LINEÁRNÍ ALGEBRA

LIBOR BARTO A JIŘÍ TŮMA

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

Toto jsou průběžně vznikající zápisky z přednášek Lineární algebra a geometrie 1 a Lineární algebra a geometrie 2. Pokud naleznete jakoukoliv chybu, dejte nám určitě vědět!

---

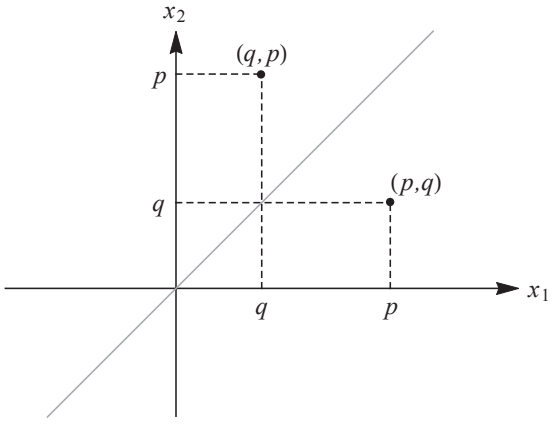
1. Opakování

Cíl. *Zopakujeme si základy analytické geometrie v rovině a prostoru a počítání s komplexními čísly.*

V úvodní kapitole si zopakujeme některé poznatky, se kterými se většina z vás seznámila už na střední škole.

Připomeneme si základy analytické geometrie, zejména rovnici přímky v rovině a roviny v prostoru a jejich parametrická vyjádření. V druhé části zopakujeme počítání s komplexními čísly. Ukážeme jejich geometrický význam a podrobněji se budeme věnovat řešení binomických rovnic.

1.1. **Analytická geometrie v rovině a prostoru.**

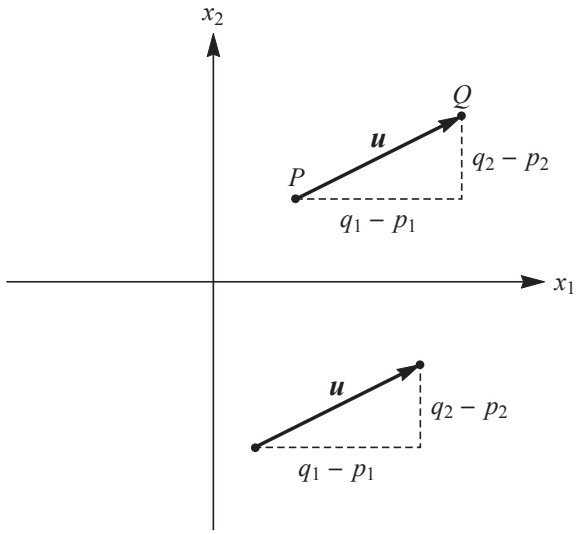


Obrázek 1. Souřadnice bodu v rovině

Date: 13. ledna 2015.

1.1.1. *Souřadnice v rovině.* Pokud zvolíme v rovině nějaký souřadný systém, můžeme každý bod zapsat pomocí jeho souřadnic jako uspořádanou dvojici reálných čísel (p, q). A naopak, každé uspořádané dvojici reálných čísel odpovídá právě jeden bod v rovině. Na přídavné jméno *uspořádaná* nesmíme zapomínat, protože v uspořádané dvojici čísel záleží na jejich pořadí. Je-li $p \neq q$, jsou dvojice (p, q) a (q, p) různé. Dvojicím (p, q) a (q, p) také odpovídají různé body v rovině. Jsou symetrické vzhledem k ose prvního a třetího kvadrantu.

Je-li $\mathbf{u}$ vektor v rovině s počátečním bodem $P = (p_1, p_2)$ a koncovým bodem $Q = (q_1, q_2)$, pak za jeho souřadnice považujeme uspořádanou dvojici $(q_1 - p_1, q_2 - p_2)$ reálných čísel. Souřadnice vektoru $\mathbf{u}$ nezávisí na volbě počátečního bodu.



