left(\begin{array}{c|c|c|c} A_{11} & A_{12} & \dots & A_{1r} \\ \hline 0 & A_{22} & \dots & A_{2r} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline 0 & 0 & \dots & A_{rr} \end{array}\right),$$

kde $A_{11}, A_{22}, \dots, A_{rr}$ jsou čtvercové matice (ne nutně stejného řádu). Dokažte, že $\det(A) = \det(A_{11})\det(A_{22})\dots\det(A_{rr})$.

9. Z předchozího cvičení by se mohlo zdát, že determinanty můžeme počítat blokově. Není tomu tak. Nalezněte matici

$$A = \left(\begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{21} & A_{22} \end{array}\right)$$

se čtvercovými bloky takovou, že $\det(A) \neq \det(A_{11})\det(A_{22}) - \det(A_{12})\det(A_{21})$.

10. Dokažte, že pro regulární matici A řádu n platí $\det(\operatorname{adj}(A)) = \det(A)^{n-1}$.

11. Dokažte tvrzení 6.25

7. Lineární zobrazení

Cíl. .

7.1. Definice a příklady.

Připomeňme, že matice A nad tělesem $\mathbf{T}$ typu $m \times n$ určuje zobrazení $f_A : T^n \to T^m$ předpisem $f_A(\mathbf{x}) = A\mathbf{x}$. Tento pohled motivoval řadu zavedených pojmů:

- **Násobení matic:** Je-li B matice nad $\mathbf{T}$ typu $p \times m$, pak složené zobrazení $f_B \circ f_A : T^n \to T^p$ je rovno zobrazení f_{BA}.
- **Inverzní matice:** Je-li $m = n$ a f_A je bijekce, pak inverzní zobrazení $(f_A)^{-1}$ je rovno $f_{A^{-1}}$.
- **Jádro matice:** $\operatorname{Ker} A$ je rovno množině všech vektorů $\mathbf{x} \in T^n$, které f_A zobrazí na nulový vektor.
$$\operatorname{Ker} A = \{x : f_A(\mathbf{x}) = \mathbf{o}\} \leq \mathbf{T}^n$$
- **Sloupcový prostor matice a hodnost:** $\operatorname{Im} A$ je roven obrazu zobrazení f_A. Hodnost A je rovna dimenzi $\operatorname{Im} A$.
$$\operatorname{Im} A = \{f_A(\mathbf{x}) : \mathbf{x} \in \mathbf{T}^n\} = f_A(T^n) \leq \mathbf{T}^m, \quad \operatorname{rank}(A) = \dim(\operatorname{Im} A)$$
- **Determinant:** Je-li $\mathbf{T} = \mathbb{R}$ a $m = n = 2$ (resp. $m = n = 3$), pak $\det(A)$ udává změnu obsahu (resp. objemu) a orientace při zobrazení f_A.

Rovněž nám tento pohled poskytl geometrickou interpretaci řady tvrzení.

Ne každé zobrazení $T^n \to T^m$ je tvaru f_A pro nějakou matici A. Zobrazení tvaru f_A mají tu vlastnost, že „zachovávají“ sčítání a násobení. Takovým zobrazením říkáme *lineární* a za okamžik nahlédneme, že linearita tato zobrazení charakterizuje. Lineární zobrazení definujeme mezi obecnými vektorovými prostory (nejen aritmetickými).

Definice 7.1. Nechť $\mathbf{V}, \mathbf{W}$ jsou vektorové prostory nad stejným tělesem $\mathbf{T}$. Zobrazení $f : V \to W$ nazýváme *lineární zobrazení* (nebo *homomorfismus*) z $\mathbf{V}$ do $\mathbf{W}$, pokud

(1) $f(\mathbf{u} + \mathbf{v}) = f(\mathbf{u}) + f(\mathbf{v})$ pro libovolné $\mathbf{u}, \mathbf{v} \in V$ a
(2) $f(t\mathbf{u}) = tf(\mathbf{u})$ pro libovolné $\mathbf{u} \in V$ a $t \in T$.

Skutečnost, že f je lineární zobrazení z $\mathbf{V}$ do $\mathbf{W}$ zapisujeme $f : \mathbf{V} \to \mathbf{W}$.

Vlevo v rovnostech vystupují operace v prostoru $\mathbf{V}$ a vpravo operace v prostoru $\mathbf{W}$. Zdůrazněme, že prostory $\mathbf{V}$ a $\mathbf{W}$ musí být nad stejným tělesem. Všimněte si rovněž, že každé lineární zobrazení zobrazuje nulový vektor ve $\mathbf{V}$ na nulový vektor v $\mathbf{W}$.

Pro libovolnou matici A nad $\mathbf{T}$ typu $m \times n$ je zobrazení $f_A : T^n \to T^m$ lineární, protože

$$f_A(\mathbf{u} + \mathbf{v}) = A(\mathbf{u} + \mathbf{v}) = A\mathbf{u} + A\mathbf{v} = f_A(\mathbf{u}) + f_A(\mathbf{v})$$

a

$$f_A(t\mathbf{u}) = A(t\mathbf{u}) = t(A\mathbf{u}) = tf_A(\mathbf{u}) \ .$$

To nám dává řadu příkladů lineárních zobrazení mezi aritmetickými vektorovými prostory (a jak jsme zmínili, jiná lineární zobrazení mezi aritmetickými prostory neexistují, viz níže).

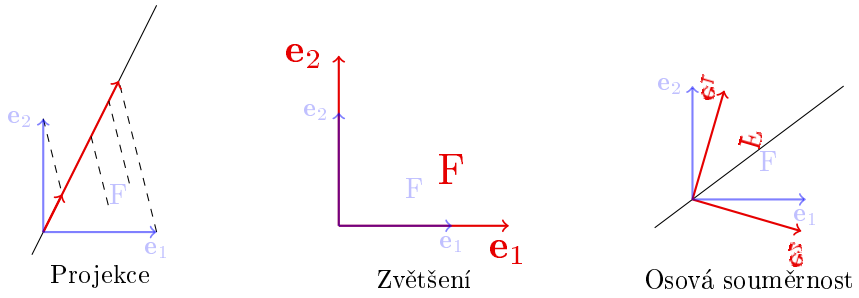
Příklad 7.2. Příklady lineárních zobrazení z $\mathbb{R}^2$ do $\mathbb{R}^2$:

- Otočení (rotace) o daný úhel.
- Zkosení

Otočení Zkosení

Obrázek 10. Zobrazení v rovině: otočení a zkosení

- Projekce na přímku procházející počátkem.
- Osová souměrnost podle přímky procházející počátkem.
- Zvětšení (zmenšení)



Obrázek 11. Zobrazení v rovině: projekce, zvětšení a osová souměrnost

Lineární zobrazení z $\mathbb{R}^3$ do $\mathbb{R}^3$ jsou například rotace, zrcadlení podle roviny procházející počátkem, osová souměrnost podle přímky procházející počátkem, projekce na rovinu nebo přímku procházející počátkem.

Příkladem lineárního zobrazení z $\mathbb{R}^2$ do $\mathbb{R}^3$ je zobrazení f_A pro matici

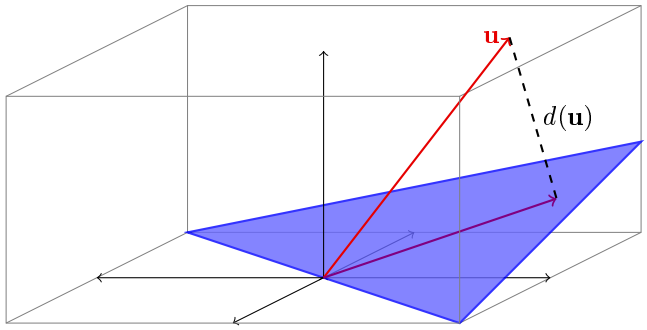
$$A = \begin{pmatrix} 1 & 2 \\ 1 & 0 \\ 1 & 3 \end{pmatrix}$$

OBRAZEK

Lineární zobrazení z $\mathbb{R}^3$ do $\mathbb{R}^2$ používáme při kreslení trojrozměrných útvarů na tabuli (papír):

OBRAZEK

Příkladem lineárního zobrazení z $\mathbb{R}^3$ do $\mathbb{R}$ je zobrazení d udávající orientovanou vzdálenost od zvolené roviny procházející počátkem.



Obrázek 12. Lineární zobrazení z $\mathbb{R}^3$ do $\mathbb{R}$: orientovaná vzdálenost od plochy

Ještě než popíšeme, jak vypadají lineární zobrazení obecně, podíváme se na další příklady.

Příklad 7.3.

- Identické zobrazení $\mathrm{id}_{\mathbf{V}}$ na libovolném vektorovém prostoru $\mathbf{V}$ je lineární zobrazení $\mathbf{V} \to \mathbf{V}$.
- Tzv. *nulové zobrazení* 0 z $\mathbf{V}$ do $\mathbf{W}$ přiřazující všem vektorům ve $\mathbf{V}$ nulový vektor ve $\mathbf{W}$ je lineární.
- Nechť $B = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ je báze vektorového prostoru $\mathbf{V}$. Zobrazení f z V do T^n definované $f(\mathbf{v}) = [\mathbf{v}]_B$ je lineární zobrazení $\mathbf{V} \to \mathbf{T}^n$ podle tvrzení 5.64 o souřadnicích a operacích.
- Zobrazení přiřazující matici nad $\mathbf{T}$ typu $n \times n$ součet prvků na diagonále (tzn. stopu) je lineárním zobrazením $\mathbf{T}^{n\times n} \to \mathbf{T}$.
- Determinant můžeme chápat jako zobrazení přiřazující n-tici vektorů z $\mathbf{T}^n$ prvek $\mathbf{T}$, tedy jako zobrazení

$$\mathrm{Det} : \underbrace{T^n \times T^n \times \cdots \times T^n}_{n\times} \to T \ .$$

  Toto zobrazení je tzv. *multilineární*, tj. zvolíme-li pevně $n-1$ z celkových n argumentů, vznikne lineární zobrazení $\mathbf{T}^n \to \mathbf{T}$. Například jsou-li $\mathbf{v}_1, \mathbf{v}_3 \in \mathbf{T}^3$ libovolné vektory, je zobrazení $f(\mathbf{x}) = \det(\mathbf{v}_1|\mathbf{x}|\mathbf{v}_3)$ lineární zobrazení z $\mathbf{T}^3$ do $\mathbf{T}$. Linearita byla použitá při odvozování vzorců na začátku kapitoly o determinantech a formulována jako body (1) a (2) v tvrzení 6.19.

- Derivace je lineárním zobrazením (např.) z prostoru reálných diferencovatelných funkcí do prostoru všech reálných funkcí.
- Zobrazení přiřazující funkci její určitý integrál od 1 do 10 je lineárním zobrazením z prostoru všech reálných spojitých funkcí na $[1,10]$ do $\mathbb{R}$.

7.2. **Matice lineárního zobrazení.**

Z definice lineárního zobrazení se snadno indukcí dokáže, že obrazem lineární kombinace je lineární kombinace obrazů, tj. pro libovolné lineární zobrazení $f : \mathbf{V} \to \mathbf{W}$, vektory $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n \in V$ a skaláry $t_1, t_2, \dots, t_k \in T$ platí

$$f(t_1\mathbf{v}_1 + t_2\mathbf{v}_2 + \cdots + t_k\mathbf{v}_n) = t_1 f(\mathbf{v}_1) + t_2 f(\mathbf{v}_2) + \cdots + t_k f(\mathbf{v}_n).$$

Toto jednoduché pozorování má důležitý důsledek, že lineární zobrazení je jednoznačně určené obrazy prvků libovolné báze. Tvrzení formulujeme pro konečně generované prostory, zobecnění necháme do cvičení.

Tvrzení 7.4. *Nechť $\mathbf{V}$ a $\mathbf{W}$ jsou vektorové prostory nad tělesem $\mathbf{T}$, $B = (\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$ je báze $\mathbf{V}$ a $\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_n \in W$ jsou libovolné vektory. Pak existuje právě jedno lineární zobrazení $f : \mathbf{V} \to \mathbf{W}$ splňující $f(\mathbf{v}_i) = \mathbf{w}_i$ pro každé $i \in \{1, 2, \dots, n\}$.*

Důkaz. Předpokládejme, že f je lineární zobrazení splňující $f(\mathbf{v}_i) = \mathbf{w}_i$. Každý vektor $\mathbf{x} \in \mathbf{V}$ lze zapsat jediným způsobem jako lineární kombinaci $\mathbf{x} = t_1\mathbf{v}_1 + t_2\mathbf{v}_2 + \cdots + t_n\mathbf{v}_n$ (jinými slovy, $[\mathbf{x}]_B = (t_1, t_2, \dots, t_n)$) a pak podle výše uvedeného vztahu platí

$$f(\mathbf{x}) = t_1\mathbf{w}_1 + t_2\mathbf{w}_2 + \cdots + t_n\mathbf{w}_n$$

To dokazuje jednoznačnost.

Na druhou stranu je potřeba ověřit, že zobrazení f definované tímto předpisem je lineární a splňuje $f(\mathbf{v}_i) = \mathbf{w}_i$, a tím bude dokázána existence. Vztah $f(\mathbf{v}_i) = \mathbf{w}_i$ necháme k ověření čtenáři. K důkazu linearity uvažujme vektory $\mathbf{x}, \mathbf{y} \in \mathbf{V}$, jejichž vyjádření vzhledem k B jsou

$$[\mathbf{x}]_B = (t_1, t_2, \dots, t_n)^T, \quad [\mathbf{y}]_B = (s_1, s_2, \dots, s_n)^T \ .$$

Pak $[\mathbf{x} + \mathbf{y}]_B = (t_1 + s_1, t_2 + s_2, \dots, t_n + s_n)^T$ (viz tvrzení 5.64 o souřadnicích a operacích) a tedy

$$\begin{aligned} f(\mathbf{x} + \mathbf{y}) &= (t_1 + s_1)\mathbf{w}_1 + (t_2 + s_2)\mathbf{w}_2 + \cdots + (t_n + s_n)\mathbf{w}_n \\ &= t_1\mathbf{w}_1 + t_2\mathbf{w}_2 + \cdots + t_n\mathbf{w}_n + s_1\mathbf{w}_1 + s_2\mathbf{w}_2 + \cdots + s_n\mathbf{w}_n \\ &= f(\mathbf{x}) + f(\mathbf{y}) \ . \end{aligned}$$

Podobně se ukáže zachovávání násobení skalárem. □

Tvrzení nám dává geometrickou představu lineárních zobrazení: podíváme se na obrazy prvků nějaké báze, obrazy zbylých vektorů jsou určeny linearitou. Na obrázku je znázorněné lineární zobrazení z prostoru dimenze 2 s bází $(\mathbf{u}, \mathbf{v})$, obraz vektoru $-\mathbf{u} + 2\mathbf{v}$ a obraz komplikovanějšího útvaru.

OBRAZEK

Algebraickým důsledkem je, že každé lineární zobrazení je „určené“ maticí. Než zformulujeme příslušné definice a tvrzení obecněji, ukážeme, že každé lineární zobrazení f z $\mathbf{T}^n$ do $\mathbf{T}^m$ je rovno f_A pro jistou (jednoznačně určenou) matici A nad $\mathbf{T}$ typu $m \times n$. Skutečně, pro libovolný vektor $\mathbf{x} = (x_1, x_2, \dots, x_n)$ platí

$$f(\mathbf{x}) = f(x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + \cdots + x_n\mathbf{e}_n) = x_1 f(\mathbf{e}_1) + x_2 f(\mathbf{e}_2) + \cdots + x_n f(\mathbf{e}_n) \ ,$$

což lze maticově zapsat jako

$$f(\mathbf{x}) = (f(\mathbf{e}_1)|f(\mathbf{e}_2)|\dots|f(\mathbf{e}_n))\mathbf{x} \ ,$$

takže stačí položit $A = (f(\mathbf{e}_1)|f(\mathbf{e}_2)|\dots|f(\mathbf{e}_n))$ a máme $f = f_A$. Matice A je určena jednoznačně, protože i-tý sloupec musí být f-obrazem i-tého vektoru kanonické báze.

Lineární zobrazení $f : \mathbf{V} \to \mathbf{W}$, kde $\mathbf{V}, \mathbf{W}$ jsou konečně generované, můžeme obdobně popsat maticově, počítáme-li v prostorech $\mathbf{V}$ a $\mathbf{W}$ vzhledem ke zvoleným bázím B a C. Konkrétně, existuje (jednoznačně určená) matice A typu $\dim(\mathbf{W}) \times \dim(\mathbf{V})$ taková, že

$$[f(\mathbf{x})]_C = A[\mathbf{x}]_B$$

pro libovolný vektor $\mathbf{x} \in V$. Této matici říkáme matice f vzhledem k B a C. Odvození, jak tato matice vypadá, se udělá podobně jako výše.

Definice 7.5. Nechť $\mathbf{V}, \mathbf{W}$ jsou konečně generované vektorové prostory nad tělesem $\mathbf{T}$, $f : \mathbf{V} \to \mathbf{W}$, $B = (\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$ je báze $\mathbf{V}$ a C je báze $\mathbf{W}$. *Maticí lineárního zobrazení f vzhledem k bázím B a C* rozumíme matici

$$[f]_C^B = ([f(\mathbf{v}_1)]_C|[f(\mathbf{v}_2)]_C|\dots|[f(\mathbf{v}_n)]_C)$$

V matici f vzhledem k B a C je tedy i-tý sloupec roven souřadnicím obrazu i-tého vektoru báze B v bázi C. Matice je typu $\dim(\mathbf{W}) \times \dim(\mathbf{V})$.

Tvrzení 7.6. *Jsou-li $\mathbf{V}, \mathbf{W}$ konečně generované vektorové prostory nad tělesem $\mathbf{T}$, B báze $\mathbf{V}$, C báze $\mathbf{W}$ a $f : \mathbf{V} \to \mathbf{W}$, pak pro libovolný vektor $\mathbf{x} \in V$ platí*

$$[f(\mathbf{x})]_C = [f]_C^B [\mathbf{x}]_B \ .$$

Důkaz. Pro libovolný vektor $\mathbf{x} \in V$ s vyjádřením $[\mathbf{x}]_B = (x_1, x_2, \ldots, x_n)^T$ vzhledem k bázi $B = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ platí

$$f(\mathbf{x}) = f(x_1\mathbf{v}_1 + x_2\mathbf{v}_2 + \cdots + x_n\mathbf{v}_n) = x_1 f(\mathbf{v}_1) + x_2 f(\mathbf{v}_2) + \cdots + x_n f(\mathbf{v}_n) \ ,$$

pro vyjádření vzhledem k bázi C pak podle tvrzení 5.64 o souřadnicích a operacích platí

$$[f(\mathbf{x})]_C = x_1[f(\mathbf{v}_1)]_C + x_2[f(\mathbf{v}_2)]_C + \cdots + x_n[f(\mathbf{v}_n)]_C \ ,$$

což se maticově přepíše

$$[f(\mathbf{x})]_C = ([f(\mathbf{v}_1)]_C | [f(\mathbf{v}_2)]_C | \ldots | [f(\mathbf{v}_n)]_C)(x_1, x_2, \ldots, x_n)^T = [f]_C^B [\mathbf{x}]_B \ .$$

□

Sami si rozmyslete, že $[f]_C^B$ je jediná matice splňující rovnost $[f(\mathbf{x})]_C = [f]_C^B [\mathbf{x}]_B$.

Matice lineárního zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^m$ vzhledem ke kanonickým bázím je původní matice A, tj.

$$[f_A]_{K_m}^{K_n} = A,$$

kde K_i značí kanonickou bázi $\mathbf{T}^i$.

Příklad 7.7. Uvažujme zobrazení $f : \mathbb{Z}_5^3 \to \mathbb{Z}_5^2$ dané předpisem

$$f\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 2x_1 + 3x_2 + x_3 \\ 4x_1 + 2x_3 \end{pmatrix} \ .$$

Vztah lze maticově zapsat

$$f\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 \\ 4 & 0 & 2 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \ .$$

Z toho vidíme, že $f = f_A$ pro matici

$$A = \begin{pmatrix} 2 & 3 & 1 \\ 4 & 0 & 2 \end{pmatrix} \ ,$$

takže f je lineární zobrazení a podle předchozí poznámky $[f]_{K_2}^{K_3} = A$.

Určíme matici f vzhledem k bázím B a C, kde

$$B = \left(\begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \\ 4 \end{pmatrix}\right) \quad \text{a} \quad C = \left(\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 3 \end{pmatrix}\right) \ .$$

K tomu dosazením spočítáme obrazy vektorů v bázi B:

$$f(1,1,2)^T = (2\cdot 1 + 3\cdot 1 + 1\cdot 2, 4\cdot 1 + 2\cdot 2)^T = (2,3)^T$$
$$f(2,2,0)^T = (2\cdot 2 + 3\cdot 2 + 1\cdot 0, 4\cdot 2 + 2\cdot 0)^T = (0,3)^T$$
$$f(3,4,4)^T = (2\cdot 3 + 3\cdot 4 + 1\cdot 4, 4\cdot 3 + 2\cdot 4)^T = (2,0)^T$$

a obrazy vyjádříme v bázi C tím, že vyřešíme tři soustavy rovnic se stejnou maticí zároveň.

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

Zpětnou substitucí dostáváme $[(2,3)^T]_C = (1,2)^T$, $[(0,3)^T]_C = (3,4)^T$, $[(2,0)^T]_C = (3,3)^T$ (toto je dobré ověřit zkouškou, např. $(2,3)^T = 1\cdot(1,2)^T + 2\cdot(3,3)^T$, takže souřadnice vektoru $(2,3)^T$ vzhledem k C jsou spočteny správně). Matice f vzhledem k B a C je

$$[f]_C^B = \begin{pmatrix} 1 & 3 & 3 \\ 2 & 4 & 3 \end{pmatrix} \ .$$

Ověříme vztah $[f(\mathbf{x})]_C = [f]_C^B [\mathbf{x}]_B$ pro vektor $[\mathbf{x}]_B = (1,2,3)^T$, tj.

$$\mathbf{x} = 1\cdot(1,1,2)^T + 2\cdot(2,2,0)^T + 3\cdot(3,4,4)^T = (4,2,4)^T \ .$$

Obraz tohoto vektoru je podle definice

$$f(\mathbf{x}) = \begin{pmatrix} 2\cdot 4 + 3\cdot 2 + 1\cdot 4 \\ 4\cdot 4 + 2\cdot 4 \end{pmatrix} = \begin{pmatrix} 3 \\ 4 \end{pmatrix} .$$

Podle $[f(\mathbf{x})]_C = [f]_C^B[\mathbf{x}]_B$ musí také platit

$$[f(\mathbf{x})]_C = \begin{pmatrix} 1 & 3 & 3 \\ 2 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 \\ 4 \end{pmatrix},$$

což odpovídá, protože $1\cdot(1,2)^T + 4\cdot(3,3)^T = (3,4)^T$, takže skutečně $[(3,4)^T]_C = (1,4)^T$.

Příklad 7.8. S nabytými znalostmi můžeme nyní rychleji určovat matice některých lineárních zobrazení. Budeme hledat matici A, aby příslušné zobrazení f_A byla rotace o α. V novější terminologii, hledáme matici rotace f v $\mathbb{R}^2$ o úhel α vzhledem ke kanonickým bázím. K tomu stačí určit obrazy prvků kanonické báze a napsat je do sloupců. Máme

$$f\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix}, \quad f\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -\sin\alpha \\ \cos\alpha \end{pmatrix} ,$$

tedy

$$A = [f]_{K_2}^{K_2} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$$

Srovnejte tento výpočet s odvozením v části 4.2.1.