Obrázek 2. Souřadnice vektoru v rovině

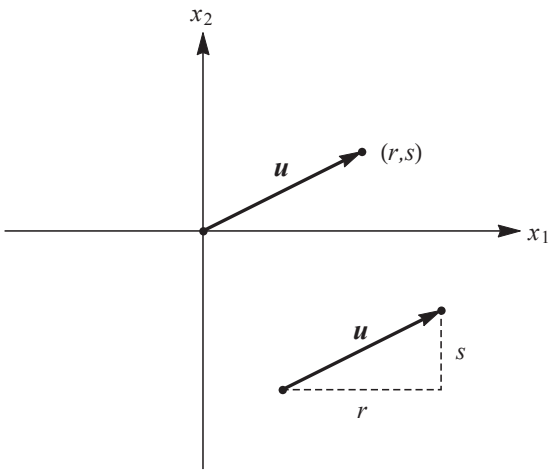
Naopak, každá uspořádaná dvojice (r, s) reálných čísel určuje vektor $\mathbf{u}$ v rovině. Počáteční bod $P = (p, q)$ můžeme zvolit libovolně, koncový bod Q má pak souřadnice $(p + r, q + s)$. Pokud za počáteční bod zvolíme počátek souřadnic $(0, 0)$, pak mluvíme o *polohovém vektoru* bodu (r, s).

Každé uspořádané dvojici reálných čísel (r, s) tak odpovídá buď nějaký bod $R = (r, s)$ nebo nějaký vektor $\mathbf{u} = (r, s)$ v rovině.

Připomeňme ještě, že body v rovině můžeme zapsat pomocí souřadnic až poté, co jsme si zvolili nějaký souřadný systém. Jeden a ten samý bod může mít v různých souřadných systémech různé souřadnice. Totéž platí pro vektory. S jedinou výjimkou, a tou je *nulový vektor*, který má stejný počáteční a koncový bod. Ten má v jakémkoliv souřadném systému souřadnice $(0, 0)$.

1.1.2. *Rovnice přímky a parametrické vyjádření přímky v rovině.* Každé řešení jedné lineární rovnice o dvou neznámých

$$a_1x_1 + a_2x_2 = b$$

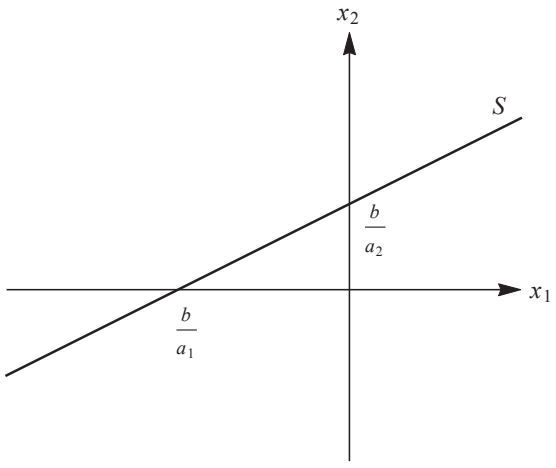


OBRÁZEK 3. Polohový vektor bodu

je uspořádaná dvojice reálných čísel (x_1, x_2). Množina S všech řešení takové rovnice je nějaká množina uspořádaných dvojic reálných čísel:

$$S = \{(x_1, x_2) \in \mathbb{R}^2 : a_1x_1 + a_2x_2 = b\} \ .$$

Tyto dvojice můžeme považovat za souřadnice bodů v rovině. Množina všech řešení rovnice pak geometricky odpovídá přímce v rovině (pokud je aspoň jeden z koeficientů a_1, a_2 nenulový).



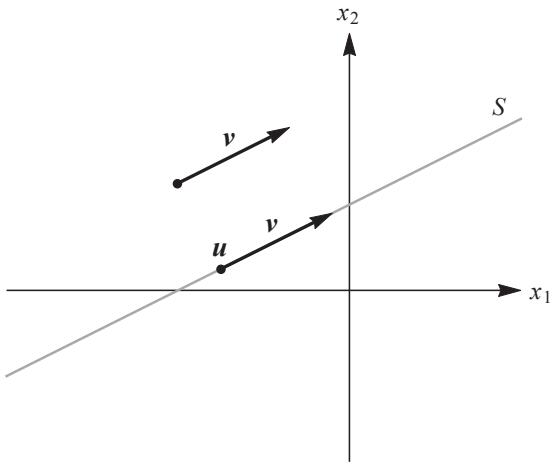
OBRÁZEK 4. Rovnice přímky

Je-li $a_1 = 0$, je přímka rovnoběžná s první souřadnou osou, je-li $a_2 = 0$, je rovnoběžná s druhou souřadnou osou.

Přímku v rovině můžeme také zapsat parametricky pomocí dvou vektorů $\mathbf{u}$ a $\mathbf{v} \neq (0,0)$ jako množinu

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

vektory sčítáme a násobíme reálným číslem po složkách. Vektor $\mathbf{v}$ nazýváme *směrový vektor přímky.*



Obrázek 5. Parametrické vyjádření přímky

Příklad 1.1. Najdeme rovnici a parametrické vyjádření přímky S, která prochází body $P = (2,3)$ a $Q = (-1,1)$.

Snazší je vyjádřit přímku v parametrickém tvaru. Za vektor $\mathbf{u}$ zvolíme polohový vektor $(2,3)$ bodu P. Vektorem $\mathbf{v}$ bude vektor s počátečním bodem P a koncovým bodem Q, tj. $\mathbf{v} = (-1,1) - (2,3) = (-3,-2)$. Parametrické vyjádření přímky S je

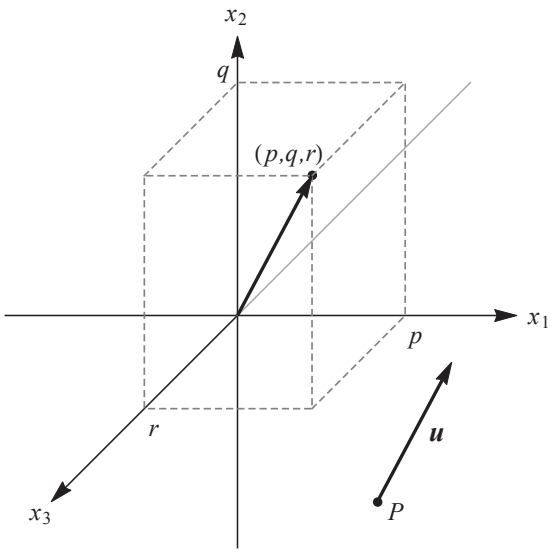
$$\{\mathbf{u} + t\mathbf{v} : t \in \mathbb{R}\} = \{(2,3) + t(-3,-2) : t \in \mathbb{R}\} \ .$$

K nalezení rovnice přímky najdeme průsečíky přímky S se souřadnými osami. Vyjdeme z parametrického vyjádření. Volbou $t = 2/3$ dostáváme bod $(0, 5/3)$ přímky S na druhé souřadné ose, a volbou $t = 3/2$ najdeme průsečík $(-5/2, 0)$ přímky S s první souřadnou osou. Z obrázku 4 pak nahlédneme, že musí platit

$$\frac{-5}{2} = \frac{b}{a_1} \qquad \text{a} \qquad \frac{5}{3} = \frac{b}{a_2} \ .$$

Stačí tedy zvolit např. $b = 5$, $a_1 = -2$ a $a_2 = 3$. Jedna z možných rovnic přímky S je tedy $-2x_1 + 3x_2 = 5$.

Otázky 1.2. K rovnici přímky $-2x_1 + 3x_2 = 5$ najděte rovnici nějaké rovnoběžné přímky. Které další rovnice popisují stejnou přímku jako rovnice $-2x_1 + 3x_2 = 5$? Kdy dvě rovnice určují různoběžné přímky?



Obrázek 6. Souřadnice bodu a vektoru v prostoru

1.1.3. *Souřadnice v prostoru.* Podobně volba souřadného systému v prostoru umožňuje zapsat každý bod prostoru jako uspořádanou trojici (p, q, r) reálných čísel.