Příklad 7.9. Uvažujme zrcadlení $f : \mathbb{R}^2 \to \mathbb{R}^2$ podle přímky p procházející počátkem se směrem $(2,5)^T$. K nalezení matice f vzhledem ke kanonickým bázím, bychom potřebovali nalézt obrazy vektorů kanonické báze, což vyžaduje netriviální výpočet. Je ale snadné určit obrazy vektorů vhodně zvolené báze, například $B = ((2,5)^T, (-5,2)^T)$. Máme totiž $f(2,5)^T = (2,5)^T$, protože tento vektor $(2,5)^T$ leží na přímce p, a $f(-5,2)^T = (5,-2)^T$, protože vektor $(-5,2)^T$ je kolmý na p. Matice f vzhledem k B a K_2 je tedy

$$[f]_{K_2}^B = \begin{pmatrix} 2 & 5 \\ 5 & -2 \end{pmatrix} .$$

Zanedlouho si ukážeme, jak z nalezené matice určit matici f vzhledem k jakýmkoliv jiným bázím, například kanonickým.

Příklad 7.10. Určíme matici derivace chápané jako lineární zobrazení f z prostoru polynomů stupně nejvýše 3 do stejného prostoru vzhledem k bázím $B = (1, x, x^2, x^3)$ a stejné bázi B. K tomu stačí vypočítat vyjádření f-obrazů prvků B vzhledem k bázi B:

$$[1']_B = [0]_B = (0,0,0,0)^T$$
$$[x']_B = [1]_B = (1,0,0,0)^T$$
$$[(x^2)']_B = [2x]_B = (0,2,0,0)^T$$
$$[(x^3)']_B = [3x^2]_B = (0,0,3,0)^T$$

Hledaná matice je

$$[f]_B^B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix} .$$

Matici identity vzhledem k bázím B a C nazýváme maticí přechodu od B k C, protože nám umožňuje rychle počítat souřadnice vektoru vzhledem k C ze souřadnic vzhledem k B.

Definice 7.11. Nechť $\mathbf{V}$ je konečně generovaný prostor a B, C jsou jeho báze. *Maticí přechodu od B k C* rozumíme matici id_V vzhledem k bázím B a C, tj. matici $[\mathrm{id}_V]_C^B$.

V matici přechodu od B k C je tedy čtvercová matice řádu $\dim(\mathbf{V})$, který má v i-tém sloupci vyjádření i-tého vektoru báze B vzhledem k bázi C.

Tvrzení 7.12. *Je-li $\mathbf{V}$ konečně generovaný prostor a B, C jeho báze, pak pro libovolný vektor $\mathbf{x} \in V$ platí*

$$[\mathbf{x}]_C = [\mathrm{id}_V]_C^B[\mathbf{x}]_B .$$

Důkaz. Tvrzení je okamžitým důsledkem tvrzení 7.6. □

Index V budeme většinou vynechávat, tedy píšeme pouze $[\mathrm{id}]_C^B$.

V aritmetických prostorech je snadné určit matici přechodu od dané k bázi ke kanonické. To odpovídá skutečnosti, že souřadnice vzhledem ke kanonické bázi se určí snadno ze souřadnic vzhledem k dané bázi (ale ne naopak).

Příklad 7.13. Matice přechodu od báze $B = ((1,2,3)^T, (6,7,8)^T, (\pi,\pi,10)^T)$ ke kanonické bázi prostoru $\mathbb{R}^3$ je

$$[\mathrm{id}]_{K_3}^B = \begin{pmatrix} 1 & 6 & \pi \\ 2 & 7 & \pi \\ 3 & 8 & 10 \end{pmatrix} ,$$

protože vyjádření i-tého vektoru báze B v kanonické bázi je ten samý vektor.

Příklad 7.14. Matice přechodu od B k B je vždy identická matice, protože vyjádření i-tého vektoru báze B vzhledem k bázi B je $\mathbf{e}_i$.

7.3. **Operace s lineárními zobrazeními.** Lineární zobrazení a matice spolu úzce souvisí, proto není překvapivé, že s lineárními zobrazeními můžeme provádět podobné operace jako s maticemi: můžeme je násobit skalárem, sčítat, násobit (pro zobrazení tím myslíme skládat) a invertovat, samozřejmě jen za určitých podmínek. Přičemž operace s lineárními zobrazeními odpovídají při maticovém popisu příslušným operacím pro matice.

Tvrzení 7.15. *Nechť $\mathbf{V}, \mathbf{W}, \mathbf{Z}$ jsou vektorové prostory nad $\mathbf{T}$, B, C, D báze $\mathbf{V}, \mathbf{W}, \mathbf{Z}$, $f, g : \mathbf{V} \to \mathbf{W}$, $h : \mathbf{W} \to \mathbf{Z}$ a $t \in T$. Pak platí:*

(1) *Zobrazení tf definované vztahem*

$$(tf)(\mathbf{x}) = t \cdot f(\mathbf{x}), \quad \mathbf{x} \in V$$

je lineární zobrazení $\mathbf{V} \to \mathbf{W}$ a platí

$$[tf]_C^B = t[f]_C^B \ .$$

(2) *Zobrazení $f + g$ definované vztahem*

$$(f+g)(\mathbf{x}) = f(\mathbf{x}) + g(\mathbf{x}), \quad \mathbf{x} \in V$$

je lineární zobrazení $\mathbf{V} \to \mathbf{W}$ a platí

$$[f+g]_C^B = [f]_C^B + [g]_C^B \ .$$

(3) *Složené zobrazení hg je lineární zobrazení $\mathbf{V} \to \mathbf{Z}$ a platí*

$$[hg]_D^B = [h]_D^C [g]_C^B \ .$$

(4) *Je-li f bijekce, pak zobrazení f^{-1} je lineární zobrazení $\mathbf{W} \to \mathbf{V}$ a platí*

$$[f^{-1}]_B^C = ([f]_C^B)^{-1} \ .$$

Důkaz. Pro ověření linearity vezmeme libovolné vektory $\mathbf{u}, \mathbf{v} \in V$ a skalár $s \in T$.

(1) Je třeba ověřit, že $(tf)(\mathbf{u}+\mathbf{v}) = (tf)(\mathbf{u}) + (tf)(\mathbf{v})$ a $(tf)(s\mathbf{u}) = s(tf)(\mathbf{u})$. Obojí je snadný výpočet.
(2) Je třeba ověřit, že $(f+g)(\mathbf{u}+\mathbf{v}) = (f+g)(\mathbf{u}) + (f+g)(\mathbf{v})$ a $(f+g)(s\mathbf{u}) = s(f+g)(\mathbf{u})$. Obojí je snadný výpočet.
(3) Zde musíme ověřit, že $(hg)(\mathbf{u}+\mathbf{v}) = (hg)(\mathbf{u}) + (hg)(\mathbf{v})$ a $(hg)(s\mathbf{u}) = s(hg)(\mathbf{u})$. Opět snadné.
(4) V tomto případě ověřujeme $f^{-1}(\mathbf{u}+\mathbf{v}) = f^{-1}(\mathbf{u}) + f^{-1}(\mathbf{v})$ a $f^{-1}(s\mathbf{u}) = sf^{-1}(\mathbf{u})$. Toto vyžaduje drobný trik, podíváme se na první rovnost. Protože f je bijekce, rovnost platí právě tehdy, když platí rovnost $f(f^{-1}(\mathbf{u}+\mathbf{v})) = f(f^{-1}(\mathbf{u}) + f^{-1}(\mathbf{v}))$, tuto novou rovnost již ověříme snadno z linearity f.

Důkaz, že matice zobrazení jsou uvedeny správně můžeme provést v bodech (1),(2) a (3) tak, že zkontrolujeme rovnost v tvrzení 7.6. Opět pouze vypíšeme ověřované rovnosti a jednoduchý výpočet přenecháme čtenáři.

(1) $[(tf)(\mathbf{x})]_C = (t[f]_C^B)[\mathbf{x}]_B$
(2) $[(f+g)(\mathbf{x})]_C = ([f]_C^B + [g]_C^B)[\mathbf{x}]_B$
(3) $[(hg)(\mathbf{x})]_D = ([h]_D^C [g]_C^B)[\mathbf{x}]_B$

U bodu (4) můžeme využít předchozí bod: podle (3) platí $[f^{-1}]_B^C [f]_C^B = [ff^{-1}]_B^B = [\mathrm{id}]_B^B = I_n$, takže skutečně $[f^{-1}]_B^C = ([f]_C^B)^{-1}$. □

Ukážeme si použití pravidel (3) a (4) na početních příkladech.

Příklad 7.16. Určíme matici přechodu od kanonické báze prostoru $\mathbb{R}^2$ k bázi $B = ((2,5)^T, (-5,2)^T)$. Matici přechodu od B ke kanonické bázi určíme snadno.

$$[\mathrm{id}]^B_{K_2} = \begin{pmatrix} 2 & -5 \\ 5 & 2 \end{pmatrix}$$

Využijeme $\mathrm{id}^{-1} = \mathrm{id}$ a (4):

$$[\mathrm{id}]^{K_2}_B = [\mathrm{id}^{-1}]^{K_2}_B = ([\mathrm{id}]^B_{K_2})^{-1} = \begin{pmatrix} 2 & -5 \\ 5 & 2 \end{pmatrix}^{-1} = \frac{1}{29}\begin{pmatrix} 2 & 5 \\ -5 & 2 \end{pmatrix} .$$

Inverzní matici jsme spočítali pomocí adjungované matice (viz příklad 6.39).

Nalezenou matici přechodu můžeme použít k výpočtu matice zrcadlení $f : \mathbb{R}^2 \to \mathbb{R}^2$ podle přímky p procházející počátkem se směrem $(2,5)^T$ vzhledem ke kanonickým bázím. V příkladu 7.9 jsme nahlédli, že matice f vzhledem k B a kanonické bázi je

$$[f]^B_{K_2} = \begin{pmatrix} 2 & 5 \\ 5 & -2 \end{pmatrix} .$$

Pomocí (4) nyní můžeme spočítat matici f vzhledem ke kanonickým bázím:

$$[f]^{K_2}_{K_2} = [f]^B_{K_2}[\mathrm{id}]^{K_2}_B = \begin{pmatrix} 2 & 5 \\ 5 & -2 \end{pmatrix}\frac{1}{29}\begin{pmatrix} 2 & 5 \\ -5 & 2 \end{pmatrix} = \frac{1}{29}\begin{pmatrix} -21 & 20 \\ 20 & 21 \end{pmatrix} .$$

Příklad 7.17. V prostoru $\mathbb{Z}_5^2$ jsou dány báze $B = ((2,4)^T, (3,3)^T)$ a $C = ((1,3)^T, (2,4)^T)$. Vektor $\mathbf{v} \in \mathbb{Z}_5^2$ má vzhledem k bázi B souřadnice $[\mathbf{v}]_B = (x_1, x_2)^T$. Najdeme souřadnice vektoru $\mathbf{v}$ vzhledem k bázi C.

K tomu určíme matici přechodu od B k C užitím (3) a (4):

$$\begin{aligned}[\mathrm{id}]^B_C = [\mathrm{id}]^{K_2}_C[\mathrm{id}]^B_{K_2} = ([\mathrm{id}]^C_{K_2})^{-1}[\mathrm{id}]^B_{K_2} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^{-1}\begin{pmatrix} 2 & 3 \\ 4 & 3 \end{pmatrix} \\ = \frac{1}{3}\begin{pmatrix} 4 & 3 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 2 & 3 \\ 4 & 3 \end{pmatrix} = 2\begin{pmatrix} 0 & 1 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 1 & 3 \end{pmatrix}\end{aligned}$$

Souřadnice $\mathbf{v}$ vzhledem k C jsou

$$[\mathbf{v}]_C = [\mathrm{id}]^B_C[\mathbf{v}]_B = \begin{pmatrix} 0 & 2 \\ 1 & 3 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 2x_2 \\ x_1 + 3x_2 \end{pmatrix} .$$

Výsledek ještě můžeme ověřit například volbou $(x_1, x_2)^T = (1,0)^T$. Je $[\mathbf{v}]_B = (1,0)^T$, takže $\mathbf{v} = (2,4)^T$. Podle odvozeného vzorce by mělo platit $[\mathbf{v}]_C = (0,1)^T$ a skutečně $(2,4)^T = 0 \cdot (1,3)^T + 1 \cdot (2,4)^T$. K nabytí úplné jistoty bychom mohli ještě ověřit pro $(x_1, x_2)^T = (0,1)^T$.

Příklad 7.18. V příkladu 7.7 jsme určili matici lineárního zobrazení $f : \mathbb{Z}_5^3 \to \mathbb{Z}_5^2$ daného předpisem

$$f\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 2x_1 + 3x_2 + x_3 \\ 4x_1 + 2x_3 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 \\ 4 & 0 & 2 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

vzhledem k bázím B a C, kde

$$B = \left(\begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \\ 4 \end{pmatrix}\right) \quad \text{a} \quad C = \left(\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 3 \end{pmatrix}\right) .$$

Spočítáme tuto matici jiným postupem. Ze zadání můžeme přímo určit $[f]^{K_3}_{K_2}$, $[\mathrm{id}]^B_{K_3}$ a $[\mathrm{id}]^C_{K_2}$, pomocí těchto matic lze spočítat $[f]^B_C$ užitím (3) a (4):

$$\begin{aligned}[f]^B_C &= [\mathrm{id}]^{K_2}_C[f]^{K_3}_{K_2}[\mathrm{id}]^B_{K_3} = ([\mathrm{id}]^C_{K_2})^{-1}[f]^{K_3}_{K_2}[\mathrm{id}]^B_{K_3} \\ &= \begin{pmatrix} 1 & 3 \\ 2 & 3 \end{pmatrix}^{-1}\begin{pmatrix} 2 & 3 & 1 \\ 4 & 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 4 \\ 2 & 0 & 4 \end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix} 3 & 2 \\ 3 & 1 \end{pmatrix}\begin{pmatrix} 2 & 0 & 2 \\ 3 & 3 & 0 \end{pmatrix} = 3\begin{pmatrix} 2 & 1 & 1 \\ 4 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 3 \\ 2 & 4 & 3 \end{pmatrix} .\end{aligned}$$

7.4. **Jádro, obraz.** Následující definice zavádí terminologii pro různé typy lineárních zobrazení.

Definice 7.19. Nechť $\mathbf{V}$, $\mathbf{W}$ jsou vektorové prostory nad tělesem $\mathbf{T}$ a $f : \mathbf{V} \to \mathbf{W}$ je lineární zobrazení.

- Pokud f je prosté, říkáme, že f je *monomorfismus*.
- Pokud f je na, říkáme, že f je *epimorfismus*.
- Pokud f je bijekce, říkáme, že f je *izomorfismus*.
- Pokud $\mathbf{V} = \mathbf{W}$, říkáme, že f je *endomorfismus* prostoru $\mathbf{V}$ (též *lineární operátor* na $\mathbf{V}$).
- Pokud $\mathbf{W} = \mathbf{T}$, říkáme, že f je *lineární forma* na $\mathbf{V}$.
- Pokud f je izomorfismus a endomorfismus, říkáme, že f je *automorfismus*.

Příklad 7.20. Rotace a osové souměrnosti jsou automorfismy $\mathbb{R}^2 \to \mathbb{R}^2$.

Zobrazení přiřazující vektoru z $\mathbf{V}$ souřadnice ve zvolené bázi $B = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ je izomorfismus z $\mathbf{V}$ do $\mathbf{T}^n$.

Zobrazení přiřazující vektoru z $\mathbb{R}^3$ jeho orientovanou vzdálenost od zvolené roviny procházející počátkem je lineární forma na $\mathbb{R}^3$, je to epimorfismus, který není monomorfismus.

Projekce na rovinu procházející počátkem (chápaná jako zobrazení $\mathbb{R}^3 \to \mathbb{R}^3$) je endomorfismus, který není ani epimorfismus ani monomorfismus.

Zobrazení $f : \mathbb{R}^2 \to \mathbb{R}^3$ definované vztahem $f(x_1, x_2)^T = (x_1, x_2, 0)^T$ (vložení roviny do $\mathbb{R}^3$) je monomorfismus a není to epimorfismus.

Jako defekt prostoty zavedeme jádro lineárního zobrazení.

Definice 7.21. Nechť $f : \mathbf{V} \to \mathbf{W}$ je lineární zobrazení. *Jádrem* f rozumíme množinu

$$\operatorname{Ker} f = \{\mathbf{x} \in \mathbf{V} : f(\mathbf{x}) = \mathbf{o}\} \ .$$

Snadno se dokáže, že $\operatorname{Ker} f$ je podprostorem $\mathbf{V}$ (viz následující tvrzení). Tento podprostor díky linearitě přesně určuje, které dvojice vektorů se zobrazí na stejný vektor: $f(\mathbf{u}) = f(\mathbf{v})$ platí právě tehdy, když $\mathbf{u} - \mathbf{v} \in \operatorname{Ker} f$ (viz cvičení). To je ilustrováno na obrázku níže, kde $f : \mathbb{R}^3 \to \mathbb{R}^3$ je projekce na přímku p podél roviny U.

OBRAZEK

Z ekvivalence $f(\mathbf{u}) = f(\mathbf{v}) \Leftrightarrow \mathbf{u} - \mathbf{v} \in \operatorname{Ker} f$ je také vidět, že f je monomorfismus právě tehdy, když $\operatorname{Ker} f = \{\mathbf{o}\}$.

Obraz i jádro lineárního zobrazení určíme snadno z jeho libovolné matice – v příslušných bázích je to sloupcový prostor resp. jádro této matice. Toho jsme si již dříve všimli pro zobrazení mezi aritmetickými prostory a jejich matici vzhledem ke kanonickým bázím.

Tvrzení 7.22. *Nechť $\mathbf{V}, \mathbf{W}$ jsou konečně generované vektorové prostory, B je báze $\mathbf{V}$, C je báze $\mathbf{W}$ a $f : \mathbf{V} \to \mathbf{W}$ je lineární zobrazení. Pak platí:*

- *Obraz f je podprostorem $\mathbf{W}$ a platí*
$$[f(V)]_C = \operatorname{Im} [f]_C^B.$$
Speciálně, f je epimorfismus právě tehdy, když $\operatorname{rank}([f]_C^B) = \dim(\mathbf{W})$
- *Jádro f je podprostorem $\mathbf{V}$ a platí*
$$[\operatorname{Ker} f]_B = \operatorname{Ker} [f]_C^B.$$
Speciálně, f je monomorfismus právě tehdy, když $\dim \operatorname{Ker} [f]_C^B = 0$.
- *(věta o dimenzi jádra a obrazu)*
$$\dim(\operatorname{Ker} f) + \dim(f(V)) = \dim(\mathbf{V}) \ .$$

Důkaz.

- Obraz je zřejmě neprázdný. Ověříme uzavřenost na sčítání, uzavřenost na násobení skalárem se dokáže podobně. Jsou-li $\mathbf{w}_1, \mathbf{w}_2 \in W$ v obrazu f, pak existují $\mathbf{v}_1, \mathbf{v}_1 \in V$ takové, že $f(\mathbf{v}_1) = \mathbf{w}_1$ a $f(\mathbf{v}_2) = \mathbf{w}_2$. Z linearity $f(\mathbf{v}_1 + \mathbf{v}_2) = f(\mathbf{v}_1) + f(\mathbf{v}_2) = \mathbf{w}_1 + \mathbf{w}_2$, takže v obrazu leží i součet $\mathbf{w}_1 + \mathbf{w}_2$.

  Z tvrzení 7.6 o matici homomorfismu dostáváme
$$\begin{aligned}[f(V)]_C &= [\{f(\mathbf{v}) : \mathbf{v} \in V]_C = \{[f(\mathbf{v})]_C : \mathbf{v} \in V\} = \{[f]_C^B [\mathbf{v}]_B : \mathbf{v} \in V\} \\ &= \{[f]_C^B \mathbf{x} : \mathbf{x} \in T^{\dim(V)}\} = \operatorname{Im} [f]_C^B \ .\end{aligned}$$
- Jádro je neprázdné, protože obsahuje nulový vektor. Je uzavřené na sčítání, protože z $\mathbf{u}, \mathbf{v} \in \operatorname{Ker} f$ plyne $f(\mathbf{u} + \mathbf{v}) = f(\mathbf{u}) + f(\mathbf{v}) = \mathbf{o}$, čili $\mathbf{u} + \mathbf{v} \in \operatorname{Ker} f$, a podobně se ukáže uzavřenost na násobení skalárem.

  Použijeme opět vzorec pro matici homomorfismu:
$$\begin{aligned}[\operatorname{Ker} f]_B &= [\{\mathbf{v} : f(\mathbf{v}) = \mathbf{o}\}]_B = \{[\mathbf{v}]_B : f(\mathbf{v}) = \mathbf{o}\} = \{[\mathbf{v}]_B : [f(\mathbf{v})]_C = \mathbf{o}\} \\ &= \{[\mathbf{v}]_B : [f]_C^B [\mathbf{v}]_B = \mathbf{o}\} = \{\mathbf{x} \in T^{\dim(V)} : [f]_C^B \mathbf{x} = \mathbf{o}\} = \operatorname{Ker} [f]_C^B\end{aligned}$$

- Z předchozích bodů vyplývá, že dimenze obrazu f je rovná dimenzi sloupcového prostoru matice $[f]_C^B$ a dimenze jádra f je rovná dimenzi jádra $[f]_C^B$. Matice $[f]_C^B$ má $\dim(V)$ sloupců, takže tvrzení vyplývá z věty 5.83 o dimenzi jádra a obrazu pro matice.

□

Příklad 7.23. Lineární zobrazení $f : \mathbb{R}^3 \to \mathbb{R}^2$ máme dáno maticí vzhledem k bázím B a C:

$$B = \left(\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ 3 \\ 0 \end{pmatrix} \right), \quad C = \left(\begin{pmatrix} 3 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \end{pmatrix} \right),$$

$$A = [f]_C^B = \begin{pmatrix} 2 & 1 & -3 \\ -4 & -2 & 6 \end{pmatrix} .$$

Určíme $\operatorname{Ker} f$ a $f(\mathbb{R}^3)$.

Nejprve spočítáme $\operatorname{Ker} A$ (tj. určíme nějakou bázi $\operatorname{Ker} A$), tedy vyřešíme homogenní soustavu rovnic s maticí A.

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

Báze $\operatorname{Ker} A$ je například $(-1, 2, 0)^T, (3, 0, 2)^T$ (za parametry jsme volili $(2, 0)^T$ a $(0, 2)^T$, aby vycházela hezčí čísla). Takže

$$[\operatorname{Ker} f]_B = \operatorname{Ker} A = \left\langle \begin{pmatrix} -1 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 0 \\ 2 \end{pmatrix} \right\rangle ,$$

z čehož dopočteme

$$\begin{aligned} \operatorname{Ker} f &= \left\langle -1 \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + 2 \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}, 3 \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + 2 \begin{pmatrix} 3 \\ 3 \\ 0 \end{pmatrix} \right\rangle \\ &= \left\langle \begin{pmatrix} 3 \\ -2 \\ -1 \end{pmatrix}, \begin{pmatrix} 9 \\ 12 \\ 9 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} 3 \\ -2 \\ -1 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \\ 3 \end{pmatrix} \right\rangle \end{aligned}$$

Nyní řádkovými úpravami určíme bázi $\operatorname{Im} A$:

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

Takže

$$[f(\mathbb{R}^3)]_C = \operatorname{Im} A = \left\langle \begin{pmatrix} 1 \\ -2 \end{pmatrix} \right\rangle$$

a

$$f(\mathbb{R}^3) = \left\langle 1 \begin{pmatrix} 3 \\ 1 \end{pmatrix} - 2 \begin{pmatrix} -1 \\ 1 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} 5 \\ -1 \end{pmatrix} \right\rangle$$

Dimenze jádra f je 2 a dimenze obrazu f je 1, což je v souladu s větou o dimenzi jádra a obrazu. Zobrazení f je znázorněné na obrázku

OBRAZEK

7.4.1. *Izomorfismus.* Krátce se ještě zastavíme u pojmu izomorfismu.