Na obrázku 6 je také znázorněn polohový vektor bodu (p, q, r) a vektor s počátečním bodem P a souřadnicemi (p, q, r). Jakékoliv uspořádané trojici reálných čísel odpovídá jednoznačně určený bod v prostoru a také jednoznačně určený vektor v prostoru.

Stejně jako v rovině také souřadnice bodů v prostoru závisí na volbě souřadného systému. Rovněž na něm závisí souřadnice jakéhokoliv nenulového vektoru. Nulový vektor má v každém souřadném systému souřadnice $(0, 0, 0)$.

1.1.4. *Rovnice roviny a parametrické vyjádření roviny v prostoru.* Každé řešení jedné lineární rovnice o třech neznámých

$$a_1x_1 + a_2x_2 + a_3x_3 = b$$

je uspořádaná trojice (x_1, x_2, x_3) reálných čísel, která odpovídá nějakému bodu v prostoru. Množina všech řešení

$$S = \{(x_1, x_2, x_3) \in \mathbb{R}^3 : a_1x_1 + a_2x_2 + a_3x_3 = b\}$$

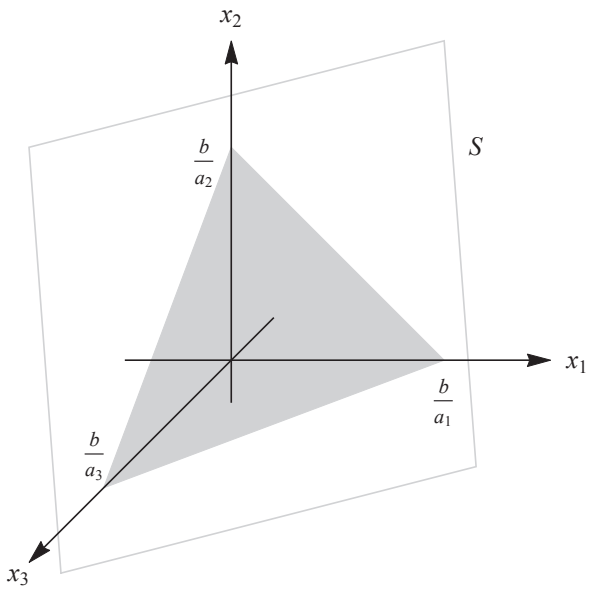
pak odpovídá nějaké rovině v prostoru, pokud je aspoň jeden z koeficientů a_1, a_2, a_3 nenulový. Rovina je rovnoběžná s první souřadnou osou právě když je $a_1 = 0$, podobně s dalšími osami. V případě $a_1 = a_2 = 0$ jde tedy o rovinu rovnoběžnou s rovinou určenou prvními dvěma souřadnými osami x_1, x_2.

Také rovinu v prostoru můžeme vyjádřit v parametrickém tvaru

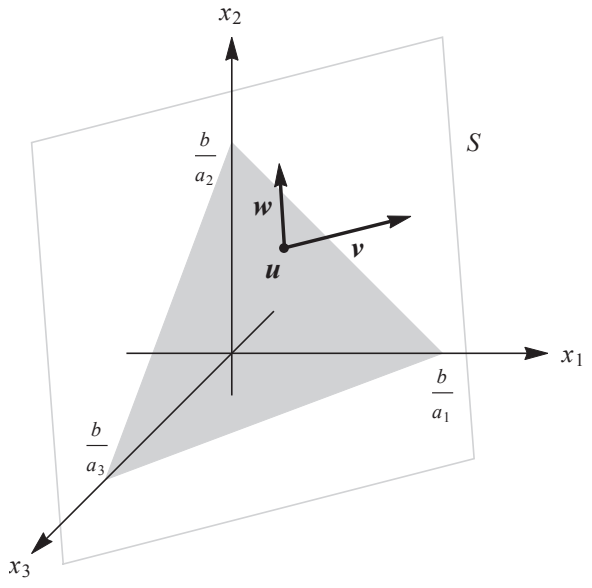
$$S = \{\mathbf{u} + s\mathbf{v} + t\mathbf{w} : s, t \in \mathbb{R}\} \ ,$$

kde $\mathbf{u}$ je polohový vektor nějakého bodu roviny a $\mathbf{v}, \mathbf{w}$ jsou další vhodné vektory.