Předpokládejme, že $\mathbf{V}$ a $\mathbf{W}$ jsou konečně generované prostory a $f : \mathbf{V} \to \mathbf{W}$ je izomorfismus (předpoklad o konečné generovanosti lze vynechat, ale my jsme tvrzení v této kapitole formulovali jen pro takové prostory). Pak $\dim(f(V)) = \dim(W)$ a $\dim(\operatorname{Ker} f) = 0$. Z věty o dimenzi jádra a obrazu dostáváme $\dim(W) = \dim(V)$. Naopak, mezi prostory stejné dimenze vždy existuje izomorfismus, stačí bázi jednoho prostoru zobrazit na bázi druhého prostoru:

Věta 7.24. *Nechť $\mathbf{V}$ a $\mathbf{W}$ jsou dva konečně generované prostory. Pak následující tvrzení jsou ekvivalentní:*

(1) *Existuje izomorfismus $f : \mathbf{V} \to \mathbf{W}$.*
(2) $\dim(\mathbf{V}) = \dim(\mathbf{W})$.

Důkaz. Implikace (1) ⇒ (2) byla dokázána před větou. Jiný důkaz je ve cvičeních.

Rozvedeme myšlenku důkazu druhé implikace. Zvolíme bázi $B = (\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$ prostoru $\mathbf{V}$ a bázi $C = (\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_n)$ prostoru $\mathbf{W}$ a vezeme lineární zobrazení $f : \mathbf{V} \to \mathbf{W}$ splňující $f(\mathbf{v}_i) = \mathbf{w}_i$ pro každé $i \in \{1, 2, \dots, n\}$ (takové lineární zobrazení existuje podle tvrzení 7.4 o rozšiřování zobrazení definovaného na bázi na lineární zobrazení). Toto lineární zobrazení je izomorfismem například proto, že $[f]_C^B = I_n$, takže f je prosté i na podle tvrzení 7.22 o jádře a obrazu. □

Izomorfismus je bijektivní zobrazení, které zachovává obě operace ve vektorovém prostoru. Izomorfní prostory (tedy prostory, mezi kterými existuje izomorfismus) jsou tedy „v podstatě“ stejné, liší se jenom přejmenováním vektorů. Ještě trochu jinak řečeno, vektory v izomorfních prostorech mohou „vypadat“ jinak, ale „chovají se“ naprosto stejně. Předchozí tvrzení vlastně znova formuluje skutečnost, že vektorový prostor nad daným tělesem dané dimenze je „v podstatě“ jen jeden (např. $\mathbf{T}^n$).

Jak poznáme, že lineární zobrazení $f : \mathbf{V} \to \mathbf{W}$ je izomorfismus podle jeho matice vzhledem k nějakým bázím? Protože musí platit $\dim(V) = \dim(W)$, musí být čtvercová. Navíc (například z $\operatorname{Ker} f = \{\mathbf{o}\}$) musí být tato matice regulární. A naopak, regulární matice je vždy maticí izomorfismu. Důkaz přenecháme jako cvičení, rovněž srovnejte s body (1)–(4) z charakterizační věty 4.30 regulárních matic.

Tvrzení 7.25. *Nechť $\mathbf{V}, \mathbf{W}$ jsou vektorové prostory nad tělesem $\mathbf{T}$ stejné, konečné dimenze, B je báze $\mathbf{V}$, C je báze $\mathbf{W}$ a $f : \mathbf{V} \to \mathbf{W}$ je lineární zobrazení. Pak je ekvivalentní*

(1) *f je izomorfismus.*
(2) *f je monomorfismus.*
(3) *f je epimorfismus.*
(4) *$[f]_C^B$ je regulární matice.*

Cvičení

1. Zobecněte tvrzení 7.4 na případ nekonečné dimenze.

2. Dokažte, že matice $[f]_C^B$ v tvrzení 7.6 je jediná matice splňující rovnost $[f(\mathbf{x})]_C = [f]_C^B[\mathbf{x}]_B$.

3. Nechť $f : \mathbf{V} \to \mathbf{W}$ je lineární zobrazení. Dokažte, že $f(\mathbf{u}) = f(\mathbf{v})$ právě tehdy, když $\mathbf{u} - \mathbf{v} \in \operatorname{Ker} f$.

4. Nechť $f : \mathbf{V} \to \mathbf{W}$ je lineární zobrazení a B je báze $\mathbf{V}$. Dokažte, že f je monomorfismus právě tehdy, když obraz B je lineárně nezávislá posloupnost.

5. Nechť $f : \mathbf{V} \to \mathbf{W}$ je lineární zobrazení a B je báze $\mathbf{V}$. Dokažte, že f je epimorfismus právě tehdy, když obraz B generuje $\mathbf{W}$.

6. Nechť $f : \mathbf{V} \to \mathbf{W}$ je lineární zobrazení a B je báze $\mathbf{V}$. Dokažte, že f je izomorfismus právě tehdy, když obraz B je báze $\mathbf{W}$. To podává jiný důkaz implikace (1) ⇒ (2) ve větě 7.24.

7. Nechť $\mathbf{V}, \mathbf{W}$ jsou konečně generované prostory nad tělesem $\mathbf{T}$. Ukažte, že množina všech lineárních zobrazení z $\mathbf{V}$ do $\mathbf{W}$ tvoří vektorový prostor izomorfní $\mathbf{T}^{\dim(\mathbf{W}) \times \dim(\mathbf{V})}$.

8. Dokažte 7.25.

8. Skalární součin

Cíl. .

V abstraktním vektorovém prostoru nemáme metrické pojmy jako délka vektoru nebo úhel dvou vektorů. Tyto pojmy zavedeme přidáním skalárního součinu.

8.1. Standardní skalární součin v $\mathbb{R}^n$ a $\mathbb{C}^n$.

8.1.1. $\mathbb{R}^n$. Podíváme se nejprve na standardní skalární součin $\cdot$ v aritmetickém vektorovém prostoru $\mathbb{R}^n$. Pro dva vektory $\mathbf{u} = (x_1, x_2, \dots, x_n)^T$, $\mathbf{v} = (y_1, y_2, \dots, y_n)$ v $\mathbb{R}^n$ je definován vztahem

$$\mathbf{u} \cdot \mathbf{v} = \mathbf{u}^T \mathbf{v} = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n \ .$$

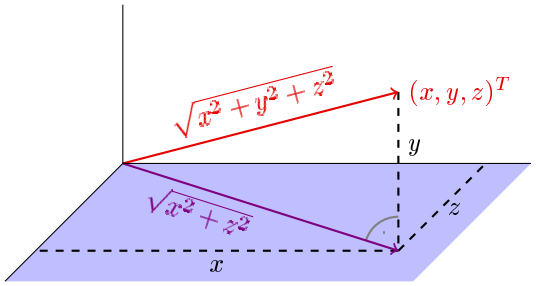
Pomocí standardního skalárního součinu můžeme vyjádřit eukleidovskou délku (též zvanou normu) vektoru $\mathbf{u} \in \mathbb{R}^n$.

$$\|\mathbf{u}\| = \sqrt{\mathbf{u} \cdot \mathbf{u}} \ .$$

Délka vektoru $\mathbf{u} = (x_1, x_2, \dots, x_n)^T$ je podle vzorce

$$\|\mathbf{u}\| = \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2} \ ,$$

což pro $n = 2$ a $n = 3$ vidíme z Pythagorovy věty (a pro $n = 1$ máme $\|\mathbf{u}\| = |x_1|$, což rovněž souhlasí).



Obrázek 13. Eukleidovská norma v $\mathbb{R}^3$

Ze standardního skalárního součinu můžeme rovněž určit úhel α mezi vektory $\mathbf{u}$ a $\mathbf{v}$. Platí totiž

$$\mathbf{u} \cdot \mathbf{v} = \|\mathbf{u}\| \cdot \|\mathbf{v}\| \cdot \cos\alpha \ .$$

Přesvědčíme se o platnosti tohoto vztahu tak, že zapomeneme na chvíli na původní definici standardního skalárního součinu, místo toho budeme za definici považovat tento vztah a původní vzorec odvodíme. Při odvozování budeme používat geometrickou intuici, takže si budeme představovat situaci $n = 2$ nebo $n = 3$.

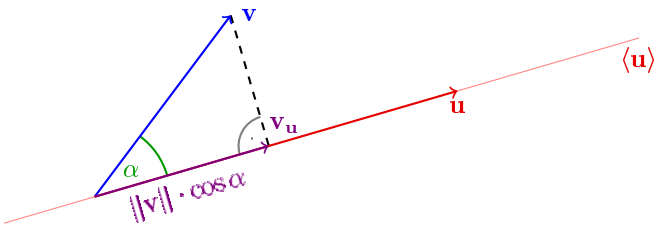
Nejprve si všimneme, že výraz je symetrický, tedy

$$\mathbf{u} \cdot \mathbf{v} = \mathbf{v} \cdot \mathbf{u} \ ,$$

a že délka vektoru $\mathbf{u}$ je rovná

$$\|\mathbf{u}\| = \sqrt{\mathbf{u} \cdot \mathbf{u}} \ .$$

Výraz $\|\mathbf{u}\| \cdot \|\mathbf{v}\| \cdot \cos\alpha$ můžeme chápat jako součin délky vektoru $\mathbf{u}$ a délky ortogonální (kolmé) projekce $\mathbf{v_u}$ vektoru $\mathbf{v}$ na přímku $\langle \mathbf{u} \rangle$:



Obrázek 14. Geometrický význam standardního skalárního součinu

(Symetricky se na výraz můžeme dívat jako na součin délky $\mathbf{v}$ a délky ortogonální projekce $\mathbf{u_v}$.)

Z toho můžeme nahlédnout, že skalární součin je lineární v první proměnné, tj. pro libovolné $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w} \in \mathbb{R}^n$ a $t \in \mathbb{R}$ platí

$$(t\mathbf{u}) \cdot \mathbf{v} = t(\mathbf{u} \cdot \mathbf{v}), \quad (\mathbf{u} + \mathbf{v}) \cdot \mathbf{w} = \mathbf{u} \cdot \mathbf{w} + \mathbf{v} \cdot \mathbf{w} \ .$$

OBRAZEK

Ze symetrie nebo podobným odvozením získáme linearitu v druhé proměnné

$$\mathbf{u} \cdot (t\mathbf{v}) = t(\mathbf{u} \cdot \mathbf{v}), \quad \mathbf{u} \cdot (\mathbf{v} + \mathbf{w}) = \mathbf{u} \cdot \mathbf{v} + \mathbf{u} \cdot \mathbf{w} \ .$$

Vektory kanonické báze jsou na sebe kolmé a mají délku 1, takže

$$\mathbf{e}_i \mathbf{e}_j = 0 \ \ (i \neq j), \quad \mathbf{e}_i \cdot \mathbf{e}_i = 1 \ .$$

Z odvozených vztahů dostaneme původní vzorec pro skalární součin součin $\mathbf{u} = (x_1, x_2, \ldots, x_n)^T$ a $\mathbf{v} = (y_1, y_2, \ldots, y_n)^T$. Pro přehlednost uvedeme nejprve odvození v případě $n = 2$.

$$\begin{aligned}
\mathbf{u} \cdot \mathbf{v} &= (x_1\mathbf{e}_1 + x_2\mathbf{e}_2) \cdot (y_1\mathbf{e}_1 + y_2\mathbf{e}_2) \\
&= (x_1\mathbf{e}_1) \cdot (y_1\mathbf{e}_1 + y_2\mathbf{e}_2) + (x_2\mathbf{e}_2) \cdot (y_1\mathbf{e}_1 + y_2\mathbf{e}_2) \\
&= (x_1\mathbf{e}_1) \cdot (y_1\mathbf{e}_1) + (x_1\mathbf{e}_1) \cdot (y_2\mathbf{e}_2) + (x_2\mathbf{e}_2) \cdot (y_1\mathbf{e}_1) + (x_2\mathbf{e}_2) \cdot (y_2\mathbf{e}_2) \\
&= x_1y_1(\mathbf{e}_1 \cdot \mathbf{e}_1) + x_1y_2(\mathbf{e}_1 \cdot \mathbf{e}_2) + x_2y_1(\mathbf{e}_2 \cdot \mathbf{e}_1) + x_2y_2(\mathbf{e}_2 \cdot \mathbf{e}_2) \\
&= x_1y_1 + x_2y_2
\end{aligned}$$

Obdobně v obecném případě:

$$\begin{aligned}
\mathbf{u} \cdot \mathbf{v} &= \left(\sum_{i=1}^{n} x_i\mathbf{e}_i\right) \cdot \left(\sum_{i=1}^{n} y_i\mathbf{e}_i\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} (x_i\mathbf{e}_i) \cdot (y_j\mathbf{e}_j) \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n} x_iy_j(\mathbf{e}_i \cdot \mathbf{e}_k) = \sum_{i=1}^{n} x_iy_i
\end{aligned}$$

Všimněte si, že odvození probíhalo podobně jako odvození vzorce pro determinant: Ukázali jsme linearitu ve všech proměnných a všimli jsme si, jak skalární součin (determinant) vypadá na kanonické bázi.

8.1.2. $\mathbb{C}^n$. Nad komplexními čísly je standardní skalární součin vektorů $\mathbf{u} = (x_1, x_2, \ldots, x_n)^T$ a $\mathbf{v} = (y_1, y_2, \ldots, y_n)^T$ definován trochu jiným vzorcem:

$$\mathbf{u} \cdot \mathbf{v} = \overline{x_1}y_1 + \overline{x_2}y_2 + \cdots + \overline{x_n}y_n \ ,$$

kde $\overline{x}$ značí číslo komplexně sdružené k x, tj. $\overline{a + bi} = a - bi$. Pro reálné vektory tato definice souhlasí s předchozí, protože komplexní sdružování s reálnými čísly nic nedělá.

Výhodou takové definice je třeba to, že skalární součin $\mathbf{u} \cdot \mathbf{u}$ je vždy kladné reálné číslo (je součtem druhých mocnin absolutních hodnot složek), takže délka definovaná vztahem $\mathbf{u} = \sqrt{\mathbf{u} \cdot \mathbf{u}}$ je reálné číslo, které je nulové právě tehdy, když $\mathbf{u} = \mathbf{o}$. (Pokud bychom definovali skalární součin bez komplexního sdružování, výraz $\mathbf{u} \cdot \mathbf{u}$ by nebyl vždy reálný a byl by roven nule i pro některé nenulové vektory.)

V reálném případě můžeme standardní skalární součin definovat maticovým součinem $\mathbf{u}^T\mathbf{v}$. Abychom mohli maticově zapsat standardní skalární součin nad komplexními čísly, zavedeme pojem hermitovsky sdružené matice.

Definice 8.1. *Hermitovsky sdružená matice* k matici $A = (a_{ij})_{m\times n}$ je matice $A^* = (b_{ji})_{n\times m}$, kde $b_{ji} = \overline{a_{ij}}$ pro libovolné indexy $i \in \{1, 2, \ldots, m\}$ a $j \in \{1, 2, \ldots, n\}$.

Hermitovsky sdruženou matici k A tedy dostaneme transponováním a nahrazením všech prvků prvky komplexně sdruženými. Hermitovské sdružování se chová k ostatním operacím podobně jako transponování, viz cvičení.

Příklad 8.2.

$$\begin{pmatrix} 1+2i & 3 & i \\ 0 & 3-2i & 4i \end{pmatrix}^* = \begin{pmatrix} 1-2i & 0 \\ 3 & 3+2i \\ -i & -4i \end{pmatrix}$$

S tímto značením můžeme psát

$$\mathbf{u} \cdot \mathbf{v} = \mathbf{u}^*\mathbf{v}$$

Standardní skalární součin nad komplexními čísly je stále lineární v druhé proměnné a platí $(\mathbf{u}+\mathbf{v})\cdot\mathbf{w} = \mathbf{u}\cdot\mathbf{w}+\mathbf{v}\cdot\mathbf{w}$, ale není lineární v první proměnné a není symetrický. Místo toho máme pro $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w} \in \mathbb{C}^n$ a $t \in \mathbb{C}$ vztahy

$$(t\mathbf{u}) \cdot \mathbf{v} = \overline{t}(\mathbf{u} \cdot \mathbf{v}), \quad \mathbf{v} \cdot \mathbf{u} = \overline{\mathbf{u} \cdot \mathbf{v}} \ .$$

8.2. **Obecný skalární součin.** Obecně definujeme skalární součin jako zobrazení přiřazující dvojici vektorů skalár, které má podobné vlastnosti jako standardní skalární součin. Skalární součin vektorů $\mathbf{u}$ a $\mathbf{v}$ budeme značit $\langle \mathbf{u} \,|\, \mathbf{v} \rangle$, značení $\mathbf{u} \cdot \mathbf{v}$ budeme používat pouze pro standardního skalární součin v $\mathbb{R}^n$ nebo $\mathbb{C}^n$. Skalární součin se definuje **pouze pro vektorové prostory nad tělesem $\mathbb{R}$ nebo $\mathbb{C}$.**

Definice 8.3. Nechť V je vektorový prostor nad $\mathbb{R}$ (resp. nad $\mathbb{C}$). Zobrazení $\langle \,|\, \rangle$ z $V \times V$ do $\mathbb{R}$ (resp do $\mathbb{C}$), které dvojici $\mathbf{u}, \mathbf{v}$ přiřadí vektor $\langle \mathbf{u} \,|\, \mathbf{v} \rangle$, se nazývá *skalární součin*, pokud pro libovolné $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ a $t \in \mathbb{R}$ (resp. $t \in \mathbb{C}$) platí

(SL1) $\langle t\mathbf{u} \,|\, \mathbf{v} \rangle = \overline{t} \, \langle \mathbf{u} \,|\, \mathbf{v} \rangle$, $\langle \mathbf{u} \,|\, t\mathbf{v} \rangle = t \, \langle \mathbf{u} \,|\, \mathbf{v} \rangle$,
(SL2) $\langle \mathbf{u} + \mathbf{v} \,|\, \mathbf{w} \rangle = \langle \mathbf{u} \,|\, \mathbf{w} \rangle + \langle \mathbf{v} \,|\, \mathbf{w} \rangle$, $\langle \mathbf{u} \,|\, \mathbf{v} + \mathbf{w} \rangle = \langle \mathbf{u} \,|\, \mathbf{v} \rangle + \langle \mathbf{u} \,|\, \mathbf{w} \rangle$,
(SCS) $\langle \mathbf{v} \,|\, \mathbf{u} \rangle = \overline{\langle \mathbf{u} \,|\, \mathbf{v} \rangle}$ a
(SP) $\langle \mathbf{u} \,|\, \mathbf{u} \rangle$ je nezáporné reálné číslo, které je nulové právě tehdy, když $\mathbf{u} = \mathbf{o}$.

Axiomy nejsou nezávislé, například druhé části axiomů linearity (SL1) a (SL2) vyplývají ze zbylých axiomů. Z axiomu (SL1) plyne, že $\langle \mathbf{u} \,|\, \mathbf{o} \rangle = \langle \mathbf{o} \,|\, \mathbf{u} \rangle = 0$. V případě reálných vektorových prostorů můžeme v axiomech (SL1) a (SCS) vynechat komplexní sdružení.

8.2.1. *Příklady.*

- Standardní skalární součin v $\mathbb{R}^n$ (resp. $\mathbb{C}^n$) je skalárním součinem v $\mathbb{R}^n$ (resp. $\mathbb{C}^n$). Všechny vlastnosti se ověří snadno z definice.
- Je-li A čtvercová matice nad $\mathbb{R}$ (resp. $\mathbb{C}$), pak zobrazení z $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ (resp. $\mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$) definované vztahem
$$\langle \mathbf{u} \,|\, \mathbf{v} \rangle = \mathbf{u}^* A \mathbf{v}$$
vždy splňuje (SL1) a (SL2) (cvičení). Vlastnost (SCS) je splněna právě tehdy, když $A^* = A$ (cvičení). V reálném případě to znamená, že A je symetrická, v komplexním případě se maticím splňujícím $A^* = A$ říká *hermitovské*. Hermitovským maticím, pro které takto definované zobrazení splňuje i (SP) se říká pozitivně definitní.

  Definice 8.4. Hermitovská matice A řádu n se nazývá *pozitivně definitní*, pokud $\mathbf{u}^* A \mathbf{u}$ je pro libovolné $\mathbf{u} \in \mathbb{C}^n$ nezáporné reálné číslo, které je nulové právě když $\mathbf{u} = \mathbf{o}$.

  Příkladem pozitivně definitních matic (viz cvičení) jsou matice typu $A = B^*B$, kde B je regulární matice řádu n nad $\mathbb{R}$ (resp. nad $\mathbb{C}$). Později ukážeme, že platí i opak, tj. každá pozitivně definitní matice A je tvaru $A = B^*B$, pro regulární matici B. Dokonce každý skalární součin na $\mathbb{R}^n$ (a na $\mathbb{C}^n$) je tohoto tvaru.

  Shrnutí: Je-li $A = B^*B$, pak zobrazení definované $\langle \mathbf{u} \,|\, \mathbf{v} \rangle = \mathbf{u}^* A \mathbf{v}$ je skalární součin. Pro $A = I_n$ dostáváme standardní skalární součin. Jako ukázku jiného konkrétního příkladu vezmeme
$$B = \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix} ,$$
  tedy
$$A = B^*B = B^TB = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix} = \begin{pmatrix} 5 & -2 \\ -2 & 1 \end{pmatrix} .$$
  Příslušný skalární součin v $\mathbb{C}^n$ je dán vztahem
$$\langle \mathbf{u} \,|\, \mathbf{v} \rangle = (\overline{x_1}, \overline{x_2}) \begin{pmatrix} 5 & -2 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = 5\overline{x_1}y_1 - 2\overline{x_1}y_2 - 2\overline{x_2}y_1 + \overline{x_2}y_2$$
  kde $\mathbf{u} = (x_1, x_2)^T$ a $\mathbf{v} = (y_1, y_2)^T$. Stejný vztah (kde nemusíme komplexně sdružovat) definuje skalární součin v $\mathbb{R}^n$.
- Na prostoru spojitých reálných (nebo komplexních) funkcí na intervalu $\langle 1, 10 \rangle$ je
$$\langle \mathbf{u} \,|\, \mathbf{v} \rangle = \int_1^{10} \overline{\mathbf{u}} \mathbf{v}$$
  skalární součin. Obecněji například
$$\langle \mathbf{u} \,|\, \mathbf{v} \rangle = \int_1^{10} \overline{\mathbf{u}} \mathbf{v} \mathbf{w} \ ,$$
  kde $\mathbf{w}$ je nějaká kladná váhová funkce.

8.2.2. *Norma.* Normu vektoru v prostoru se skalárním součinem zavedeme stejným vztahem jakým jsme vyjádřili eukleidovskou normu (délku) pomocí standardního skalárního součinu.

Definice 8.5. Nechť V je vektorový prostor se skalárním součinem $\langle\,|\,\rangle$. *Normou* vektoru $\mathbf{v} \in V$ rozumíme reálné číslo

$$\|\mathbf{u}\| = \sqrt{\langle \mathbf{u}\,|\,\mathbf{u}\rangle}\ .$$

Vektor $\mathbf{u}$ se nazývá *jednotkový*, pokud $\|\mathbf{u}\| = 1$.

Definice dává smysl, protože výraz pod odmocninou je podle (SP) vždy nezáporné reálné číslo. Norma závisí na skalárním součinu, takže když používáme symbol normy, musí být z kontextu jasné, se kterým skalárním součinem pracujeme. Podobně i pro další pojmy jako úhel nebo kolmost, které budou zavedeny později.