Příklad 1.3. Najdeme parametrické vyjádření roviny určené body $P = (0, 2, 1)$, $Q = (1, 2, 3)$, $R = (2, 1, 0)$. Za vektor $\mathbf{u}$ zvolíme polohový vektor bodu P, tj. $\mathbf{u} =$



Obrázek 7. Rovnice roviny v prostoru



Obrázek 8. Parametrické vyjádření roviny v prostoru

$(0, 2, 1)$. Za vektor $\mathbf{v}$ můžeme zvolit například vektor s počátečním bodem P a koncovým bodem Q, tj. $\mathbf{v} = (1, 2, 3) - (0, 2, 1) = (1, 0, 2)$. A nakonec za vektor $\mathbf{w}$ zvolíme vektor s počátečním bodem P a koncovým bodem R, tj. $\mathbf{w} = (2, 1, 0) -$

$(0,2,1) = (2,-1,-1)$. Parametrické vyjádření roviny je tedy

$$\{(0,2,1) + s(1,0,2) + t(2,-1,-1) : s,t \in \mathbb{R}\} \ .$$

Rovnici této roviny můžeme z jejího parametrického vyjádření najít podobně, jako jsme hledali rovnici přímky v rovině z jejího parametrického tvaru. Najdeme hodnoty parametrů s,t, které určují bod roviny na první souřadné ose. Takový bod musí mít druhou a třetí souřadnici rovnou 0. Tato podmínka vede na soustavu dvou lineárních rovnic o dvou neznámých:

$$\begin{aligned} 2 + 0s - 1t &= 0 \\ 1 + 2s - t &= 0 \ , \end{aligned}$$

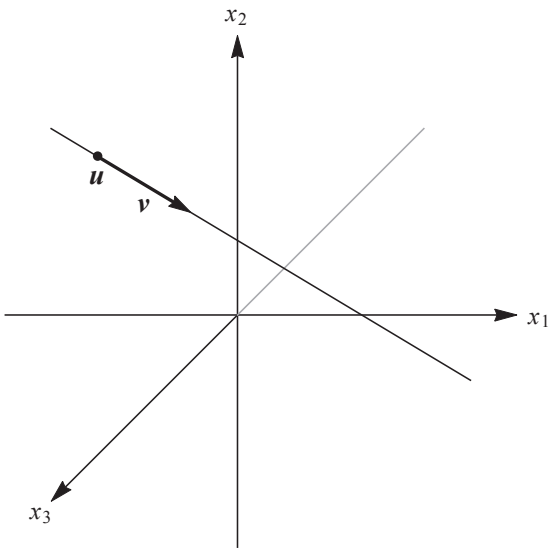
která má řešení $t = 2$ a $s = 1/2$, na první souřadné ose leží bod $(0 + 1s + 2t, 0, 0) = (5/2, 0, 0)$. Podobně najdeme průsečíky parametricky zadané roviny s dalším souřadnými osami. Ze souřadnic těchto průsečíků potom odvodíme koeficienty a_1, a_2, a_3 a b pomocí obrázku 7. Brzy se naučíme mnohem rychlejší postup a proto ten právě naznačený už nebudeme dělat podrobně až do konce.

Otázky 1.4. Jak poznáme, že dvě lineární rovnice o třech neznámých určují rovnoběžné roviny? Kdy určují různoběžné roviny? Jak by řešení předchozího příkladu probíhalo, kdyby body P, Q, R ležely na jedné přímce?

1.1.5. *Soustava rovnic přímky a parametrické vyjádření přímky v prostoru.* Jednodušší je najít v tomto případě parametrické vyjádření. To je

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

kde $\mathbf{u}, \mathbf{v}$ jsou vhodné vektory v prostoru.