Příklad 8.6. Norma vektoru $(1+i, 2, 3-2i)^T$ v prostoru $\mathbb{C}^3$ se standardním skalárním součinem je

$$\left\| \begin{pmatrix} 1+i \\ 2 \\ 3-2i \end{pmatrix} \right\| = \sqrt{\begin{pmatrix} 1-i \\ 2 \\ 3+2i \end{pmatrix} \cdot \begin{pmatrix} 1+i \\ 2 \\ 3-2i \end{pmatrix}} = \sqrt{|1+i|^2 + |2|^2 + |3+2i|^2} = \sqrt{17}\ .$$

Norma určená skalárním součinem má následující vlastnosti.

Tvrzení 8.7. *Nechť V je vektorový prostor nad $\mathbb{R}$ (resp. $\mathbb{C}$) se skalárním součinem $\langle\,|\,\rangle$, $\mathbf{u}, \mathbf{v} \in V$ a $t \in \mathbb{R}$ (resp. $t \in \mathbb{C}$). Pak platí*

(1) $\|\mathbf{u}\| \geq 0$, *přičemž* $\|\mathbf{u}\| = 0$ *právě tehdy, když* $\mathbf{u} = \mathbf{o}$.
(2) $\|t\mathbf{u}\| = |t|\,\|\mathbf{u}\|$.
(3) *(Rovnoběžníkové pravidlo.)* $\|\mathbf{u}+\mathbf{v}\|^2 + \|\mathbf{u}-\mathbf{v}\|^2 = 2\,\|\mathbf{u}\|^2 + 2\,\|\mathbf{v}\|^2$.
(4) *(Polarizační identita.)* $\mathrm{Re}(\langle \mathbf{u}\,|\,\mathbf{v}\rangle) = \frac{1}{2}(\|\mathbf{u}+\mathbf{v}\|^2 - \|\mathbf{u}\|^2 - \|\mathbf{v}\|^2)$, *kde* $\mathrm{Re}(x)$ *značí reálnou část* x.

Důkaz.

(1) Snadný důsledek (SP).
(2) Použitím (SL1) dostáváme

$$\|t\mathbf{u}\| = \sqrt{\langle t\mathbf{u}\,|\,t\mathbf{u}\rangle} = \sqrt{t\bar{t}\,\langle \mathbf{u}\,|\,\mathbf{u}\rangle} = \sqrt{|t|^2\,\langle \mathbf{u}\,|\,\mathbf{u}\rangle} = |t|\sqrt{\langle \mathbf{u}\,|\,\mathbf{u}\rangle} = |t|\,\|\mathbf{u}\|\ .$$

(3) Ve výpočtu stačí použít (SL2).

$$\begin{aligned} \|\mathbf{u}+\mathbf{v}\|^2 + \|\mathbf{u}-\mathbf{v}\|^2 &= \langle \mathbf{u}+\mathbf{v}\,|\,\mathbf{u}+\mathbf{v}\rangle + \langle \mathbf{u}-\mathbf{v}\,|\,\mathbf{u}-\mathbf{v}\rangle \\ &= \langle \mathbf{u}\,|\,\mathbf{u}\rangle + \langle \mathbf{u}\,|\,\mathbf{v}\rangle + \langle \mathbf{v}\,|\,\mathbf{u}\rangle + \langle \mathbf{v}\,|\,\mathbf{v}\rangle \\ &\quad + \langle \mathbf{u}\,|\,\mathbf{u}\rangle - \langle \mathbf{u}\,|\,\mathbf{v}\rangle - \langle \mathbf{v}\,|\,\mathbf{u}\rangle + \langle \mathbf{v}\,|\,\mathbf{v}\rangle \\ &= 2\,\langle \mathbf{u}\,|\,\mathbf{u}\rangle + 2\,\langle \mathbf{v}\,|\,\mathbf{v}\rangle = 2\,\|\mathbf{u}\|^2 + 2\,\|\mathbf{v}\|^2 \end{aligned}$$

(4) Ze (SL2) a (SCS) vypočteme

$$\|\mathbf{u}+\mathbf{v}\|^2 = \langle \mathbf{u}\,|\,\mathbf{u}\rangle + \langle \mathbf{u}\,|\,\mathbf{v}\rangle + \langle \mathbf{v}\,|\,\mathbf{u}\rangle + \langle \mathbf{v}\,|\,\mathbf{v}\rangle = \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 + \langle \mathbf{u}\,|\,\mathbf{v}\rangle + \overline{\langle \mathbf{u}\,|\,\mathbf{v}\rangle}\ .$$

Protože $x + \overline{x} = 2\mathrm{Re}(x)$, dostáváme

$$2\mathrm{Re}(\langle \mathbf{u}\,|\,\mathbf{v}\rangle) = \|\mathbf{u}+\mathbf{v}\|^2 - \|\mathbf{u}\|^2 - \|\mathbf{v}\|^2\ .$$

□

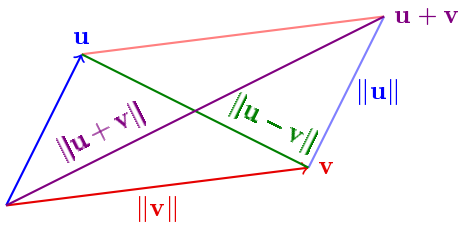
Důsledkem (1) a (2) je, že pro nenulový vektor $\mathbf{u}$ je jeho násobek

$$\frac{\mathbf{u}}{\|\mathbf{u}\|}$$

jednotkový vektor. Říkáme, že $\frac{\mathbf{u}}{\|\mathbf{u}\|}$ vznikl z $\mathbf{u}$ *znormováním*.

Rovnoběžníkové pravidlo je ilustrováno na obrázku.

Polarizační identita vyjadřuje reálnou část skalárního součinu pouze pomocí normy. Podobný vztah jde napsat i pro imaginární část (pokud pracujeme v prostoru nad $\mathbb{C}$), viz cvičení. Skalární součin je tedy určen normou. Různé další varianty polarizační identity jsou ve cvičeních.



Obrázek 15. Rovnoběžníkové pravidlo

8.2.3. *Cauchy-Schwarzova nerovnost, úhel.* Pro vektory $\mathbf{u}, \mathbf{v} \in \mathbb{R}^3$ jsme nahlédli, že $\mathbf{u} \cdot \mathbf{v} = \|\mathbf{u}\| \, \|\mathbf{v}\| \cos\alpha$. Z toho také vyplývá, že absolutní hodnota $|\mathbf{u} \cdot \mathbf{v}|$ nemůže být větší než součin norem $\|\mathbf{u}\| \, \|\mathbf{v}\|$, protože kosinus úhlu je vždy v intervalu $\langle -1, 1 \rangle$.

Vztah $\langle \mathbf{u} \, | \mathbf{v} \rangle = \|\mathbf{u}\| \, \|\mathbf{v}\| \cos\alpha$ jde naopak použít pro zavedení úhlu mezi dvěma vektory v libovolném prostoru se skalárním součinem. Aby byl úhel dobře definován, musíme dokázat, že obecně platí $|\langle \mathbf{u} \, | \mathbf{v} \rangle| \leq \|\mathbf{u}\| \, \|\mathbf{v}\|$. Tato nerovnost se nazývá Cauchy-Schwarzova nerovnost (též Bunjakovského nerovnost, nebo Cauchy-Schwarzova-Bunjakovského nerovnost, apod.) a je asi jednou z nejdůležitějších nerovností v matematice.

Věta 8.8 (Cauchy-Schwarzova nerovnost)**.** *Nechť V je vektorový prostor se skalárním součinem $\langle \, | \, \rangle$ a $\mathbf{u}, \mathbf{v} \in \mathbf{V}$. Pak platí*

$$|\langle \mathbf{u} \, | \mathbf{v} \rangle| \leq \|\mathbf{u}\| \, \|\mathbf{v}\| \quad ,$$

přičemž rovnost nastává právě tehdy, když $(\mathbf{u}, \mathbf{v})$ je lineárně závislá posloupnost.

Důkaz. Pokud je posloupnost $(\mathbf{u}, \mathbf{v})$ lineárně závislá, pak $\mathbf{u} = t\mathbf{v}$ nebo $\mathbf{v} = t\mathbf{u}$ pro nějaké $t \in \mathbb{C}$. V prvním případě je

$$|\langle \mathbf{u} \, | \mathbf{v} \rangle| = |\langle t\mathbf{v} \, | \mathbf{v} \rangle| = |\bar{t} \, \langle \mathbf{v} \, | \mathbf{v} \rangle| = |t| \, \|\mathbf{v}\|^2$$

a

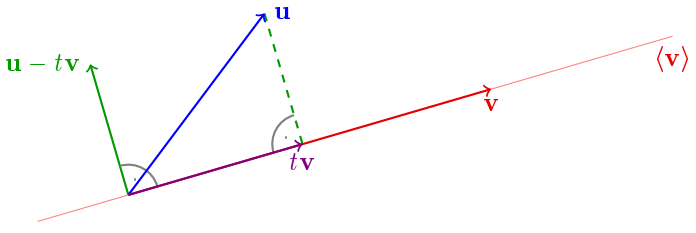
$$\|\mathbf{u}\| \, \|\mathbf{v}\| = \|t\mathbf{v}\| \, \|\mathbf{v}\| = |t| \, \|\mathbf{v}\|^2 \quad .$$

V případě $\mathbf{v} = t\mathbf{u}$ se rovnost odvodí podobně.

Předpokládejme, že $(\mathbf{u}, \mathbf{v})$ je lineárně nezávislá posloupnost a odvoďme ostrou nerovnost. Díky lineární nezávislosti pro libovolné $t \in \mathbb{C}$ platí

$$0 < \|\mathbf{u} - t\mathbf{v}\|^2 \quad .$$

Zvolíme $t \in \mathbb{C}$ tak, aby platilo $\langle \mathbf{v} \, | \mathbf{u} - t\mathbf{v} \rangle = 0$. Geometrický význam v případě standardního skalárního součinu v $\mathbb{R}^n$ je vyznačen na obrázku: vektor $t\mathbf{v}$ je ortogonální projekcí vektoru $\mathbf{u}$ na $\langle \mathbf{v} \rangle$. Později dáme této intuici přesný význam pro obecný skalární součin.



Obrázek 16. K důkazu Cauchy-Schwarzovy nerovnosti

Vztah $\langle \mathbf{v} \, | \mathbf{u} - t\mathbf{v} \rangle = 0$ je ekvivalentní $\langle \mathbf{v} \, | \mathbf{u} \rangle - t \, \langle \mathbf{v} \, | \mathbf{v} \rangle = 0$, což je ekvivalentní

$$t = \frac{\langle \mathbf{v} \, | \mathbf{u} \rangle}{\|\mathbf{v}\|^2} \quad .$$

(Nulou nedělíme, protože vektor je $\mathbf{v}$ je nenulový podle předpokladu o lineární nezávislosti $(\mathbf{u}, \mathbf{v})$.)

Při této volbě t dostáváme

$$0 < \|\mathbf{u} - t\mathbf{v}\|^2 = \langle \mathbf{u} - t\mathbf{v} \,|\mathbf{u} - t\mathbf{v}\rangle = \langle \mathbf{u} \,|\mathbf{u} - t\mathbf{v}\rangle - \bar{t}\,\langle \mathbf{v} \,|\mathbf{u} - t\mathbf{v}\rangle = \langle \mathbf{u} \,|\mathbf{u} - t\mathbf{v}\rangle$$
$$= \langle \mathbf{u} \,|\mathbf{u}\rangle - t\,\langle \mathbf{u} \,|\mathbf{v}\rangle = \|\mathbf{u}\|^2 - \frac{\langle \mathbf{v} \,|\mathbf{u}\rangle}{\|\mathbf{v}\|^2}\,\langle \mathbf{u} \,|\mathbf{v}\rangle = \|\mathbf{u}\|^2 - \frac{\overline{\langle \mathbf{u} \,|\mathbf{v}\rangle}\,\langle \mathbf{u} \,|\mathbf{v}\rangle}{\|\mathbf{v}\|^2} = \|\mathbf{u}\|^2 - \frac{|\,\langle \mathbf{u} \,|\mathbf{v}\rangle\,|^2}{\|\mathbf{v}\|^2}$$

Po vynásobení $\|\mathbf{v}\|^2$, drobné úpravě a odmocnění (oba výrazy, z nichž se počítá druhá mocnina jsou kladné) vyjde dokazovaná nerovnost:

$$0 < \|\mathbf{u}\|^2 - \frac{|\,\langle \mathbf{u} \,|\mathbf{v}\rangle\,|^2}{\|\mathbf{v}\|^2}$$
$$0 < \|\mathbf{u}\|^2 \|\mathbf{v}\|^2 - |\,\langle \mathbf{u} \,|\mathbf{v}\rangle\,|^2$$
$$|\,\langle \mathbf{u} \,|\mathbf{v}\rangle\,|^2 < \|\mathbf{u}\|^2 \|\mathbf{v}\|^2$$
$$|\,\langle \mathbf{u} \,|\mathbf{v}\rangle\,| < \|\mathbf{u}\|\,\|\mathbf{v}\|$$

□

Příklad 8.9. Pro standardní skalární součin v $\mathbb{C}^n$ říká Cauchy-Schwarzova nerovnost

$$|\overline{x_1}y_1 + \overline{x_2}y_2 + \cdots + \overline{x_n}y_n| \le \sqrt{|x_1|^2 + |x_2|^2 + \cdots + |x_n|^2}\sqrt{|y_1|^2 + |y_2|^2 + \cdots + |y_n|^2}\ .$$

V případě skalárního součinu na $\mathbb{C}^2$ daného vzorcem

$$\left\langle (x_1, x_2)^T \,\middle|\, (y_1, y_2)^T \right\rangle = 5\overline{x_1}y_1 - 2\overline{x_1}y_2 - 2\overline{x_2}y_1 + \overline{x_2}y_2$$

dostáváme

$$|5\overline{x_1}y_1 - 2\overline{x_1}y_2 - 2\overline{x_2}y_1 + \overline{x_2}y_2|$$
$$\le \sqrt{5|x_1|^2 - 4\mathrm{Re}(\overline{x_1}x_2) + |x_2|^2}\sqrt{5|y_1|^2 - 4\mathrm{Re}(\overline{y_1}y_2) + |y_2|^2}\ .$$

Pro prostor spojitých komplexních funkcí na intervalu $\langle 1, 10\rangle$ se skalárním součinem $\langle f \,|g\rangle = \int_1^{10} fg$ je nerovnost

$$\left|\int_1^{10} \overline{f}g\right| \le \sqrt{\int_1^{10} |f|^2}\sqrt{\int_1^{10} |g|^2}$$

Důležitým důsledkem Cauchy-Schwarzovy nerovnosti je trojúhelníková nerovnost.

Důsledek 8.10 (Trojúhelníková nerovnost)**.** *Nechť V je prostor se skalárním součinem $\langle\,|\,\rangle$ a $\mathbf{u}, \mathbf{v} \in V$. Pak platí*

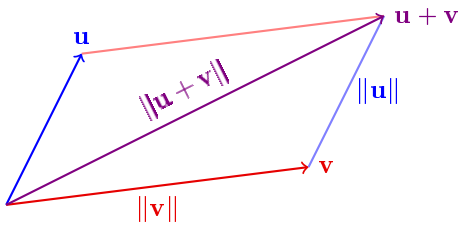
$$\|\mathbf{u} + \mathbf{v}\| \le \|\mathbf{u}\| + \|\mathbf{v}\|\ .$$

Důkaz.

$$\|\mathbf{u} + \mathbf{v}\|^2 = \langle \mathbf{u} + \mathbf{v} \,|\mathbf{u} + \mathbf{v}\rangle = \langle \mathbf{u} \,|\mathbf{u}\rangle + \langle \mathbf{u} \,|\mathbf{v}\rangle + \overline{\langle \mathbf{u} \,|\mathbf{v}\rangle} + \langle \mathbf{v} \,|\mathbf{v}\rangle$$
$$= \|\mathbf{u}\|^2 + 2\mathrm{Re}(\langle \mathbf{u} \,|\mathbf{v}\rangle) + \|\mathbf{v}\|^2 \le \|\mathbf{u}\|^2 + 2|\,\langle \mathbf{u} \,|\mathbf{v}\rangle\,| + \|\mathbf{v}\|^2$$
$$\le \|\mathbf{u}\|^2 + 2\,\|\mathbf{u}\|\,\|\mathbf{v}\| + \|\mathbf{v}\|^2 = (\|\mathbf{u}\| + \|\mathbf{v}\|)^2$$

Cauchy-Schwarzovu nerovnost jsme použili v předposlední úpravě. Výrazy pod druhými mocninami jsou kladné, takže nerovnost plyne odmocněním. □

Geometrický význam je patrný z obrázku.



Obrázek 17. Trojúhelníková nerovnost

Zobrazení, které vektoru přiřadí skalár, které splňuje podmínky (1) a (2) z tvrzení 8.7 a trojúhelníkovou nerovnost, se nazývá norma. Existuje mnoho norem, které nepochází ze skalárního součinu, například v $\mathbb{R}^n$ máme normu $\|(x_1, x_2, \dots, x_n)\| = |x_1| + |x_2| + \cdots + |x_n|$, která měří vzdálenost, když se můžeme pohybovat pouze pravoúhlým směrem (proto se jí někdy říká manhattanská norma). Norma pochází ze skalárního součinu právě tehdy, když splňuje rovnoběžníkové pravidlo, viz cvičení.

Cauchy-Schwarzova nerovnost nám umožňuje definovat úhel mezi vektory. Úhel definujeme v případě reálných vektorových prostorů.

Definice 8.11. Nechť V je prostor nad $\mathbb{R}$ se skalárním součinem $\langle\,|\,\rangle$ a $\mathbf{o} \neq \mathbf{u}, \mathbf{v} \in V$. *Úhlem mezi vektory* $\mathbf{u}$ *a* $\mathbf{v}$ rozumíme reálné číslo $\alpha \in \langle 0, \pi\rangle$ splňující

$$\cos\alpha = \frac{\langle \mathbf{u}\,|\,\mathbf{v}\rangle}{\|\mathbf{u}\|\,\|\mathbf{v}\|}$$

Úhel mezi vektory existuje a je určen jednoznačně, protože zlomek je v intervalu $\langle -1, 1\rangle$ podle Cauchy-Schwarzovo nerovnosti a funkce cos je bijekcí $\langle 0, \pi\rangle$ na interval $\langle -1, 1\rangle$.

Pro libovolný skalární součin nad reálnými čísly tedy máme vztah

$$\langle \mathbf{u}\,|\,\mathbf{v}\rangle = \|\mathbf{u}\|\,\|\mathbf{v}\|\cos\alpha \quad .$$

Z tohoto vztahu snadno odvodíme kosinovou větu.

Tvrzení 8.12 (Kosinová věta)**.** *Nechť V je prostor nad $\mathbb{R}$ se skalárním součinem $\langle\,|\,\rangle$ a $\mathbf{o} \neq \mathbf{u}, \mathbf{v} \in V$. Pak platí*

$$\|\mathbf{u} - \mathbf{v}\|^2 = \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 - 2\,\|\mathbf{u}\|\,\|\mathbf{v}\|\cos\alpha \quad ,$$

kde α je úhel mezi vektory $\mathbf{u}$ a $\mathbf{v}$.

Důkaz.

$$\begin{aligned}\|\mathbf{u} - \mathbf{v}\|^2 &= \langle \mathbf{u} - \mathbf{v}\,|\,\mathbf{u} - \mathbf{v}\rangle = \langle \mathbf{u}\,|\,\mathbf{u}\rangle - 2\,\langle \mathbf{u}\,|\,\mathbf{v}\rangle + \langle \mathbf{v}\,|\,\mathbf{v}\rangle \\ &= \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 - 2\,\|\mathbf{u}\|\,\|\mathbf{v}\|\cos\alpha\end{aligned}$$

□

Nad komplexními čísly se úhel definuje jako číslo z intervalu $\langle 0, \pi/2\rangle$ splňující $\cos\alpha = \frac{|\langle \mathbf{u}|\mathbf{v}\rangle|}{\|\mathbf{u}\|\|\mathbf{v}\|}$, ale tento pojem nebudeme používat.

8.3. **Kolmost.**

Ze vztahu $\langle \mathbf{u}\,|\,\mathbf{v}\rangle = \|\mathbf{u}\|\,\|\mathbf{v}\|\cos\alpha$ vidíme, že (nenulové) vektory svírají úhel $\pi/2$ právě tehdy, když je jejich skalární součin nula. To vede k přirozené definici kolmosti vektorů.

Definice 8.13. Nechť V je prostor se skalárním součinem $\langle\,|\,\rangle$. Vektory $\mathbf{u}, \mathbf{v} \in V$ nazýváme *kolmé* (nebo *ortogonální*) a píšeme $\mathbf{u} \perp \mathbf{v}$, pokud $\langle \mathbf{u}\,|\,\mathbf{v}\rangle = 0$.

Množina, nebo posloupnost, M vektorů z V se nazývá *ortogonální*, pokud $\mathbf{u} \perp \mathbf{v}$ pro libovolné dva různé prvky množiny (nebo posloupnosti) M.

Množina (posloupnost) M se nazývá *ortonormální*, pokud je ortogonální a každý vektor v M je jednotkový.

Z vlastnosti (SCS) plyne, že ortogonalita nezávisí na pořadí vektorů. Z vlastnosti (SL1) vidíme, že jsou-li dva vektory kolmé, pak jsou kolmé i jejich libovolné násobky. Máme-li ortogonální množinu nenulových vektorů $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k\}$, můžeme z ní vytvořit ortonormální množinu znormováním, tj.

$$\left\{\frac{\mathbf{v}_1}{\|\mathbf{v}_1\|}, \frac{\mathbf{v}_2}{\|\mathbf{v}_2\|}, \dots, \frac{\mathbf{v}_k}{\|\mathbf{v}_k\|}\right\}$$

je ortonormální.

Z geometrického náhledu v $\mathbb{R}^3$ vidíme, že ortogonální posloupnost nenulových vektorů je lineárně nezávislá. Obecně:

Tvrzení 8.14. *Nechť V je prostor se skalárním součinem $\langle\,|\,\rangle$. Ortogonální posloupnost nenulových vektorů z V je lineárně nezávislá.*

Důkaz. Je-li $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k)$ ortogonální posloupnost vektorů z V a platí

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k = \mathbf{o} \quad ,$$

pak skalárním vynásobením obou stran zleva vektorem $\mathbf{v}_i$ ($i \in \{1, 2, \dots, k\}$) a využitím (SL1), (SL2) a kolmosti dostáváme

$$\begin{aligned} \langle \mathbf{v}_i \,|a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k \rangle &= \langle \mathbf{o} \,|\mathbf{v} \rangle \\ a_1 \langle \mathbf{v}_i \,|\mathbf{v}_1 \rangle + a_2 \langle \mathbf{v}_i \,|\mathbf{v}_2 \rangle + \cdots + a_k \langle \mathbf{v}_i \,|\mathbf{v}_k \rangle &= 0 \\ a_i \langle \mathbf{v}_i \,|\mathbf{v}_i \rangle &= 0 \ . \end{aligned}$$

Protože vektor $\mathbf{v}_i$ je nenulový, platí podle (SP) vztah $\langle \mathbf{v}_i \,|\mathbf{v}_i \rangle = \|\mathbf{v}_i\|^2 > 0$, takže z odvozeného vztahu vyplývá $a_i = 0$. Ukázali jsme, že jediná lineární kombinace, která dává nulový vektor, je triviální, takže posloupnost je lineárně nezávislá (viz bod (2) tvrzení 5.26). □

Z tvrzení vyplývá, že ortogonální posloupnost n nenulových vektorů v prostoru dimenze n je ortogonální báze, protože je lineárně nezávislá a lineárně nezávislá posloupnost n vektorů je báze podle bodu (4) v pozorování 5.57

Příklad 8.15. V prostoru $\mathbb{R}^n$ (nebo $\mathbb{C}^n$) se standardním skalárním součinem je kanonická báze ortonormální.

Posloupnost vektorů $((1,2,2)^T, (-2,-1,2)^T)$ v $\mathbb{R}^3$ (nebo $\mathbb{C}^3$) je ortogonální, ale není ortonormální. Znormováním dostaneme ortonormální posloupnost

$$\left(\frac{1}{3}(1,2,2)^T, \frac{1}{3}(-2,-1,2)^T\right) \ .$$

Tuto posloupnost lze doplnit na ortonormální bázi: posloupnost

$$\left(\frac{1}{3}(1,2,2)^T, \frac{1}{3}(-2,-1,2)^T, \frac{1}{3}(2,-2,1)\right)$$

je ortonormální, takže je to podle poznámky za tvrzením ortonormální báze. Později budeme pomocí Gram-Schmidtova ortogonalizačního procesu umět každou ortogonální (resp. ortonormální) posloupnost nenulových vektorů v konečně generovaném prostoru doplnit do ortogonální (resp. ortonormální) báze.

Příklad 8.16. V prostoru $\mathbb{R}^2$ se skalárním součinem daným

$$\langle (x_1,x_2)^T \,|(y_1,y_2) \rangle = (x_1,x_2) \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = 2x_1y_1 + x_1y_2 + x_2y_1 + x_2y_2$$

(ověřte, že je to skutečně skalární součin) je posloupnost

$$\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 2 \end{pmatrix} \right)$$

ortogonální, protože

$$\langle (1,0)^T \,|(-1,2)^T \rangle = (1,0) \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} -1 \\ 2 \end{pmatrix} = (2,1) \begin{pmatrix} -1 \\ 2 \end{pmatrix} = 0 \ ,$$

tedy tvoří ortogonální bázi. Spočítáme normy vektorů a vytvoříme ortonormální bázi.

$$\left\| \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\| = \sqrt{(1,0) \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}} = \sqrt{(2,1) \begin{pmatrix} 1 \\ 0 \end{pmatrix}} = \sqrt{2}$$

$$\left\| \begin{pmatrix} -1 \\ 2 \end{pmatrix} \right\| = \sqrt{(-1,2) \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} -1 \\ 2 \end{pmatrix}} = \sqrt{(0,1) \begin{pmatrix} -1 \\ 2 \end{pmatrix}} = \sqrt{2}$$

Posloupnost

$$\left(\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ 2 \end{pmatrix} \right)$$

je tedy ortonormální báze.

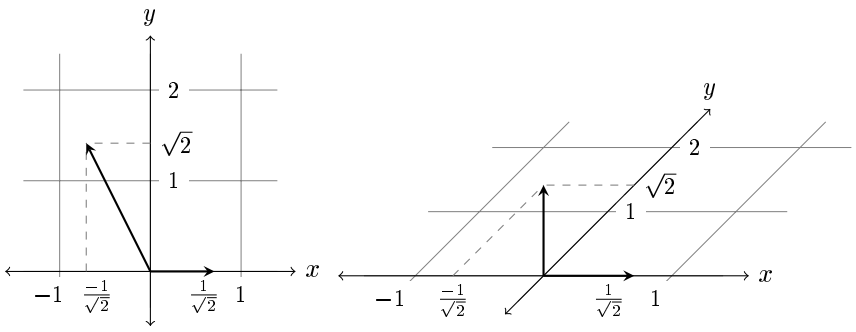
Pokud si nakreslíme tyto dva vektory jako kolmé vektory jednotkové velikosti a ostatní vektory kreslíme v tomto souřadném systému, pak délky a úhly při daném skalárním součinu jsou běžné, eukleidovské délky a úhly na obrázku. Tento fakt dokážeme v tvrzení 8.21.

Příklad 8.17. V prostoru spojitých funkcí na intervalu $\langle -\pi, \pi \rangle$ se skalárním součinem

$$\langle f \,|g \rangle = \int_{-\pi}^{\pi} fg$$

je množina $\{1, \sin x, \cos x, \sin(2x), \cos(2x), \dots\}$ ortogonální. Toto je základní fakt v oboru Fourierových řad.

Jednoduchým důsledkem definice kolmosti je zobecnění Pythagorovy věty pro libovolný skalární součin:



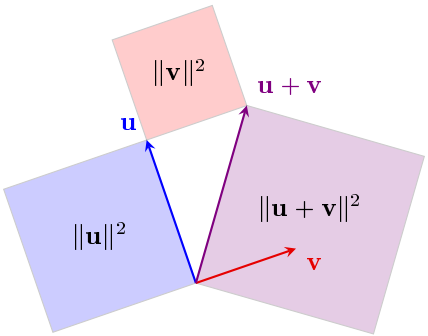
Tvrzení 8.18 (Pythagorova věta)**.** *Nechť V je prostor se skalárním součinem $\langle\,|\,\rangle$. Jsou-li vektory $\mathbf{u},\mathbf{v}\in V$ kolmé, pak*

$$\|\mathbf{u}+\mathbf{v}\|^2=\|\mathbf{u}\|^2+\|\mathbf{v}\|^2\quad.$$

Důkaz.

$$\|\mathbf{u}+\mathbf{v}\|^2=\langle\mathbf{u}+\mathbf{v}\,|\mathbf{u}+\mathbf{v}\rangle=\langle\mathbf{u}\,|\mathbf{u}\rangle+\langle\mathbf{u}\,|\mathbf{v}\rangle+\langle\mathbf{v}\,|\mathbf{u}\rangle+\langle\mathbf{v}\,|\mathbf{v}\rangle$$

Díky kolmosti jsou prostřední dva členy nulové, takže výraz je roven $\|\mathbf{u}\|^2+\|\mathbf{v}\|^2$. □



Indukcí lze Pythagorovu větu zobecnit na libovolný konečný počet vektorů: Je-li $\{\mathbf{v}_1,\mathbf{v}_2,\dots,\mathbf{v}_k\}$ ortogonální množina, pak

$$\|\mathbf{v}_1+\mathbf{v}_2+\cdots+\mathbf{v}_k\|^2=\|\mathbf{v}_1\|^2+\|\mathbf{v}_1\|^2+\cdots+\|\mathbf{v}_k\|^2\quad.$$

Zobecnění této rovnosti na nekonečné množiny vektorů se někdy říká *Parsevalova identita*.

8.3.1. *Souřadnice vektoru vzhledem k ortonormální bázi.* Vzhledem k ortonormální bázi se souřadnice vektoru počítají velmi snadno:

Tvrzení 8.19. *Nechť V je prostor se skalárním součinem $\langle\,|\,\rangle$, $B=(\mathbf{v}_1,\dots,\mathbf{v}_n)$ jeho ortonormální báze a $\mathbf{u}\in V$. Pak*

$$\mathbf{u}=\langle\mathbf{v}_1\,|\mathbf{u}\rangle\,\mathbf{v}_1+\langle\mathbf{v}_2\,|\mathbf{u}\rangle\,\mathbf{v}_2+\cdots+\langle\mathbf{v}_n\,|\mathbf{u}\rangle\,\mathbf{v}_n\quad,$$

jinými slovy,

$$[\mathbf{u}]_B=(\langle\mathbf{v}_1\,|\mathbf{u}\rangle,\langle\mathbf{v}_2\,|\mathbf{u}\rangle,\dots,\langle\mathbf{v}_n\,|\mathbf{u}\rangle)^T\quad.$$

Důkaz. Označme $[\mathbf{u}]_B=(a_1,a_2,\dots,a_n)^T$, neboli

$$\mathbf{u}=a_1\mathbf{v}_1+a_2\mathbf{v}_2+\cdots+a_n\mathbf{v}_n\quad.$$

Podobně jako v důkazu lineární nezávislosti ortogonální množiny nenulových vektorů skalárně vynásobíme obě strany zleva vektorem $\mathbf{v}_i$ a dostaneme

$$\begin{aligned}\langle\mathbf{v}_i\,|\mathbf{u}\rangle&=\langle\mathbf{v}_i\,|a_1\mathbf{v}_1+a_2\mathbf{v}_2+\cdots+a_k\mathbf{v}_k\rangle\\ \langle\mathbf{v}_i\,|\mathbf{u}\rangle&=a_1\langle\mathbf{v}_i\,|\mathbf{v}_1\rangle+a_2\langle\mathbf{v}_i\,|\mathbf{v}_2\rangle+\cdots+a_k\langle\mathbf{v}_i\,|\mathbf{v}_k\rangle\\ \langle\mathbf{v}_i\,|\mathbf{u}\rangle&=a_i\langle\mathbf{v}_i\,|\mathbf{v}_i\rangle=a_i\quad,\end{aligned}$$

takže $a_i=\langle\mathbf{v}_i\,|\mathbf{u}\rangle$. □

Souřadnicím vzhledem k ortonormální bázi se někdy říká *Fourierovy koeficienty* vzhledem k této bázi. Obecněji z důkazu vidíme, že pro ortogonální B platí

$$[\mathbf{u}]_B = \left(\frac{\langle \mathbf{v}_1 \,|\mathbf{u}\rangle}{\|\mathbf{v}_1\|^2}, \frac{\langle \mathbf{v}_2 \,|\mathbf{u}\rangle}{\|\mathbf{v}_2\|^2}, \dots, \frac{\langle \mathbf{v}_n \,|\mathbf{u}\rangle}{\|\mathbf{v}_n\|^2} \right)^T$$

Příklad 8.20. Určíme souřadnice vektoru $\mathbf{u} = (3+i, 2, i)^T \in \mathbb{C}^3$ vzhledem k ortonormální bázi

$$B = (\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) = \left(\frac{1}{3} \begin{pmatrix} i \\ 2i \\ 2i \end{pmatrix}, \frac{1}{3} \begin{pmatrix} -2 \\ -1 \\ 2 \end{pmatrix}, \frac{1}{3} \begin{pmatrix} 2 \\ -2 \\ 1 \end{pmatrix} \right)$$

prostoru $\mathbb{C}^3$ se standardním skalárním skalárním součinem.

$$\begin{aligned} [\mathbf{u}]_B &= (\mathbf{v}_1^* \cdot \mathbf{u}, \mathbf{v}_2^* \cdot \mathbf{u}, \mathbf{v}_3^* \cdot \mathbf{u})^T \\ &= \left(\frac{1}{3}(-i, -2i, -2i) \begin{pmatrix} 3+i \\ 2 \\ i \end{pmatrix}, \frac{1}{3}(-2, -1, 2) \begin{pmatrix} 3+i \\ 2 \\ i \end{pmatrix}, \right. \\ &\qquad \left. \frac{1}{3}(2, -2, 1) \begin{pmatrix} 3+i \\ 2 \\ i \end{pmatrix} \right)^T \\ &= \left(\frac{1}{3}(3-7i), -\frac{8}{3}, \frac{1}{3}(2+3i) \right)^T \quad . \end{aligned}$$

Skutečně

$$\begin{pmatrix} 3+i \\ 2 \\ i \end{pmatrix} = \frac{1}{3}(3-7i) \cdot \frac{1}{3} \begin{pmatrix} i \\ 2i \\ 2i \end{pmatrix} - \frac{8}{3} \cdot \frac{1}{3} \begin{pmatrix} -2 \\ -1 \\ 2 \end{pmatrix} + \frac{1}{3}(2+3i) \cdot \frac{1}{3} \begin{pmatrix} 2 \\ -2 \\ 1 \end{pmatrix} \quad .$$

Vzhledem k ortonormální bázi přechází skalární součin na standardní. Přesněji, skalární součin dvou vektorů je roven standardnímu skalárnímu součinu souřadnic těchto vektorů vzhledem k ortonormální bázi.

Tvrzení 8.21. *Nechť V je prostor se skalárním součinem $\langle\,|\,\rangle$, $B = (\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$ jeho ortonormální báze a $\mathbf{u}, \mathbf{w} \in V$. Pak*

$$\langle \mathbf{u} \,|\mathbf{w}\rangle = [\mathbf{u}]_B^* [\mathbf{w}]_B \quad .$$

Důkaz. Označme $[\mathbf{u}]_B = (a_1, a_2, \dots, a_n)^T$, $[\mathbf{w}]_B = (b_1, b_2, \dots, b_n)^T$, tedy

$$\mathbf{u} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n, \quad \mathbf{w} = b_1\mathbf{v}_1 + b_2\mathbf{v}_2 + \cdots + b_n\mathbf{v}_n \quad .$$

Pomocí (SL2), (SL1) a ortonormality postupně dostáváme

$$\begin{aligned} \langle \mathbf{u} \,|\mathbf{w}\rangle &= \left\langle \sum_{i=1}^n a_i\mathbf{v}_i \,\middle|\, \sum_{j=1}^n b_i\mathbf{v}_i \right\rangle = \sum_{i=1}^n \sum_{j=1}^n \langle a_i\mathbf{v}_i \,|b_j\mathbf{v}_j\rangle \\ &= \sum_{i=1}^n \sum_{j=1}^n a_i^* b_j \langle \mathbf{v}_i \,|\mathbf{v}_j\rangle = \sum_{i=1}^n a_i^* b_i = [\mathbf{u}]_B^* [\mathbf{w}]_B \end{aligned}$$

□

Tvrzení ospravedlňuje poznámku z příkladu 8.16: Pokud si nakreslíme vektory ortonormální báze jako jednotkové navzájem kolmé vektory a ostatní vektory kreslíme v tomto souřadném systému, pak délky a úhly při daném skalárním součinu jsou běžné, eukleidovské délky a úhly na obrázku.

Příklad 8.22. V prostoru $\mathbb{R}^2$ se skalárním součinem

$$\left\langle (x_1, x_2)^T \,|(y_1, y_2)\right\rangle^T = (x_1, x_2) \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = 2x_1y_1 + x_1y_2 + x_2y_1 + x_2y_2$$

je posloupnost

$$B = \left(\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ 2 \end{pmatrix} \right)$$

ortonormální báze (viz příklad 8.16. Uvažujme vektory $\mathbf{u} = (2,3)^T$ a $\mathbf{v} = (1,1)^T$. Z tvrzení 8.19 spočteme jejich souřadnice vzhledem k B a pak vypočítáme skalární součin podle tvrzení 8.21.

$$[\mathbf{u}]_B = \left(\left\langle \mathbf{u} \middle| \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\rangle, \left\langle \mathbf{u} \middle| \frac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ 2 \end{pmatrix} \right\rangle \right)^T = \frac{1}{\sqrt{2}} \begin{pmatrix} 7 \\ 3 \end{pmatrix}$$

$$[\mathbf{v}]_B = \left(\left\langle \mathbf{v} \middle| \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\rangle, \left\langle \mathbf{v} \middle| \frac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ 2 \end{pmatrix} \right\rangle \right)^T = \frac{1}{\sqrt{2}} \begin{pmatrix} 3 \\ 1 \end{pmatrix}$$

$$\langle \mathbf{u} \,|\mathbf{v} \rangle = [\mathbf{u}]_B \cdot [\mathbf{v}]_B = \frac{1}{\sqrt{2}}(7,3) \frac{1}{\sqrt{2}} \begin{pmatrix} 3 \\ 1 \end{pmatrix} = 12$$

To můžeme ověřit z definice skalárního součinu.

8.3.2. *Ortogonální doplněk.* Definici kolmosti rozšíříme na množiny vektorů.

Definice 8.23. Nechť V je prostor se skalárním součinem $\langle\,|\,\rangle$ a $\mathbf{v} \in V$, $M, N \subseteq V$. Říkáme, že $\mathbf{v}$ je kolmý na M, zapisujeme $\mathbf{v} \perp M$, pokud $\mathbf{v}$ je kolmý na každý vektor z množiny M.

Říkáme, že M je kolmá na N, zapisujeme $M \perp N$, pokud každý vektor množiny M je kolmý na každý vektor množiny N.

Pokud M je kolmá na N, pak v jejich průniku může být pouze nulový vektor (rozmyslete si jako cvičení). Například tabule není kolmá na podlahu, i když svírají úhel $\pi/2$ (úhel mezi podprostory definujeme později jako největší úhel, který svírají vektory jednotlivých podprostorů). Kolmost se přenáší na lineární obal:

Pozorování 8.24. *Nechť V je prostor se skalárním součinem $\langle\,|\,\rangle$ a $M, N \subseteq V$. Pokud $M \perp N$, pak $\langle M \rangle \perp \langle N \rangle$.*

Důkaz. Pokud $\mathbf{u} = \sum_{i=1}^{k} a_i \mathbf{u}_i$, kde a_i jsou skaláry a $\mathbf{u}_i \in M$, a $\mathbf{v} = \sum_{j=1}^{l} b_j \mathbf{v}_j$, kde b_j jsou skaláry a $\mathbf{v}_j \in N$, pak z linearity, tj. z vlastností (SL1) a (SL2), máme

$$\langle \mathbf{u} \,|\mathbf{v} \rangle = \left\langle \sum_{i=1}^{k} a_i \mathbf{u}_i \middle| \sum_{j=1}^{l} b_j \mathbf{v}_j \right\rangle = \sum_{i=1}^{k} \sum_{j=1}^{l} \overline{a_i} b_j \langle \mathbf{v}_i \,|\mathbf{v}_j \rangle = 0 \ .$$

□

Největší množina vektorů kolmá na danou množinu M se nazývá ortogonální doplněk.

Definice 8.25. Nechť V je prostor se skalárním součinem $\langle\,|\,\rangle$ a $M \subseteq V$. *Ortogonální doplňkem* množiny M rozumíme množinu všech vektorů kolmých na každý vektor z M, značíme $M^\perp$:

$$M^\perp = \{\mathbf{v} \in V : \mathbf{v} \perp M\} \ .$$

Podle definice M je kolmá na $M^\perp$ a $M^\perp$ je největší taková množina. Další jednoduché vlastnosti:

Pozorování 8.26. *Nechť V je prostor se skalárním součinem $\langle\,|\,\rangle$ a $M, N \subseteq V$. Pak platí*

(1) *$M^\perp$ je podprostor V,*
(2) *Je-li $M \subseteq N$, pak $N^\perp \subseteq M^\perp$,*
(3) *$M^\perp = \langle M \rangle^\perp$,*

Důkaz. Důkaz se provede snadno z definic a předchozího pozorování. Přenecháme jej do cvičení. □

V $\mathbb{R}^3$ se standardním skalárním součinem je ortogonální doplněk množiny $M = \{\mathbf{u}, \mathbf{v}\}$ dvou lineárně nezávislých vektorů přímka kolmá na rovinu $\langle \mathbf{u}, \mathbf{v} \rangle$. Ortogonálním doplňkem nenulového vektoru (nebo jeho lineárního obalu) je rovina.

Příklad 8.27. Určíme ortogonální doplněk roviny $U = \langle (1,2,5)^T, (0,1,1)^T) \rangle$ v prostoru $\mathbb{R}^3$ se standardním skalárním součinem. Podle (3) je $U^\perp$ rovná množině všech vektorů $\mathbf{x}$ kolmých na oba generátory, tj. množině vektorů, pro které $(1,2,5)\mathbf{x} = 0$ a $(0,1,1)\mathbf{x} = 0$. Maticově

$$\begin{pmatrix} 1 & 2 & 5 \\ 0 & 1 & 1 \end{pmatrix} \mathbf{x} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Hledáme tedy řešení homogenní soustavy s maticí, jejíž řádkové vektory jsou generátory U:

$$U^\perp = \operatorname{Ker} \begin{pmatrix} 1 & 2 & 5 \\ 0 & 1 & 1 \end{pmatrix} = \left\langle \begin{pmatrix} -3 \\ -1 \\ 1 \end{pmatrix} \right\rangle$$

V příkladu jsme viděli, že k určení ortogonálního doplňku množiny vektorů $M = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k\}$ (nebo podprostoru $\langle M \rangle$) v aritmetickém vektorovém prostoru $\mathbb{R}^n$ se standardním skalárním součinem stačí napsat vektory $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k$ do řádků matice a vyřešit příslušnou homogenní soustavu. Při standardním skalárním součinu tedy platí

$$(\operatorname{Im} A^T)^\perp = \operatorname{Ker} A \ .$$

To nám dává nad $\mathbb{R}$ další interpretaci řešení homogenní soustavy rovnic $A\mathbf{x} = \mathbf{o}$ – určujeme ortogonální doplněk řádků matice A. V $\mathbb{C}^n$ se standardním skalárním součinem je ještě třeba přidat komplexní sdružování:

$$(\operatorname{Im} A^*)^\perp = \operatorname{Ker} A \ .$$

Obecněji, počítáme-li vzhledem k ortonormální bázi, pak skalární součin se chová jako standardní (viz tvrzení 8.21), takže ortogonální doplněk množiny vektorů můžeme spočítat podobně:

Pozorování 8.28. *Nechť V je konečně generovaný prostor se skalárním součinem $\langle\,|\,\rangle$, B jeho ortonormální báze, $M = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k\}$. Označme A matici s řádky $[\mathbf{v}_1]_B^*$, $[\mathbf{v}_2]_B^*$, …, $[\mathbf{v}_k]_B^*$. Pak*

$$[M^\perp]_B = \operatorname{Ker} A \ .$$

Důkaz.

$$\begin{aligned}[M^\perp]_B &= \{[\mathbf{u}]_B : \mathbf{u} \perp M\} = \{[\mathbf{u}]_B : \langle \mathbf{v}_1 \,|\mathbf{u}\rangle = \langle \mathbf{v}_2 \,|\mathbf{u}\rangle = \cdots = \langle \mathbf{v}_k \,|\mathbf{u}\rangle = 0\} \\ &= \{[\mathbf{u}]_B : [\mathbf{v}_1]_B^*[\mathbf{u}]_B = [\mathbf{v}_2]_B^*[\mathbf{u}]_B = \cdots = [\mathbf{v}_k]_B^*[\mathbf{u}]_B = 0\} \\ &= \{\mathbf{x} : A\mathbf{x} = \mathbf{o}\} = \operatorname{Ker} A\end{aligned}$$

□

Důležité netriviální vlastnosti ortogonálního doplňku jsou shrnuty v následující větě.

Věta 8.29. *Nechť V je konečně generovaný prostor dimenze n se skalárním součinem $\langle\,|\,\rangle$ a W je podprostor V. Pak platí*

(1) $\dim(W^\perp) = n - \dim(W)$,
(2) $V = W \oplus W^\perp$,
(3) $(W^\perp)^\perp = W$.

Důkaz. V důkazu použijeme skutečnost, která bude dokázána teprve později ve větě 8.44, a to, že každý prostor konečné dimenze má nějakou ortonormální bázi B.

Zvolme nějakou bázi $(\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_k)$ prostoru W, tj. $\dim(W) = k$.

(1) Označme A matici s řádky $[\mathbf{w}_1]_B$, $[\mathbf{w}_2]_B$, …, $[\mathbf{w}_k]_B$. Ortogonální doplněk prostoru W vyjádřený v bázi B je podle pozorování 8.28 jádrem matice $\overline{A}$. Matice má k lineárně nezávislých řádků, takže $\operatorname{rank}(\overline{A}) = \operatorname{rank}(A) = k$. Podle věty 5.83 o dimenzi jádra a obrazu máme $\dim(\operatorname{Ker} A) = n - k$.

(2) Protože podprostor W je kolmý na $W^\perp$, jejich průnikem je triviální podprostor $\{\mathbf{o}\}$. Podle věty 5.87 o dimenzi součtu a průniku máme

$$\dim(W + W^\perp) = \dim(W) + \dim(W^\perp) - \dim(W \cap W^\perp) = k + n - k - 0 = n \ .$$

Podprostor dimenze n v prostoru dimenze n je celý prostor (tvrzení 5.59), takže $W + W^\perp = V$.