Obrázek 9. Parametrické vyjádření přímky v prostoru

Máme-li parametricky vyjádřit přímku procházející body $P = (-2,3,1)$ a $Q = (1,0,5)$, zvolíme $\mathbf{u} = (-2,3,1)$, tj. polohový vektor bodu P, a za $\mathbf{v}$ například

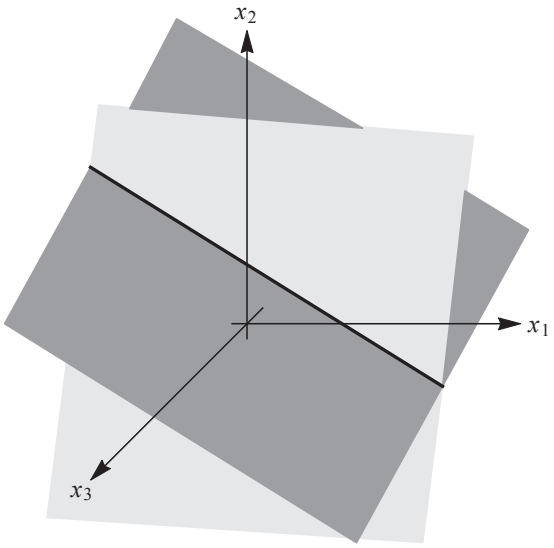
vektor s počátečním bodem P a koncovým bodem Q, tj. $\mathbf{v} = (1,0,5) - (-2,3,1) = (3,-3,4)$. Parametrické vyjádření je tedy

$$\{(-2,3,1) + t(3,-3,4) : t \in \mathbb{R}\} \ .$$

Neexistuje jedna lineární rovnice o třech neznámých, jejíž množina řešení by odpovídala přímce v prostoru. Každou přímku v prostoru ale můžeme vyjádřit jako množinu všech řešení soustavy dvou lineárních rovnic o třech neznámých:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 &= b_1 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 &= b_2 \ . \end{aligned}$$

Každá přímka je totiž průnikem dvou rovin a každou z těchto dvou rovin můžeme popsat jednou lineární rovnicí o třech neznámých Průnik těchto dvou rovin odpovídá množině všech společných řešení obou rovnic.



Obrázek 10. Průnik dvou rovin v prostoru

Musíme dát jenom pozor, aby každá z rovnic určovala rovinu, tj. aspoň jeden z koeficientů a_{11}, a_{12}, a_{13} byl nenulový, a stejně tak mezi koefienty a_{21}, a_{22}, a_{32} musí být aspoň jeden různý od nuly. A ještě musí být obě roviny různoběžné, což zajistíme požadavkem, že žádný z vektorů (a_{11}, a_{12}, a_{13}) a (a_{21}, a_{22}, a_{23}) není násobkem druhého.

Nyní můžeme geometricky nahlédnout, jak může vypadat množina všech řešení jakékoliv soustavy lineárních rovnic o třech neznámých. Protože je to průnik nějakých rovin, může to být buď rovina, nebo přímka, nebo bod, a nebo prázdná množina (to v případě, že je soustava neřešitelná). A nakonec musíme ještě přidat celý prostor, což nastane pokud je každá rovnice v soustavě tvaru $0x_1 + 0x_2 + 0x_3 = 0$, kterou splňuje jakákoliv trojice (x_1, x_2, x_3).

Podobně nahlédneme, že množina všech řešení jakékoliv soustavy lineárních rovnic o dvou neznámých je buď přímka, nebo bod, nebo prázdná množina, a nebo celá rovina.

1.2. **Komplexní čísla.**

1.2.1. *Počítání s komplexními čísly.* Komplexní číslo je číslo tvaru

$$a + ib \ ,$$

kde

- a, b jsou reálná čísla ,
- i je *imaginární jednotka*, pro kterou platí $i^2 = -1$.

Je-li $z = a + ib$ komplexní číslo, pak

- číslo a nazýváme *reálná část* čísla z a označujeme je $\operatorname{Re} z$,
- číslo b nazýváme *imaginární část* čísla z a označujeme je $\operatorname{Im} z$.

Každé komplexní číslo z tak můžeme zapsat jako $z = \operatorname{Re} z + i \operatorname{Im} z$. Dvě komplexní čísla $z = a + ib$ a $w = c + id$ se rovnají právě když se současně rovnají jejich reálné části a imaginární části, tj. právě když platí $a = c$ a $b = d$.