(3) Podprostor W je kolmý na $W^\perp$, takže W je podprostorem $(W^\perp)^\perp$. Podle (1) máme $\dim(W^\perp) = n - k$ a $\dim((W^\perp)^\perp) = n - (n - k) = k$. Takže $W = (W^\perp)^\perp$ opět podle tvrzení 5.59.

□

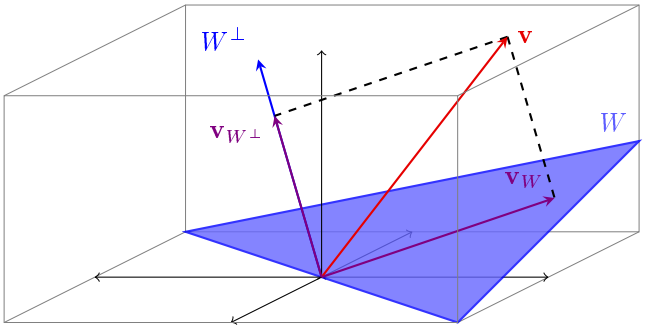
Každý vektor ve V lze podle (2) vyjádřit jednoznačně jako součet vektoru $\mathbf{v}_W$ ve W a vektoru $\mathbf{v}_{W^\perp}$ kolmého na W:

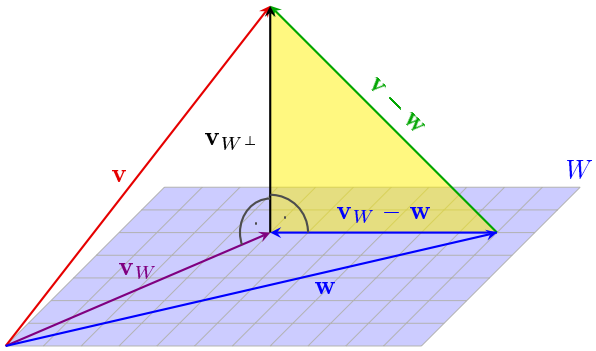
$$\mathbf{v} = \mathbf{v}_W + \mathbf{v}_{W^\perp}$$

Definice 8.30. Vektoru $\mathbf{v}_W$ říkáme *ortogonální projekce* vektoru $\mathbf{v}$ na W. Vektor $\mathbf{v}_{W^\perp}$ se nazývá *kolmice* vektoru $\mathbf{v}$ na W. (Kolmice je tedy ortogonální projekce $\mathbf{v}$ na $W^\perp$.)

Důsledkem Pythagorovy věty je, že vektor $\mathbf{v}_W$ je nejlepší aproximací vektoru $\mathbf{v}$ v prostoru W:

Tvrzení 8.31. *Nechť V je konečně generovaný prostor se skalárním součinem $\langle\,|\,\rangle$, W je podprostor V, $\mathbf{v} \in V$. Vektor $\mathbf{v} - \mathbf{v}_W$ ($=\mathbf{v}_{W^\perp}$) má nejmenší možnou normu ze všech vektorů $\mathbf{v} - \mathbf{w}$, $\mathbf{w} \in W$.*





Důkaz. Uvažujme libovolný vektor $\mathbf{w} \in W$, $\mathbf{w} \neq \mathbf{v}_W$. Napíšeme si vektor $\mathbf{v} - \mathbf{w}$ ve tvaru

$$\mathbf{v} - \mathbf{w} = (\mathbf{v} - \mathbf{v}_W) + (\mathbf{v}_W - \mathbf{w}) = \mathbf{v}_{W^\perp} + (\mathbf{v}_W - \mathbf{w}) \ .$$

Vektor $\mathbf{v}_{W^\perp}$ je kolmý na $\mathbf{v}_W - \mathbf{w}$ protože je kolmý na oba dva vektory $\mathbf{v}_W$ a $\mathbf{w}$. Podle Pythagorovy věty 8.18 je

$$\|\mathbf{v} - \mathbf{w}\|^2 = \|\mathbf{v}_{W^\perp}\|^2 + \|\mathbf{v}_W - \mathbf{w}\|^2 > \|\mathbf{v}_{W^\perp}\|^2 \ .$$

□

Předpoklad konečné generovanosti V v bodech (2), (3) věty 8.29 a v předchozím tvrzení lze nahradit slabším předpokladem, že W je konečně generovaný. To získáme jako důsledek Gram-Schmidtovy ortogonalizace, viz cvičení.

8.3.3. *Prostory určené maticí a kolmost.* Metody a aplikace hledání nejlepší aproximace budeme studovat v další části. Teď se ještě krátce podíváme na vztahy prostorů určených maticí z hlediska kolmosti a geometricky interpretujeme izomorfismus $\operatorname{Im} A^T$ a $\operatorname{Im} A$.

Uvažujme standardní skalární součin nad reálnými čísly a reálnou matici A typu $m \times n$.

Všimli jsme si, že pro standardní skalární součin nad $\mathbb{R}$ máme $(\operatorname{Im} A^T)^\perp = \operatorname{Ker} A$. Podle bodů (3) a (2) z věty 8.29 také platí

$$(\operatorname{Ker} A)^\perp = \operatorname{Im} A^T \ , \quad \operatorname{Ker} A \oplus \operatorname{Im} A^T = \mathbf{T}^n \ ,$$

kde n je počet sloupců matice A.

Jádrem lineárního zobrazení $f_A : \mathbb{R}^n \to \mathbb{R}^m$ je $\operatorname{Ker} f_A = \operatorname{Ker} A$. Jeho zúžení na libovolný doplněk $\operatorname{Ker} A$, tj. libovolný podprostor $U \leq \mathbb{R}^n$ takový, že $\operatorname{Ker} A \oplus U = \mathbb{R}^n$ je izomorfismus $U \to \operatorname{Im} A$, viz cvičení. Pro ortogonální doplněk $\operatorname{Ker} A$, což je $\operatorname{Im} A^T$, máme izomorfismus $\operatorname{Im} A^T \to \operatorname{Im} A$. Z toho například vidíme, že prostory $\operatorname{Im} A^T$ a $\operatorname{Im} A$ mají stejnou dimenzi, takže získáváme v reálném případě další důkaz, že dimenze sloupcového a řádkového prostoru matice se shodují (věta 5.73).

Příklad 8.32. Pro matici

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

máme

$$\operatorname{Ker} f_A = \operatorname{Ker} A = \langle (-1, 5, 3)^T \rangle \, , \quad \operatorname{Im} A^T = \langle (1, 2, -3)^T, (1, -1, 2)^T \rangle \ .$$

Skutečně $\operatorname{Ker} A \perp \operatorname{Im} A^T$ a $\operatorname{Ker} A \oplus \operatorname{Im} A^T = \mathbb{R}^3$.

Zúžení f na $\operatorname{Im} A^T$ je izomorfismem rovin $\operatorname{Im} A^T$ a $\operatorname{Im} A = \langle (1, 1, 2)^T, (2, -1, 1)^T \rangle$.

OBRAZEK

Obdobně pro prostory $\operatorname{Im} A$ a $\operatorname{Ker} A^T$ máme vztahy.

$$(\operatorname{Im} A)^\perp = \operatorname{Ker} A^T, \quad (\operatorname{Ker} A^T)^\perp = \operatorname{Im} A, \quad \operatorname{Ker} A^T \oplus \operatorname{Im} A = \mathbf{T}^m \ ,$$

kde m je počet řádků matice A.

Nad komplexními čísly vychází stejné vztahy, jen je potřeba transponování nahradit komplexním sdružováním.

8.4. **Ortogonální projekce.**

V této části se naučíme hledat ortogonální projekci vektorů na podprostor. Ortogonální projekce je nejlepší aproximace vektoru v podprostoru, což také využijeme na hledání nejlepších přibližných řešení soustav lineárních rovnic.

8.4.1. *Ortogonální projekce na přímku.* Jednoduchým případem ortogonální projekce je projekce na přímku $W = \langle \mathbf{w} \rangle$, $\mathbf{w} \neq \{\mathbf{o}\}$. Projekce vektoru $\mathbf{v}$ je vektor $\mathbf{v}_W = a\mathbf{w}$, pro který je vektor $\mathbf{v}_{W^\perp} = \mathbf{v} - \mathbf{v}_W$ kolmý na $\mathbf{w}$. Z toho dostáváme

$$\begin{aligned} \langle \mathbf{w} \,|\mathbf{v} - a\mathbf{w} \rangle &= 0 \\ \langle \mathbf{w} \,|\mathbf{v} \rangle - a \langle \mathbf{w} \,|\mathbf{w} \rangle &= 0 \\ a &= \frac{\langle \mathbf{w} \,|\mathbf{v} \rangle}{\|\mathbf{w}\|^2} \ , \end{aligned}$$

takže ortogonální projekce vektoru $\mathbf{v}$ na W je

$$\mathbf{v}_W = \frac{\langle \mathbf{w} \,|\mathbf{v} \rangle}{\|\mathbf{w}\|^2} \mathbf{w} \ .$$

V případě, že je vektor $\mathbf{w}$ jednotkový, se vzorec zjednoduší na

$$\mathbf{v}_W = \langle \mathbf{w} \,|\mathbf{v} \rangle \, \mathbf{w} \ .$$

OBRAZEK

Vzorec také můžeme v $\mathbb{R}^3$ nahlédnout z geometrické interpretace skalárního součinu jako součinu norem vynásobeného kosinem úhlu jimi sevřeného. Norma projekce je kosinus úhlu mezi $\mathbf{v}$ a $\mathbf{w}$ krát norma $\mathbf{v}$, tj.

$$\frac{\langle \mathbf{w} \,|\mathbf{v} \rangle}{\|\mathbf{v}\| \, \|\mathbf{w}\|} \|\mathbf{v}\| = \frac{\langle \mathbf{w} \,|\mathbf{v} \rangle}{\|\mathbf{w}\|}$$

a projekce je rovna této normě vynásobené znormovaným vektorem $\mathbf{w}$, tj.

$$\frac{\langle \mathbf{w} \,|\mathbf{v} \rangle}{\|\mathbf{w}\|} \frac{\mathbf{w}}{\|\mathbf{w}\|} = \frac{\langle \mathbf{w} \,|\mathbf{v} \rangle}{\|\mathbf{w}\|^2} \mathbf{w} \ .$$

OBRAZEK

Rovněž si všimněme souvislosti s vyjádřením vektoru $\mathbf{v}$ vzhledem k ortonormální bázi $(\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n)$ z tvrzení 8.19:

$$\mathbf{v} = \langle \mathbf{w}_1 \,|\mathbf{v} \rangle \, \mathbf{w}_1 + \langle \mathbf{w}_2 \,|\mathbf{v} \rangle \, \mathbf{w}_2 + \cdots + \langle \mathbf{w}_n \,|\mathbf{v} \rangle \, \mathbf{w}_n \ .$$

Sčítanec $\langle \mathbf{w}_i \,|\mathbf{v} \rangle \, \mathbf{w}_i$ je ortogonální projekcí vektoru $\mathbf{v}$ na přímku $\langle \mathbf{w}_i \rangle$.

Ortogonální projekci můžeme chápat jako endomorfismus prostoru V, který vektoru $\mathbf{v}$ přiřazuje vektor $\mathbf{v}_W$. V případě aritmetického vektorového prostoru $V = \mathbb{C}^n$ nebo $V = \mathbb{R}^n$ a standardního skalárního součinu máme

$$\mathbf{v}_W = \frac{\mathbf{w}^* \mathbf{v}}{\|\mathbf{w}\|^2} \mathbf{w} \ .$$

Součin skaláru $\mathbf{w}^* \mathbf{v} / \|\mathbf{w}\|^2$ a vektoru $\mathbf{w}$ lze zapsat maticovým součinem

$$\mathbf{v}_W = \mathbf{w} \frac{\mathbf{w}^* \mathbf{v}}{\|\mathbf{w}\|^2} = \frac{\mathbf{w}\mathbf{w}^*}{\|\mathbf{w}\|^2} \mathbf{v} \ .$$

Z toho vidíme, že matice $P_{\langle \mathbf{w} \rangle}$ projekce $p_{\langle \mathbf{w} \rangle}$ na přímku $\langle \mathbf{w} \rangle$ vzhledem ke kanonickým bázím je

$$P_{\langle \mathbf{w} \rangle} = [p_{\langle \mathbf{w} \rangle}]_K^K = \frac{\mathbf{w}\mathbf{w}^*}{\|\mathbf{w}\|^2} \ .$$

Příklad 8.33. V $\mathbb{R}^3$ se standardním skalárním součinem je projekce vektoru $\mathbf{v} = (x_1, x_2, x_3)^T$ na přímku $W = \langle \mathbf{w} \rangle$, kde $\mathbf{w} = (1, 2, 3)^T$, vektor

$$\mathbf{v}_W = \frac{\langle \mathbf{w} \,|\mathbf{v} \rangle}{\|\mathbf{w}\|^2}\mathbf{w} = \frac{(1,2,3)\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}}{14}\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \frac{1}{14}(x_1 + 2x_2 + 3x_3)\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$
$$= \frac{1}{14}\begin{pmatrix} x_1 + 2x_2 + 3x_3 \\ 2x_1 + 4x_2 + 6x_3 \\ 3x_1 + 6x_2 + 9x_3 \end{pmatrix}$$

Matice projekce na W vzhledem ke kanonickým bázím je

$$P_W = \frac{\mathbf{w}\mathbf{w}^T}{\|\mathbf{w}\|^2} = \frac{\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}(1,2,3)}{14} = \frac{1}{14}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 6 \\ 3 & 6 & 9 \end{pmatrix} \quad ,$$

což dává stejný vzorec.

Obecněji, pro konečně generovaný prostor V s ortonormální bází B máme podle tvrzení 8.21 o skalárním součinu vzhledem k ortonormální bázi

$$[\mathbf{v}_W]_B = \frac{[\mathbf{w}]_B^*[\mathbf{v}]_B}{\|\mathbf{w}\|^2}[\mathbf{w}]_B = [\mathbf{w}]_B\frac{[\mathbf{w}]_B^*[\mathbf{v}]_B}{\|\mathbf{w}\|^2} = \frac{[\mathbf{w}]_B[\mathbf{w}]_B^*}{\|\mathbf{w}\|^2}[\mathbf{v}]_B \quad ,$$

takže matice vzhledem k bázím B a B je

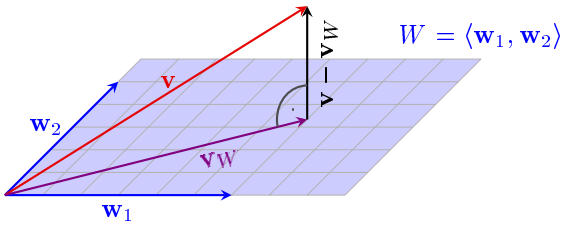
$$[p_{\langle \mathbf{w} \rangle}]_B^B = \frac{[\mathbf{w}]_B[\mathbf{w}]_B^*}{\|\mathbf{w}\|^2} \quad .$$

8.4.2. *Ortogonální projekce na obecný podprostor.* Nyní odvodíme vzorec pro ortogonální projekci vektoru $\mathbf{v}$ na obecný podprostor $W = \langle \mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k \rangle$ konečně generovaného prostoru V se skalárním součinem $\langle\,|\,\rangle$. (Předpoklad, že V je konečně generovaný můžeme vynechat.)

Vektor $\mathbf{v}_W$ leží v prostoru W, takže je lineární kombinací generátorů:

$$\mathbf{v}_W = a_1\mathbf{w}_1 + a_2\mathbf{w}_2 + \cdots + a_k\mathbf{w}_k \quad .$$

K tomu, aby $\mathbf{v}_W$ byl ortogonální projekcí $\mathbf{v}$, je nutné a stačí, aby vektor $\mathbf{v}_{W^\perp} = \mathbf{v} - \mathbf{v}_W$ byl kolmý na W.



To nastane právě tehdy (viz pozorování 8.24), když $\mathbf{v} - \mathbf{v}_W$ je kolmý na každý z vektorů $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k$. Dostáváme

$$0 = \langle \mathbf{w}_i \,|\mathbf{v} - \mathbf{v}_W \rangle = \langle \mathbf{w}_i \,|\mathbf{v} - a_1\mathbf{w}_1 - a_2\mathbf{w}_2 - \ldots - a_k\mathbf{w}_k \rangle$$
$$= \langle \mathbf{w}_i \,|\mathbf{v} \rangle - a_1 \langle \mathbf{w}_i \,|\mathbf{w}_1 \rangle - a_2 \langle \mathbf{w}_i \,|\mathbf{w}_2 \rangle - \ldots - a_k \langle \mathbf{w}_i \,|\mathbf{w}_k \rangle \quad .$$

Úpravou dostaneme pro každé $i \in \{1, 2, \ldots, k\}$ rovnici

$$a_1 \langle \mathbf{w}_i \,|\mathbf{w}_1 \rangle + a_2 \langle \mathbf{w}_i \,|\mathbf{w}_2 \rangle + \cdots + a_k \langle \mathbf{w}_i \,|\mathbf{w}_k \rangle = \langle \mathbf{w}_i \,|\mathbf{v} \rangle \quad .$$

Vektor koeficientů $(a_1, a_2, \ldots, a_k)^T \in T^n$ je tedy řešením soustavy rovnic

$$\left(\begin{array}{cccc|c} \langle \mathbf{w}_1 \,|\mathbf{w}_1 \rangle & \langle \mathbf{w}_1 \,|\mathbf{w}_2 \rangle & \ldots & \langle \mathbf{w}_1 \,|\mathbf{w}_k \rangle & \langle \mathbf{w}_1 \,|\mathbf{v} \rangle \\ \langle \mathbf{w}_2 \,|\mathbf{w}_1 \rangle & \langle \mathbf{w}_2 \,|\mathbf{w}_2 \rangle & \ldots & \langle \mathbf{w}_2 \,|\mathbf{w}_k \rangle & \langle \mathbf{w}_2 \,|\mathbf{v} \rangle \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \langle \mathbf{w}_k \,|\mathbf{w}_1 \rangle & \langle \mathbf{w}_k \,|\mathbf{w}_2 \rangle & \ldots & \langle \mathbf{w}_k \,|\mathbf{w}_k \rangle & \langle \mathbf{w}_k \,|\mathbf{v} \rangle \end{array}\right) \quad .$$

Dokázali jsme:

Tvrzení 8.34. *Nechť V je konečně generovaný prostor se skalárním součinem $\langle\,|\,\rangle$, $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k, \mathbf{v} \in V$, $W = \langle \mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k \rangle$. Ortogonální projekce vektoru $\mathbf{v}$ na podprostor W je rovná vektoru*

$$\mathbf{v}_W = a_1\mathbf{w}_1 + a_2\mathbf{w}_2 + \cdots + a_k\mathbf{w}_k \ ,$$

kde $(a_1, a_2, \ldots, a_k)^T$ je (libovolné) řešení soustavy rovnic s rozšířenou maticí

$$\left(\begin{array}{cccc|c} \langle \mathbf{w}_1 | \mathbf{w}_1 \rangle & \langle \mathbf{w}_1 | \mathbf{w}_2 \rangle & \ldots & \langle \mathbf{w}_1 | \mathbf{w}_k \rangle & \langle \mathbf{w}_1 | \mathbf{v} \rangle \\ \langle \mathbf{w}_2 | \mathbf{w}_1 \rangle & \langle \mathbf{w}_2 | \mathbf{w}_2 \rangle & \ldots & \langle \mathbf{w}_2 | \mathbf{w}_k \rangle & \langle \mathbf{w}_2 | \mathbf{v} \rangle \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \langle \mathbf{w}_k | \mathbf{w}_1 \rangle & \langle \mathbf{w}_k | \mathbf{w}_2 \rangle & \ldots & \langle \mathbf{w}_k | \mathbf{w}_k \rangle & \langle \mathbf{w}_k | \mathbf{v} \rangle \end{array}\right) .$$

Matice soustavy z tvrzení se nazývá *Gramova matice* vektorů $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k$. Je-li $B = (\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k)$ lineárně nezávislá, pak $(a_1, a_2, \ldots, a_k)^T$ jsou souřadnice vektoru $\mathbf{v}_W \in W$ vzhledem k bázi B. Ty jsou určeny jednoznačně, takže Gramova matice je regulární (detailně si promyslete jako cvičení). Naopak, jsou-li vektory $\mathbf{w}_i$ lineárně závislé, pak je Gramova matice singulární.

Determinant Gramovy matice vektorů $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k \in \mathbb{R}^n$ vzhledem ke standardnímu skalárnímu součinu je roven k-rozměrnému objemu rovnoběžnostěnu o stranách $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k$. Důkaz pro $k = n$ necháme jako cvičení, obecně jej dělat nebudeme.

Příklad 8.35. V prostoru reálných polynomů stupně nejvýše dva se skalárním součinem $\langle f\,|g\rangle = \int_0^1 fg$ najdeme nejlepší aproximaci polynomu x^2 pomocí lineárního polynomu $a + bx$ a chybu této aproximace.

Chceme tedy nalézt ortogonální projekci $\mathbf{v}_W = a+bx$ a kolmici vektoru $\mathbf{v} = x^2$ na prostor $W = \langle \mathbf{w}_1, \mathbf{w}_2 \rangle = \langle 1, x \rangle$. Koeficienty a, b jsou podle tvrzení řešením soustavy

$$\left(\begin{array}{cc|c} \langle \mathbf{w}_1 | \mathbf{w}_1 \rangle & \langle \mathbf{w}_1 | \mathbf{w}_2 \rangle & \langle \mathbf{w}_1 | \mathbf{v} \rangle \\ \langle \mathbf{w}_2 | \mathbf{w}_1 \rangle & \langle \mathbf{w}_2 | \mathbf{w}_2 \rangle & \langle \mathbf{w}_2 | \mathbf{v} \rangle \end{array}\right) = \left(\begin{array}{cc|c} \int_0^1 1 & \int_0^1 x & \int_0^1 x^2 \\ \int_0^1 x & \int_0^1 x^2 & \int_0^1 x^3 \end{array}\right) = \left(\begin{array}{cc|c} 1 & \frac{1}{2} & \frac{1}{3} \\ \frac{1}{2} & \frac{1}{3} & \frac{1}{4} \end{array}\right) .$$

Řešením soustavy dostaneme vektor $(a, b)^T = (-\frac{1}{6}, 1)^T$. Nejlepší aproximací vektoru $\mathbf{v} = x^2$ je tedy

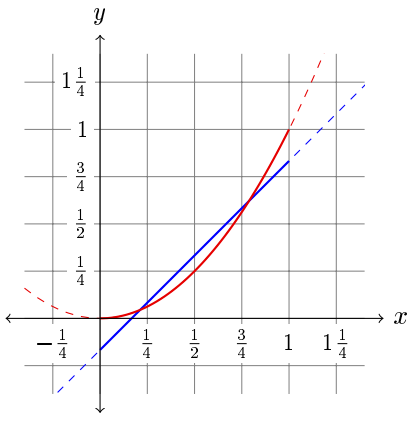
$$\mathbf{v}_W = a\mathbf{w}_1 + b\mathbf{w}_2 = -\frac{1}{6} + x,$$

chybový vektor je

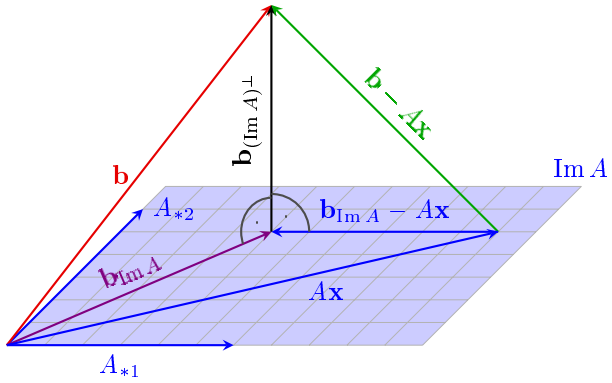
$$\mathbf{v}_{W^\perp} = \mathbf{v} - \mathbf{v}_W = x^2 - x + \frac{1}{6}$$

a velikost chyby je

$$\begin{aligned} \|\mathbf{v}_{W^\perp}\| &= \sqrt{\int_0^1 \left(x^2 - x + \frac{1}{6}\right)^2} = \sqrt{\int_0^1 x^4 - 2x^3 + \frac{4}{3}x^2 - \frac{1}{3}x + \frac{1}{36}} \\ &= \sqrt{\frac{1}{5} - \frac{1}{2} + \frac{4}{9} - \frac{1}{6} + \frac{1}{36}} = \sqrt{\frac{1}{30}} \end{aligned}$$



8.4.3. *Řešení neřešitelné soustavy lineárních rovnic.* Mějme soustavu rovnic $A\mathbf{x} = \mathbf{b}$, která nemá řešení. Řekněme, že A je matice typu $m \times n$ nad $\mathbb{R}$ nebo $\mathbb{C}$, typicky $m >> n$. Taková soustava může například vzniknout sestavením rovnic z velkého množství měření, která jsou zatížená chybami. Chceme nalézt „co nejlepší“ přibližné řešení $\mathbf{x}$ v tom smyslu, aby skutečná pravá strana $A\mathbf{x}$ byla co nejblíže ideální pravé straně $\mathbf{b}$, tj. aby norma $\|\mathbf{b} - A\mathbf{x}\|$ byla co nejmenší možná. V praktických aplikacích nás bude nejspíše zajímat eukleidovská norma na $\mathbb{C}^m$ (nebo $\mathbb{R}^m$), proto také říkáme, že soustavu řešíme *metodou nejmenších čtverců*. Zapíšeme-li $A\mathbf{x}$ jako lineární kombinaci sloupců, můžeme se na tento problém podívat tak, že hledáme $\mathbf{x} = (x_1, \dots, x_n)$, aby $A_{*1}x_1 + A_{*2}x_2 + \cdots + A_{*n}x_n$ byl co nejblíže vektoru $\mathbf{b}$. Podle tvrzení 8.31 (kde $V = T^m$, $W = \operatorname{Im} A$, $\mathbf{v} = \mathbf{b}$) je $A\mathbf{x}$ ortogonální projekce vektoru $\mathbf{b}$ na $\operatorname{Im} A$, kolmice vektoru $\mathbf{b}$ na $\operatorname{Im} A$ je chybový vektor $\mathbf{b} - A\mathbf{x}$.



Přeformulujeme si tvrzení 8.34 na tento důležitý speciální případ. Matice soustavy z tohoto tvrzení, tj. Gramova matice vektorů A_{*1}, A_{*2}, …, A_{*n}, má na místě (i, j) číslo $A_{*i} \cdot A_{*j} = A_{*i}^* A_{*j}$. Je tedy rovná matici A^*A. Pravou stranu soustavy z tvrzení můžeme maticově zapsat $A^*\mathbf{b}$. Dostáváme:

Tvrzení 8.36. *Nechť A je matice typu $m \times n$ nad $\mathbb{R}$ nebo $\mathbb{C}$, $\mathbf{b} \in \mathbb{R}^m$ (resp. $\mathbb{C}^m$). Množina všech řešení soustavy $A\mathbf{x} = \mathbf{b}$ metodou nejmenších čtverců je rovna množině všech (přesných) řešení soustavy*

$$A^*A\mathbf{x} = A^*\mathbf{b}$$

Soustavě $A^*A\mathbf{x} = A^*\mathbf{b}$ říkáme *soustava normálních rovnic* příslušná soustavě $A\mathbf{x} = \mathbf{b}$. Pokud A má lineárně nezávislé sloupce, pak je vektor $\mathbf{x}$ určen jednoznačně, takže A^*A je regulární a dostáváme jednoznačně řešení původní soustavy metodou nejmenších čtverců.

Příklad 8.37. Řešení reálné soustavy $(A|\mathbf{b})$, kde

$$(A|\mathbf{b}) = \left(\begin{array}{cc|c} 2 & 0 & 3 \\ 1 & 1 & 5 \\ -2 & -1 & -2 \end{array}\right) ,$$

metodou nejmenších čtverců je řešení soustavy

$$A^TA\mathbf{x} = A^T\mathbf{b}$$

$$\begin{pmatrix} 2 & 1 & -2 \\ 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 1 & 1 \\ -2 & -1 \end{pmatrix} \mathbf{x} = \begin{pmatrix} 2 & 1 & -2 \\ 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} 3 \\ 5 \\ -2 \end{pmatrix}$$

$$\begin{pmatrix} 9 & 3 \\ 3 & 2 \end{pmatrix} \mathbf{x} = \begin{pmatrix} 15 \\ 7 \end{pmatrix} .$$

Eliminací dostaneme $(x_1, x_2)^T = (1, 2)^T$.

Pravá strana původní soustavy vyjde $A(1, 2)^T = (2, 3, -4)$, je to ortogonální projekce vektoru $\mathbf{b}$ na prostor $\operatorname{Im} A$. Chybový vektor je

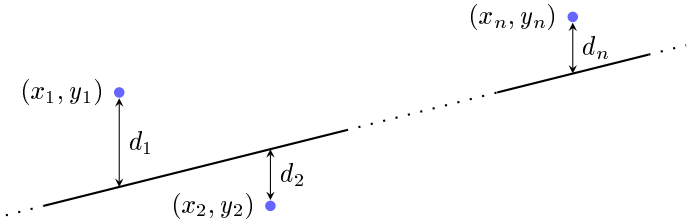
$$\mathbf{b}_{(\operatorname{Im} A)^\perp} = (3, 5, -2)^T - (2, 3, -4)^T = (1, 2, 2)^T$$

a velikost chyby je

$$\left\|\mathbf{b}_{(\operatorname{Im} A)^\perp}\right\| = \sqrt{1^2 + 2^2 + 2^2} = 3 .$$

Jednou ze situací, která vede na přibližné řešení soustavy rovnic, je *lineární regrese*, kdy chceme co nejlépe proložit přímku $y = ax + b$ danými naměřenými hodnotami (x_1, y_1), (x_2, y_2), $\ldots$, (x_n, y_n). V tomto případě hledáme nejlepší „řešení“ soustavy

$$\left(\begin{array}{cc|c} x_1 & 1 & y_1 \\ x_2 & 1 & y_2 \\ \vdots & \vdots & \vdots \\ x_n & 1 & y_n \end{array}\right) .$$



Obrázek 18. Lineární regrese – minimalizujeme $\sum d_i^2$.

Daty můžeme prokládat složitější útvary, jako paraboly, polynomy vyššího stupně, elipsy (např. při hledání dráhy planety), apod. Takové úlohy vedou na hledání řešení soustavy metodou nejmenších čtverců.

Příklad 8.38. Metodou nejmenších čtverců proložíme body $(0,1)$, $(1,1)$, $(2,2)$, $(3,4)$, $(4,5)$ v $\mathbb{R}^2$ přímku $y = ax + b$. Koeficienty a, b jsou řešením soustavy rovnic

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

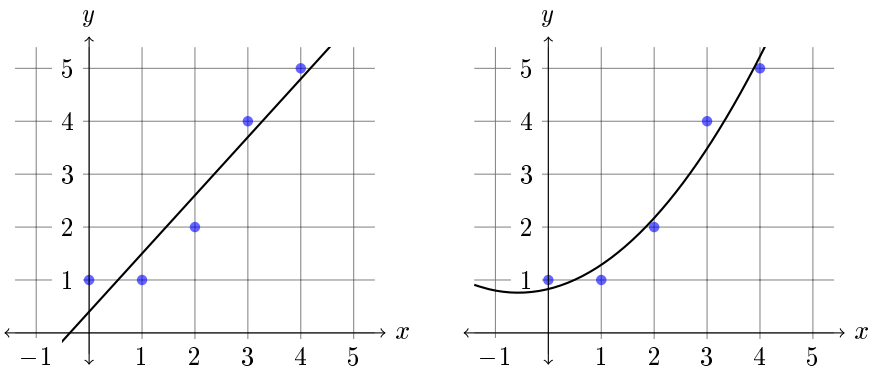
metodou nejmenších čtverců. Příslušná soustava normálních rovnic je

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 2 & 1 \\ 3 & 1 \\ 4 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 2 \\ 4 \\ 5 \end{pmatrix} ,$$

$$\begin{pmatrix} 30 & 10 \\ 10 & 5 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 37 \\ 13 \end{pmatrix} .$$

Řešením vyjde $(a, b)^T = (11/10, 2/5)$ takže hledaná přímka je

$$y = \frac{11}{10}x + \frac{2}{5} .$$



Příklad 8.39. Stejnými body proložíme co nejlépe parabolu $y = ax^2 + bx + c$. Koeficienty jsou řešením soustavy

$$\left(\begin{array}{ccc|c} 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 4 & 2 & 1 & 2 \\ 9 & 3 & 1 & 4 \\ 16 & 4 & 1 & 5 \end{array}\right)$$

metodou nejmenších čtverců. Vyjde $(a, b, c)^T = ...$

$$y =$$

8.4.4. *Matice ortogonální projekce.* Uvažujme podprostor W dimenze n aritmetického prostoru $\mathbb{C}^m$ (nebo $\mathbb{R}^m$) se standardním skalárním součinem. Určíme matici P_W ortogonální projekce p_W na podprostor W vzhledem ke kanonickým bázím.

Napíšeme si do sloupců matice A vektory nějaké báze prostoru W, tj. A je matice typu $m \times n$ s lineárně nezávislými sloupci. Ortogonální projekce vektoru $\mathbf{b}$ na $\operatorname{Im} A = W$ je podle diskuze výše vektor $A\mathbf{x}$, kde $\mathbf{x}$ je řešením rovnice $A^*A\mathbf{x} = A^*\mathbf{b}$. Protože A má lineárně nezávislé sloupce, je Gramova matice A^*A regulární, takže můžeme psát $\mathbf{x} = (A^*A)^{-1}A^*\mathbf{b}$. Projekci tedy můžeme vyjádřit $p_W(\mathbf{b}) = A\mathbf{x} = A(A^*A)^{-1}A^*\mathbf{b}$ a matice p_W vzhledem ke kanonickým bázím je

$$P_W = A(A^*A)^{-1}A^* \ .$$

Každá taková matice je, jak se snadno ověří, hermitovská a splňuje $P_W P_W = P_W$, což je též geometricky vidět z toho, že f_W je projekce. Naopak, libovolná matice splňující tyto dvě podmínky je maticí projekce na nějaký podprostor:

Tvrzení 8.40. *Nechť P je čtvercová reálná nebo komplexní matice řádu m. Následující tvrzení jsou ekvivalentní*

(1) *P je hermitovská (tj. $P^* = P$) a $P^2 = P$*
(2) *P je maticí ortogonální projekce na nějaký podprostor W aritmetického vektorového prostoru $\mathbb{R}^n$ (resp. $\mathbb{C}^n$) se standardním skalárním součinem vzhledem ke kanonickým bázím.*

Důkaz. (2) $\Rightarrow$ (1) jsme již dokázali. Nechť P je tedy hermitovská matice, pro kterou platí $P^2 = P$. Položíme $W = \operatorname{Im} P$ (jiná volba není, má-li být f_P projekce na nějaký podprostor, pak tento podprostor musí nutně být obrazem f_P). Z vlastnosti $P^2 = P$ plyne, že $P\mathbf{u} = \mathbf{u}$ pro libovolný vektor $\mathbf{u} \in W$, protože pro každý takový vektor $\mathbf{u}$ existuje $\mathbf{v}$ takové, že $P\mathbf{v} = \mathbf{u}$, z čehož dostáváme

$$P\mathbf{u} = P(P\mathbf{v}) = PP\mathbf{v} = P\mathbf{v} = \mathbf{u} \ .$$

Nyní $\operatorname{Ker} P$ je podle diskuze o podprostorech ortogonální doplněk $\operatorname{Im} P^*$ a tento prostor je rovný $\operatorname{Im} P = W$, protože P je hermitovská. Platí tedy $W^\perp = \operatorname{Ker} P$. Nyní pro libovolný vektor $\mathbf{v}$ je $\mathbf{v}_{W^\perp} \in \operatorname{Ker} P$, takže

$$P\mathbf{v} = P(\mathbf{v}_W + \mathbf{v}_{W^\perp}) = P\mathbf{v}_W + P\mathbf{v}_{W^\perp} = P\mathbf{v}_W = \mathbf{v}_W \ .$$

Z toho vidíme, že obraz vektoru $\mathbf{v}$ při zobrazení f_P je skutečně ortogonální projekce vektoru $\mathbf{v}$ na W, jak jsme chtěli. □

8.5. **Gram-Schmidtova ortogonalizace, QR-rozklad.**

Vzorec pro ortogonální projekci vektoru $\mathbf{v} \in V$ na podprostor W se značně zjednoduší, je-li báze ($\mathbf{w}_1$, $\mathbf{w}_2$, …, $\mathbf{w}_k$) prostoru W ortogonální. Gramova matice v tvrzení 8.34 je totiž v tomto případě diagonální. Protože odvození tvaru ortogonální projekce je krátké, zopakujeme jej v tomto speciálním případě. Hledáme vektor $\mathbf{v}_W = a_1\mathbf{w}_1 + a_2\mathbf{w}_2 + \cdots + a_k\mathbf{w}_k$ tak, aby vektor $\mathbf{v} - \mathbf{v}_W$ byl kolmý na každý z vektorů $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k$. Dostáváme

$$\begin{aligned} 0 &= \langle \mathbf{w}_i \,|\mathbf{v} - \mathbf{v}_W\rangle = \langle \mathbf{w}_i \,|\mathbf{v} - a_1\mathbf{w}_1 - a_2\mathbf{w}_2 - \ldots - a_k\mathbf{w}_k\rangle \\ &= \langle \mathbf{w}_i \,|\mathbf{v}\rangle - a_1\langle \mathbf{w}_i \,|\mathbf{w}_1\rangle - a_2\langle \mathbf{w}_i \,|\mathbf{w}_2\rangle - \ldots - a_k\langle \mathbf{w}_i \,|\mathbf{w}_k\rangle \\ &= \langle \mathbf{w}_i \,|\mathbf{v}\rangle - a_i\langle \mathbf{w}_i \,|\mathbf{w}_i\rangle \\ a_i &= \frac{\langle \mathbf{w}_i \,|\mathbf{v}\rangle}{\|\mathbf{w}_i\|^2} \ . \end{aligned}$$

Tvrzení 8.41. *Nechť V je konečně generovaný prostor se skalárním součinem $\langle\,|\,\rangle$, $\{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k\}$ ortogonální množina nenulových vektorů, $\mathbf{v} \in V$, $W = \langle \mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k\rangle$. Ortogonální projekce vektoru $\mathbf{v}$ na podprostor W je rovná vektoru*

$$\mathbf{v}_W = \frac{\langle \mathbf{w}_1 \,|\mathbf{v}\rangle}{\|\mathbf{w}_1\|^2}\mathbf{w}_1 + \frac{\langle \mathbf{w}_2 \,|\mathbf{v}\rangle}{\|\mathbf{w}_2\|^2}\mathbf{w}_2 + \cdots + \frac{\langle \mathbf{w}_k \,|\mathbf{v}\rangle}{\|\mathbf{w}_k\|^2}\mathbf{w}_k \ .$$

Jinými slovy, souřadnice $\mathbf{v}_W$ vzhledem k bázi $B = (\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_k)$ prostoru W jsou

$$[\mathbf{v}_W]_B = \left(\frac{\langle \mathbf{w}_1 \,|\mathbf{v}\rangle}{\|\mathbf{w}_1\|^2}, \frac{\langle \mathbf{w}_2 \,|\mathbf{v}\rangle}{\|\mathbf{w}_2\|^2}, \dots, \frac{\langle \mathbf{w}_k \,|\mathbf{v}\rangle}{\|\mathbf{w}_k\|^2} \right) \ .$$

V případě, že B je dokonce ortonormální, vzorec se dále zjednodušuje na

$$\mathbf{v}_W = \langle \mathbf{w}_1 \,|\mathbf{v}\rangle \, \mathbf{w}_1 + \langle \mathbf{w}_2 \,|\mathbf{v}\rangle \, \mathbf{w}_2 + \cdots + \langle \mathbf{w}_k \,|\mathbf{v}\rangle \, \mathbf{w}_k \ .$$

Výraz na pravé straně je shodný (až na přeznačení) s výrazem z tvrzení 8.19 o souřadnicích vzhledem k ortonormální bázi. Skutečně, tvrzení 8.41 je jeho zobecněním. Pokud $\mathbf{v} \in W$, pak $\mathbf{v} = \mathbf{v}_W$ a vzorec dává vyjádření $\mathbf{v}$ vzhledem k ortonormální bázi $(\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_k)$ prostoru W. V případě, že $\mathbf{v}$ ve W neleží, *stejný vzorec* nám dává souřadnice jeho ortogonální projekce.

Příklad 8.42. V $\mathbb{R}^3$ se standardním skalárním součinem je $((1,1,2)^T, (2,0,-1)^T)$ ortogonální množina. Ortogonální projekce vektoru $\mathbf{v} = (1,2,3)^T$ na rovinu $W = \langle (1,1,2)^T, (2,0,-1)^T \rangle$ je tedy

$$\begin{aligned} \mathbf{v}_W &= \frac{(1,1,2)(1,2,3)^T}{(1,1,2)(1,1,2)^T} \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix} + \frac{(2,0,-1)(1,2,3)^T}{(2,0,-1)(2,0,-1)^T} \begin{pmatrix} 2 \\ 0 \\ -1 \end{pmatrix} \\ &= \frac{9}{6} \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix} - \frac{1}{5} \begin{pmatrix} 2 \\ 0 \\ -1 \end{pmatrix} = \frac{1}{10} \begin{pmatrix} 11 \\ 15 \\ 32 \end{pmatrix} \ . \end{aligned}$$

Skutečně, chybový vektor $\mathbf{v}_{W^\perp} = \mathbf{v} - \mathbf{v}_W = \frac{1}{10}(-1,5,-2)^T$ je kolmý na oba dva vektory $(1,1,2)^T$, $(2,0,-1)^T$.

8.5.1. *Gram-Schmidtova ortogonalizace.* Již několikrát jsme si všimli, že je výhodné mít v prostoru ortogonální nebo ortonormální bázi. Vzhledem k ortonormální bázi se snadno počítají souřadnice (tvrzení 8.19), skalární součin přechází na standardní (tvrzení 8.21), dobře se počítají ortogonální doplňky (pozorování 8.28) a máme-li v podprostoru ortogonální bázi, můžeme na tento podprostor jednoduše počítat ortogonální projekce (tvrzení 8.41).

Gram-Schmidtův ortogonalizační proces „vyrobí“ z jakékoliv báze $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$ ortogonální bázi $(\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_n)$ a to tak, že se pro každé $i \in \{1, 2, \dots, n\}$ zachovají lineární obaly prvních i vektorů, tj. $\langle \mathbf{v}_1 \rangle = \langle \mathbf{w}_1 \rangle$, $\langle \mathbf{v}_1, \mathbf{v}_2 \rangle = \langle \mathbf{w}_1, \mathbf{w}_2 \rangle$, atd.

První vektor zvolíme $\mathbf{w}_1 = \mathbf{v}_1$. Vektor $\mathbf{w}_2$ bude kolmice $\mathbf{v}_2$ na přímku $\langle \mathbf{w}_1 \rangle = \langle \mathbf{v}_1 \rangle$, vektor $\mathbf{w}_3$ bude kolmice na rovinu $\langle \mathbf{w}_1, \mathbf{w}_2 \rangle = \langle \mathbf{v}_1, \mathbf{v}_2 \rangle$, atd. Obecně, $\mathbf{w}_i$ určíme jako kolmici na lineární obal předchozích vektorů $\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_{i-1}$.

OBRAZEK

V průběhu procesu se zachovává vlastnost $\langle \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_i \rangle = \langle \mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_i \rangle$, protože nový vektor $\mathbf{w}_i$ se volí

$$\mathbf{w}_i = (\mathbf{v}_i)_{W^\perp} = \mathbf{v}_i - (\mathbf{v}_i)_W$$

kde $W = \langle \mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_{i-1} \rangle = \langle \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_{i-1} \rangle$. Speciálně, $(\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_n)$ generuje V, takže je to báze ($\dim(V)$-prvková posloupnost generátorů je vždy bází, viz bod (2) v pozorování 5.57). Tato báze je ortogonální, protože $\mathbf{w}_i$ se volí tak, aby byl kolmý k vektorům $\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_{i-1}$.

Protože $\mathbf{w}_1, \dots, \mathbf{w}_{i-1}$ je ortogonální báze lineárního obalu těchto vektorů, máme pro vektor $\mathbf{w}_i$ explicitní vzorec z tvrzení 8.41:

$$\mathbf{w}_i = \mathbf{v}_i - (\mathbf{v}_i)_W = \mathbf{v}_i - \left(\frac{\langle \mathbf{w}_1 \,|\mathbf{v}_i\rangle}{\|\mathbf{w}_1\|^2} \mathbf{w}_1 + \frac{\langle \mathbf{w}_2 \,|\mathbf{v}_i\rangle}{\|\mathbf{w}_2\|^2} \mathbf{w}_2 + \cdots + \frac{\langle \mathbf{w}_{i-1} \,|\mathbf{v}_i\rangle}{\|\mathbf{w}_{i-1}\|^2} \mathbf{w}_{i-1} \right) \ .$$

Pokud chceme najít ortonormální bázi, můžeme buď vektory znormovat na konci, nebo je normujeme průběžně, čímž nám také ve vzorci odpadají jmenovatelé.