S komplexními čísly počítáme stejně jako s algebraickými výrazy. Sčítáme

$$(a + ib) + (c + id) = (a + c) + i(b + d) \ ,$$

a násobíme

$$(a + ib)(c + id) = (ac + i^2 bd) + iad + ibc = (ac - bd) + i(ad + bc) \ .$$

Díky předpokladu $i^2 = -1$ je součin komplexních čísel opět komplexní číslo.

Stejně snadné je odčítání,

$$(a + ib) - (c + id) = (a - c) + i(b - d) \ ,$$

zatímco při dělení komplexních čísel musíme více počítat:

$$\frac{a + ib}{c + id} = \frac{a + ib}{c + id} \cdot \frac{c - id}{c - id} = \frac{(ac + bd) + i(bc - ad)}{c^2 + d^2 + (-cd + cd)} = \frac{ac + bd}{c^2 + d^2} + i\,\frac{bc - ad}{c^2 + d^2} \ .$$

Poslední tři zlomky ve výpočtu mají smysl právě když $c^2 + d^2 > 0$, což je právě když aspoň jedno z reálných čísel c, d je různé od 0, a to nastává právě když je komplexní číslo $c + id$ nenulové.

1.2.2. *Čísla komplexně sdružená.* Při úpravě zlomku z komplexních čísel do algebraického tvaru jsme zlomek rozšířili číslem $c - id$. Při počítání s komplexními čísly má změna znaménka imaginární složky důležité místo.

Definice 1.5. Je-li $z = c + id$ komplexní číslo, pak číslo $c - id$ nazýváme *číslo komplexně sdružené k číslu* z a označujeme jej $\overline{z}$.

Číslo komplexně sdružené k $\overline{z} = c - id$ je tedy $c + id = z$, proto pro každé komplexní číslo z platí první z následujícího seznamu jednoduchých vlastností komplexního sdružování.

- $\overline{\overline{z}} = z$,
- $z = \overline{z}$ právě když je z reálné číslo ,
- $z + \overline{z} = 2c = 2 \operatorname{Re} z$,
- $z - \overline{z} = i\,2d = i\,2 \operatorname{Im} z$,
- $z\,\overline{z} = c^2 + d^2$.

Také ostatní vlastnosti snadno odovodíme z definice komplexně sdruženého čísla k číslu z a můžete si je dokázat sami. Zde si výpočtem ověříme pouze tu poslední:

$$z\,\overline{z} = (c+id)(c-id) = c^2 - i^2d^2 + i(dc-cd) = c^2+d^2 \ .$$

Komplexní sdružování také „zachovává“ algebraické operace s komplexními čísly. Je-li $w = a+ib$ další komplexní číslo, pak platí

- $\overline{w+z} = \overline{w} + \overline{z}$,
- $\overline{w\,z} = \overline{w}\,\overline{z}$.

První vlastnost říká, že číslo komplexně sdružené k součtu dvou komplexních čísel dostaneme také tak, že vezmeme čísla komplexně sdružená k oběma sčítancům a ta pak sečteme. Druhá vlastnost říká totéž pro součin. Druhou vlastnost si ověříme výpočtem:

$$\begin{aligned} \overline{wz} &= \overline{(a+ib)(c+id)} = \overline{(ac-bd)+i(ad+bc)} = (ac-bd)-i(ad+bc) \ , \\ \overline{w}\,\overline{z} &= (a-ib)(c-id) = (ac-bd)-i(ad+bc) \ . \end{aligned}$$

Obě čísla $\overline{wz}$ a $\overline{w}\,\overline{z}$ mají stejné reálné a imaginární části a proto se rovnají.