Příklad 8.43. V podprostoru

$$W = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\} = \{(1,2,0,1)^T, (1,-1,1,0)^T, (0,1,1,3)^T\}$$

prostoru $\mathbb{R}^4$ se standardním skalárním součinem najdeme ortonormální bázi $\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3$. Použijeme Gram-Schmidtovou ortogonalizací aplikovanou na vektory $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$. Budeme průběžně normovat, vektory $\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3$ před znormováním označíme $\mathbf{w}_1'$, $\mathbf{w}_2'$, $\mathbf{w}_3'$. Uvědomme si, že nemusíme ověřovat lineární nezávislost vektorů $\mathbf{v}_i$ (tj. že tvoří bázi W), pokud je totiž vektor $\mathbf{v}_i$ lineární kombinací předchozích, pak $\mathbf{w}_i$, jakožto kolmice $\mathbf{v}_i$ na lineární obal

$\langle \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_{i-1} \rangle$, je nulový vektor.

$$\mathbf{w}_1' = \mathbf{v}_1 = \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix}$$

$$\mathbf{w}_1 = \frac{\mathbf{w}_1'}{\|\mathbf{w}_1'\|} = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix}$$

$$\mathbf{w}_2' = \mathbf{v}_2 - \langle \mathbf{w}_1 | \mathbf{v}_2 \rangle \mathbf{w}_1 = \begin{pmatrix} 1 \\ -1 \\ 1 \\ 0 \end{pmatrix} - \frac{1}{\sqrt{6}}(1,2,0,1)(1,-1,1,0)^T \frac{1}{\sqrt{6}} \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 \\ -1 \\ 1 \\ 0 \end{pmatrix} + \frac{1}{6} \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix} = \frac{1}{6} \begin{pmatrix} 7 \\ -4 \\ 6 \\ 1 \end{pmatrix}$$

$$\mathbf{w}_2 = \frac{\mathbf{w}_2'}{\|\mathbf{w}_2'\|} = \frac{1}{\sqrt{102}} \begin{pmatrix} 7 \\ -4 \\ 6 \\ 1 \end{pmatrix}$$

$$\mathbf{w}_3' = \mathbf{v}_3 - \langle \mathbf{w}_1 | \mathbf{v}_3 \rangle \mathbf{w}_1 - \langle \mathbf{w}_2 | \mathbf{v}_3 \rangle \mathbf{w}_2$$

$$= \begin{pmatrix} 0 \\ 1 \\ 1 \\ 3 \end{pmatrix} - \frac{1}{\sqrt{6}}(1,2,0,1)(0,1,1,3)^T \frac{1}{\sqrt{6}} \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix}$$

$$- \frac{1}{\sqrt{102}}(7,-4,6,1)(0,1,1,3)^T \frac{1}{\sqrt{102}} \begin{pmatrix} 7 \\ -4 \\ 6 \\ 1 \end{pmatrix}$$

$$= \begin{pmatrix} 0 \\ 1 \\ 1 \\ 3 \end{pmatrix} - \frac{5}{6} \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix} - \frac{5}{102} \begin{pmatrix} 7 \\ -4 \\ 6 \\ 1 \end{pmatrix} = \frac{1}{102} \begin{pmatrix} -120 \\ -48 \\ 72 \\ 216 \end{pmatrix} = \frac{4}{51} \begin{pmatrix} -15 \\ -6 \\ 9 \\ 27 \end{pmatrix}$$

$$\mathbf{w}_3 = \frac{\mathbf{w}_3'}{\|\mathbf{w}_3'\|} = \frac{1}{\sqrt{1039}} \begin{pmatrix} -15 \\ -6 \\ 9 \\ 27 \end{pmatrix}$$

Získali jsme ortonormální bázi

$$\left(\frac{1}{\sqrt{6}} \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{102}} \begin{pmatrix} 7 \\ -4 \\ 6 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{1039}} \begin{pmatrix} -15 \\ -6 \\ 9 \\ 27 \end{pmatrix} \right)$$

Z Gram-Schmidtovy ortogonalizace vidíme, že každý konečně generovaný prostor má ortonormální bázi, protože stačí zortogonalizovat a znormovat libovolnou bázi. Obecněji, každou ortogonální posloupnost můžeme rozšířit do ortogonální báze.

Věta 8.44. *Nechť V je konečně generovaný prostor se skalárním součinem $\langle | \rangle$. Každá ortogonální (resp. ortonormální) posloupnost nenulových vektorů z V jde doplnit do ortogonální (resp. ortonormální) báze.*

Speciálně, každý konečně generovaný prostor se skalárním součinem má ortonormální bázi.

Důkaz. Nechť $C = (\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_k)$ je ortogonální posloupnost nenulových vektorů. Tato posloupnost je lineárně nezávislá (viz tvrzení 8.14), proto jde doplnit vektory $\mathbf{v}_{k+1}, \dots, \mathbf{v}_n$ na bázi V (viz důsledek 5.54). „Dokončením" Gram-Schimdtovy ortogonalizace získáme vektory $\mathbf{w}_{k+1}, \dots, \mathbf{w}_n$ takové, že $(\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_n)$ je ortogonální bází. Je-li C navíc ortonormální, můžeme vektory $\mathbf{w}_{k+1}, \dots$ znormovat a získáme ortonormální bázi.

Poznámka: Mohlo by se zdát, že jsme existenci ortonormální báze dokázali kruhem. Ve větě 8.29 o ortogonálním doplňku jsme existenci předpokládali a z této věty plyne existence ortogonální projekce a kolmice vektorů. Ke Gram-Schmidtově ortogonalizaci tuto větu ale nepotřebujeme, prostě definujeme vektory $\mathbf{w}_i$ odvozeným vzorcem a získáme ortogonální bázi. □

Gram-Schmidtova ortogonalizace je numericky nestabilní. Na ortogonalizaci se v některých praktických úlohách proto používají jiné, numericky stabilní algoritmy, například algoritmus využívající Householderovy transformace, nebo algoritmus využívající Givensovy rotace.

8.5.2. *QR-rozklad.* Ze vzorce pro Gram-Schmidtovu ortogonalizace je vidět, že původní vektory $\mathbf{v}_i$ lze vyjádřit jako lineární kombinaci vektorů $\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_i$ (ty jsou navzájem kolmé a můžeme je volit jednotkové). Použijeme-li tento fakt na aritmetické vektory a standardní skalární součin, získáme vyjádření matice $(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_n)$ jako součinu matice $(\mathbf{w}_1|\mathbf{w}_2|\dots|\mathbf{w}_n)$ a horní trojúhelníkové matice. Tomuto vyjádření říkáme QR-rozklad.

Tvrzení 8.45 (o QR-rozkladu)**.** *Nechť A je reálná nebo komplexní matice typu $m \times n$ s lineárně nezávislými sloupci. Pak existuje matice Q typu $m \times n$ nad stejným tělesem s ortonormálními sloupci (vzhledem ke standardnímu skalárnímu součinu) a horní trojúhelníková matice R řádu n s kladnými reálnými prvky na hlavní diagonále taková, že platí $A = QR$.*

Důkaz. Označíme $\mathbf{v}_1, \dots, \mathbf{v}_n$ sloupcové vektory matice A. S těmito vektory provedeme Gram-Schmidtovu ortogonalizaci s průběžným normováním, tj.

$$\mathbf{w}_i' = \mathbf{v}_i - \langle \mathbf{w}_1 | \mathbf{v}_i \rangle \mathbf{w}_1 - \langle \mathbf{w}_2 | \mathbf{v}_i \rangle \mathbf{w}_2 - \dots - \langle \mathbf{w}_{i-1} | \mathbf{v}_i \rangle \mathbf{w}_{i-1}, \quad \mathbf{w}_i = \frac{\mathbf{w}_i'}{\|\mathbf{w}_i'\|} .$$

Z toho získáme vyjádření

$$\begin{aligned} \mathbf{v}_i &= \mathbf{w}_i' + \langle \mathbf{w}_1 | \mathbf{v}_i \rangle \mathbf{w}_1 + \langle \mathbf{w}_2 | \mathbf{v}_i \rangle \mathbf{w}_2 + \dots + \langle \mathbf{w}_{i-1} | \mathbf{v}_i \rangle \mathbf{w}_{i-1} \\ &= \langle \mathbf{w}_1 | \mathbf{v}_i \rangle \mathbf{w}_1 + \langle \mathbf{w}_2 | \mathbf{v}_i \rangle \mathbf{w}_2 + \dots + \langle \mathbf{w}_{i-1} | \mathbf{v}_i \rangle \mathbf{w}_{i-1} + \|\mathbf{w}_i'\| \mathbf{w}_i \end{aligned}$$

Tyto vztahy můžeme maticově zapsat

$$(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_n) = (\mathbf{w}_1|\dots|\mathbf{w}_n) \begin{pmatrix} \|\mathbf{w}_1'\| & \langle \mathbf{w}_1 | \mathbf{v}_2 \rangle & \dots & \langle \mathbf{w}_1 | \mathbf{v}_n \rangle \\ 0 & \|\mathbf{w}_2'\| & \dots & \langle \mathbf{w}_2 | \mathbf{v}_n \rangle \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & \|\mathbf{w}_n'\| \end{pmatrix}$$

□

Příklad 8.46. Vypočítáme QR-rozklad reálné matice

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

Je potřeba provést Gram-Schmidtovu ortogonalizaci s průběžným normování pro vektory $\mathbf{v}_1 = (1, 2, 0, 1)^T$, $\mathbf{v}_2 = (1, -1, -1, 0)^T$, $\mathbf{v}_3 = (0, 1, 1, 3)^T$. To jsme provedli v příkladu 8.43. Nalezli jsme vektory

$$(\mathbf{w}_1', \mathbf{w}_2', \mathbf{w}_3') = \left(\begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix}, \frac{1}{6} \begin{pmatrix} 7 \\ -4 \\ 6 \\ 1 \end{pmatrix}, \frac{4}{51} \begin{pmatrix} -15 \\ -6 \\ 9 \\ 27 \end{pmatrix} \right)$$

$$(\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3) = \left(\frac{1}{\sqrt{6}} \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{102}} \begin{pmatrix} 7 \\ -4 \\ 6 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{1039}} \begin{pmatrix} -15 \\ -6 \\ 9 \\ 27 \end{pmatrix} \right)$$

a z průběhu ortogonalizace získáme vztahy

$$\begin{aligned}
\mathbf{w}'_1 &= \mathbf{v}_1, \quad \mathbf{w}_1 = \frac{1}{\sqrt{6}}\mathbf{w}'_1\\
\mathbf{w}'_2 &= \mathbf{v}_2 - \frac{1}{\sqrt{6}}\mathbf{w}_1, \quad \mathbf{w}_2 = \frac{6}{\sqrt{102}}\mathbf{w}'_2\\
\mathbf{w}'_3 &= \mathbf{v}_3 - \frac{5}{\sqrt{6}}\mathbf{w}_1 - \frac{5}{\sqrt{102}}\mathbf{w}_2, \quad \mathbf{w}_3 = \frac{51}{4\sqrt{1039}}\mathbf{w}'_3
\end{aligned}$$

Z těchto vztahů vyjádříme vektory $\mathbf{v}_i$

$$\begin{aligned}
\mathbf{v}_1 &= \sqrt{6}\mathbf{w}_1\\
\mathbf{v}_2 &= \frac{1}{\sqrt{6}}\mathbf{w}_1 + \frac{\sqrt{102}}{6}\mathbf{w}_2\\
\mathbf{v}_3 &= \frac{5}{\sqrt{6}}\mathbf{w}_1 + \frac{5}{\sqrt{102}}\mathbf{w}_2 + \frac{4\sqrt{1039}}{51}\mathbf{w}_3
\end{aligned}$$

a zapíšeme maticově

$$\begin{pmatrix} 1 & 1 & 0\\ 2 & -1 & 1\\ 0 & 1 & 1\\ 1 & 0 & 3 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{6}} & \frac{7}{\sqrt{102}} & -\frac{15}{\sqrt{1039}}\\ \frac{2}{\sqrt{6}} & -\frac{4}{\sqrt{102}} & -\frac{6}{\sqrt{1039}}\\ 0 & \frac{6}{\sqrt{102}} & \frac{9}{\sqrt{1039}}\\ \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{102}} & \frac{27}{\sqrt{1039}} \end{pmatrix} \begin{pmatrix} \sqrt{6} & \frac{1}{\sqrt{6}} & \frac{5}{\sqrt{7}}\\ 0 & \frac{\sqrt{102}}{6} & \frac{5}{\sqrt{102}}\\ 0 & 0 & \frac{4\sqrt{1039}}{51} \end{pmatrix}$$

QR-rozklad jde použít na hledání řešení soustavy metodou nejmenších čtverců. Všimněte si, že pro matici Q v rozkladu $A = QR$ platí $Q^*Q = I_n$ (díky ortonormalitě sloupců), takže příslušnou normální soustavu rovnic můžeme zapsat

$$\begin{aligned}
A^*A\mathbf{x} &= A^*\mathbf{b}\\
(QR)^*QR\mathbf{x} &= (QR)^*\mathbf{b}\\
R^*Q^*QR\mathbf{x} &= R^*Q^*\mathbf{b}\\
R^*R\mathbf{x} &= R^*Q^*\mathbf{b}\\
R\mathbf{x} &= Q^*\mathbf{b}\ .
\end{aligned}$$

Poslední soustava má horní trojúhelníkovou matici, takže řešení můžeme spočítat zpětnou substitucí. Postup v této podobě můžeme samozřejmě použít jen pro matice A s lineárně nezávislými sloupci.

QR-rozklad se také používá v jednom z algoritmů na hledání vlastních čísel, viz **??**.

8.6. Unitární a ortogonální matice.

Posledním pojmem kterým se budeme stručně zabývat je unitární matice. Pro jednoduchost budeme uvažovat pouze standardní skalární součin v $\mathbb{R}^n$ nebo $\mathbb{C}^n$. Čtvercová matice U řádu n určuje endomorfismus f_U tohoto prostoru. Pokud tento endomorfismus zachovává skalární součin (tj. také všechny metrické vlastnosti jako délky a úhly), nazýváme matici U *unitární*, v reálném případě též *ortogonální*. Tuto vlastnost lze vyjádřit mnoha ekvivalentními způsoby, například:

Tvrzení 8.47. *Nechť U je reálná (resp. komplexní) čtvercová matice řádu n. Následující tvrzení jsou ekvivalentní.*

1. *f_U zachovává standardní skalární součin, tj. pro libovolné $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$ (resp. $\mathbb{C}^n$) platí $U\mathbf{u} \cdot U\mathbf{v} = \mathbf{u} \cdot \mathbf{v}$.*
2. *f_U zachovává eukleidovskou normu, tj. pro libovolný vektor $\mathbf{v} \in \mathbb{R}^n$ (resp. $\mathbb{C}^n$) platí $\|U\mathbf{v}\| = \|\mathbf{v}\|$*
3. *f_U zobrazuje ortonormální bázi na ortonormální bázi.*
4. *$U^{-1} = U^*$, tj. $UU^* = U^*U = I_n$*
5. *Řádky matice U tvoří ortonormální bázi.*
6. *Sloupce matice U tvoří ortonormální bázi.*

Důkaz. Skutečnost, že řádky matice U jsou ortonormální (tedy tvoří ortonormální bázi) můžeme maticově zapsat $UU^* = I_n$. Podobně, sloupce jsou ortonormální právě tehdy, když $U^*U = I_n$. Triviálně tedy platí (4) $\Rightarrow$ (5),(6). Naopak, pokud $UU^* = I_n$ nebo $U^*U = I_n$, pak U je regulární podle charakterizace regulárních matic ve větě 4.30 a platí a $U^{-1} = U^*$. Body (4),(5),(6) jsou proto ekvivalentní.

(4) $\Rightarrow$ (1). Pokud $UU^* = U^*U = I_n$, pak f_U zachovává standardní skalární součin:

$$U\mathbf{u} \cdot U\mathbf{v} = (U\mathbf{u})^*U\mathbf{v} = \mathbf{u}^*U^*U\mathbf{v} = \mathbf{u}^*\mathbf{v} = \mathbf{u} \cdot \mathbf{v}\ .$$

(1) ⇒ (2). Pokud f_U zachovává standardní skalární součin, pak také zachovává eukleidovskou normu, protože ta je určená skalárním součinem. Obšírněji: $\|U\mathbf{v}\| = \sqrt{U\mathbf{v}\cdot U\mathbf{v}} = \sqrt{\mathbf{v}\cdot\mathbf{v}} = \|\mathbf{v}\|$. (1) ⇒ (3) je rovněž snadné.

(3) ⇒ (6). Kvůli (3) musí být $U\mathbf{e}_1$, $U\mathbf{e}_2$, …, $U\mathbf{e}_n$ ortonormální báze, což dává podmínku (6).

K dokončení důkazu stačí zdůvodnit (2) ⇒ (1), tedy, že zachovávání normy je postačující podmínkou pro zachovávání skalárního součinu. To plyne z polarizačních identit, které říkají, že skalární součin je určen normou. Obšírněji, protože U zachovává normu, dostaneme z bodu (4) tvrzení 8.7

$$\begin{aligned}\operatorname{Re}(U\mathbf{u}\cdot U\mathbf{v}) &= \frac{1}{2}(\|U\mathbf{u}+U\mathbf{v}\|^2 - \|U\mathbf{u}\|^2 - \|U\mathbf{v}\|^2)\\ &= \frac{1}{2}(\|U(\mathbf{u}+\mathbf{v})\|^2 - \|U\mathbf{u}\|^2 - \|U\mathbf{v}\|^2) = \frac{1}{2}(\|\mathbf{u}+\mathbf{v}\|^2 - \|\mathbf{u}\|^2 - \|\mathbf{v}\|^2)\\ &= \operatorname{Re}(\mathbf{u}\cdot\mathbf{v})\end{aligned}$$

Rovnost imaginárních částí dostaneme podobně z polarizační identity ve cvičeních. □

Definice 8.48. Reálnou (resp. komplexní) čtvercovou matici splňující ekvivalentní podmínky z předchozího tvrzení nazýváme *ortogonální* (resp. *unitární*).

Standardní pojmenování ortogonální matice je poněkud matoucí, smysluplnější by bylo ortonormální. Hezkou vlastností těchto matic je snadné určení inverzní matice – stačí vzít podle bodu (4) matici hermitovsky sdruženou. Příklady ortogonálních matic jsou matice rotací a zrcadlení podle podprostorů.

Součinem unitárních matic stejných řádů je opět unitární matice. Buď můžeme ověřit algebraicky nebo nahlédnout geometricky z toho, že složením dvou zobrazení zachovávajících skalární součin (nebo jen normu) je zobrazení, které skalární součin rovněž zachovává. Detaily si promyslete jako cvičení. Rovněž jako cvičení dokažte, že jakékoliv zobrazení $f : \mathbb{C}^n \to \mathbb{C}^n$ zachovávající skalární součin je lineární.

8.6.1. *Unitární zobrazení.* Pro jednoduchost jsme se zabývali pouze standardním skalárním součinem. Obecněji se zobrazení zachovávající skalární součin nazývá *unitární*. Matice takového zobrazení vzhledem k ortonormálním bázím má ortonormální sloupce. Je-li toto zobrazení navíc izomorfismem (k tomu stačí, aby bylo na, protože prosté je vždy), pak se nazývá *izometrie* a jeho matice vzhledem k ortonormálním bázím je unitární. Tyto vlastnosti přenecháme čtenáři jako cvičení.

Cvičení

1. Jsou-li A, B matice nad tělesem $\mathbb{C}$ typu $m \times n$, C je matice typu $n \times p$ nad $\mathbb{C}$ a $a \in \mathbb{C}$, pak

(1) $(A+B)^* = A^* + B^*$,
(2) $(aA)^* = \overline{a}A^*$,
(3) $(A^*)^* = A$.
(4) $(BC)^* = C^*B^*$.

Dokažte.

2. Nechť A je čtvercová matice nad $\mathbb{C}$. Dokažte, že $\det(A^*) = (\det(A))^*$.

3. Nechť A je regulární matice nad $\mathbb{C}$. Dokažte, že $(A^*)^{-1} = (A^{-1})^*$.

4. Nechť A je čtvercová matice řádu n nad $\mathbb{C}$. Dokažte, že zobrazení $\mathbb{C}\times\mathbb{C} \to \mathbb{C}$ definované vztahem $\langle \mathbf{u}\,|\mathbf{v}\rangle = \mathbf{u}^*A\mathbf{v}$ splňuje podmínky (SL1) a (SL2).

5. Nechť A je čtvercová matice řádu n nad $\mathbb{C}$. Dokažte, že zobrazení $\mathbb{C}\times\mathbb{C} \to \mathbb{C}$ definované vztahem $\langle \mathbf{u}\,|\mathbf{v}\rangle = \mathbf{u}^*A\mathbf{v}$ splňuje podmínku (SCS) právě tehdy, když A je hermitovská (tj. $A^* = A$).

6. Nechť B je regulární matice řádu n nad $\mathbb{C}$ a $A = B^*B$. Dokažte, že zobrazení $\mathbb{C}\times\mathbb{C} \to \mathbb{C}$ definované vztahem $\langle \mathbf{u}\,|\mathbf{v}\rangle = \mathbf{u}^*A\mathbf{v}$ je skalární součin.

7. Dokažte, že v libovolném vektorovém prostoru se skalárním součinem $\langle\ |\ \rangle$ platí

- $\operatorname{Re}(\langle \mathbf{u}\,|\mathbf{v}\rangle) = \frac{1}{2}(\|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 - \|\mathbf{u}-\mathbf{v}\|^2)$
- $\operatorname{Re}(\langle \mathbf{u}\,|\mathbf{v}\rangle) = \frac{1}{4}(\|\mathbf{u}+\mathbf{v}\|^2 - \|\mathbf{u}-\mathbf{v}\|^2)$
- $\operatorname{Im}(\langle \mathbf{u}\,|\mathbf{v}\rangle) = \frac{1}{2}(\|\mathbf{u}+i\mathbf{v}\|^2 - \|\mathbf{u}\|^2 - \|\mathbf{v}^2\|^2)$
- $\operatorname{Im}(\langle \mathbf{u}\,|\mathbf{v}\rangle) = \frac{1}{2}(\|\mathbf{u}\|^2 + \|\mathbf{v}^2\|^2 - \|\mathbf{u}-i\mathbf{v}\|^2)$
- $\operatorname{Im}(\langle \mathbf{u}\,|\mathbf{v}\rangle) = \frac{1}{4}(\|\mathbf{u}+i\mathbf{v}\|^2 - \|\mathbf{u}-i\mathbf{v}\|^2)$

$\operatorname{Im}(x)$ značí imaginární část čísla $x \in \mathbb{C}$.

8. Nad reálnými čísly lze Cauchy-Schwarzovu nerovnost dokázat také následujícím způsobem: Výraz $\|\mathbf{u}+t\mathbf{v}\|^2$ definuje kvadratickou funkci. Protože musí být nezáporná, její diskriminant je nekladný a to dává C-S nerovnost. Doplňte detaily.

9. Kdy nastává v trojúhelníkové nerovnosti rovnost?

10. Dokažte, že norma pochází ze skalárního součinu právě tehdy, když splňuje rovnoběžníkové pravidlo.

11. Dokažte, že platí-li $M \perp N$, pak $M \cap N \subseteq \{\mathbf{o}\}$.

12. Dokažte pozorování 8.26.

13. Dokažte, že prostorech nad $\mathbb{R}$ se skalárním součinem platí opačná implikace v Pythagorově větě, tj. pokud $\|\mathbf{u}+\mathbf{v}\|^2 = \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2$, pak $\mathbf{u} \perp \mathbf{v}$. Platí opačná implikace v prostorech nad $\mathbb{C}$?

14. Nechť $f : \mathbf{V} \to \mathbf{W}$ je lineární zobrazení a $\mathbf{U} \leq \mathbf{V}$ je doplněk $\operatorname{Ker} f$, tj. $\operatorname{Ker} f \oplus U = V$. Dokažte, že zúžení f na $\mathbf{U}$ je izomorfismus z $\mathbf{U}$ na obraz f.

15. Dokažte, že Gramova matice vektorů $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k$ je regulární právě tehdy, když je $(\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k)$ lineárně nezávislá posloupnost.

16. Dokažte, že determinant Gramovy matice vektorů $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n \in \mathbb{R}^n$ je rovný druhé mocnině determinantu matice

$$(\mathbf{w}_1|\mathbf{w}_2|\ldots|\mathbf{w}_n) \ .$$

Interpretujte geometricky.

17. Pomocí Gram-Schmidtovi ortogonalizace dokažte body (2) a (3) věty 8.29 za předpokladu, že W je konečně generovaný (prostor V konečně generovaný být nemusí).

18. Využijte QR-rozklad na důkaz následující nerovnosti pro komplexní matici A typu $m \times n$ a standardní skalární součin:

$$\det(A^*A) \leq \|A_{*1}\|^2 \|A_{*2}\|^2 \ldots \|A_{*n}\|^2$$

Připomeňme si geometrický význam determinantu $\det(A^*A)$ a interpretujte nerovnost geoemtricky.

19. Dokažte, že součinem unitárních matic stejných řádů je unitární matice.

20. Dokažte, že každé zobrazení $f : \mathbb{C}^n \to \mathbb{C}^n$ zachovávající skalární součin je lineární.

21. Dokažte, že matice unitárního zobrazení vzhledem k ortonormálním bázím má ortonormální sloupce.

22. Dokažte, že unitární zobrazení je vždy prosté.

Obsah