1.2.3. *Základní číselné obory.* Každé reálné číslo a je současně komplexním číslem $a+i0$. Množina všech reálných čísel, budeme ji označovat $\mathbb{R}$, je tak podmnožinou množiny všech komplexních čísel, kterou budeme označovat $\mathbb{C}$. Komplexní čísla jsou největším z číselných oborů, se kterými jste se dosud učili počítat. Od přirozených čísel, která značíme $\mathbb{N}$ (natural numbers), přes celá čísla $\mathbb{Z}$ (Zahlen), racionální čísla $\mathbb{Q}$ (quotients), reálná čísla $\mathbb{R}$ (reals) až po komplexní čísla $\mathbb{C}$ (complex numbers):

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \ .$$

1.2.4. *Základní věta algebry.* Jednou z příčin postupného rozšiřování číselných oborů byla potřeba řešit rovnice. V každém oboru obsaženém v množině reálných čísel $\mathbb{R}$ lze formulovat rovnici, která v tomto oboru nemá žádné řešení. Rovnice $x+2=1$ má pouze přirozené koeficienty, ale žádné přirozené číslo ji neřeší. Podobně rovnice $2x=1$ nemá žádné celočíselné řešení, rovnici $x^2=2$ neřeší žádné racionální číslo, a rovnice $x^2=-1$ nemá žádný reálný kořen. Obor komplexních čísel už kvůli řešení polynomiálních rovnic není nutné dále rozšiřovat, neboť platí následující *základní věta algebry.*

Věta 1.6. *Každý nekonstantní polynom s komplexními koeficienty má aspoň jeden komplexní kořen.*

Základní větu algebry lze formulovat také následujícím způsobem.

Věta 1.7. *Pro každý polynom* $p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ *stupně* $n \geq 1$ *s komplexními koeficienty* $a_n, a_{n-1}, \ldots, a_1, a_0$ *existují komplexní čísla* $z_1, z_2, \ldots, z_n$ *(nemusí být navzájem různá), pro která platí*

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = a_n(x-z_1)(x-z_2)\cdots(x-z_n) \ .$$

Tuto formulaci můžeme také stručně vyjádřit slovy *každý nekonstantní polynom s komplexními koeficienty se rozkládá na součin lineárních činitelů.* Každé z komplexních čísel $z_1, z_2, \ldots, z_n$ je kořenem polynomu $p(x)$ a tedy řešením polynomiální rovnice $a_nx^n + \cdots + a_1x + a_0 = 0$. Z porovnání stupňů polynomů na obou stranách poslední rovnosti dostaneme ihned následující důsledek.

Důsledek 1.8. *Každý polynom stupně* n *s komplexními koeficienty má nejvýše* n *navzájem různých komplexních kořenů.*

Polynom s reálnými koeficienty nemusí mít žádný reálný kořen, známým příkladem je polynom $x^2 + 1$. Podle základní věty algebry má ale nějaké komplexní kořeny. Pro komplexní kořeny polynomů s reálnými koeficienty platí následující tvrzení. Říká, že komplexní kořeny polynomů s reálnými koeficienty se sdružují do párů.

Věta 1.9. *Je-li $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ polynom s reálnými koeficienty, pak je číslo $z \in \mathbb{C}$ kořen polynomu $p(x)$ právě když je $\overline{z}$ (číslo komplexně sdružené k z) také kořen polynomu $p(x)$.*

Důkaz. Narozdíl od základní věty algebry má věta o komplexním sdružování kořenů jednoduchý důkaz, a proto si jej uvedeme.

Každý koeficent a_i polynomu $p(x)$ je reálné číslo, platí proto $\overline{a_i} = a_i$. Stejně tak platí $\overline{0} = 0$. Protože předpokládáme, že z je kořen polynomu $p(x)$, platí $p(z) = 0$, a tedy také $\overline{p(z)} = \overline{0} = 0$. V následujícím výpočtu použijeme, že komplexní sdružování zachovává sčítání a násobení komplexních čísel. Platí

$$\begin{aligned} 0 = \overline{p(z)} &= \overline{a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0} \\ &= \overline{a_n\, z^n} + \overline{a_{n-1}\, z^{n-1}} + \cdots + \overline{a_1\, z} + \overline{a_0} \\ &= \overline{a_n}\, \overline{z}^n + \overline{a_{n-1}}\, \overline{z}^{n-1} + \cdots + \overline{a_1}\, \overline{z} + \overline{a_0} \\ &= a_n \overline{z}^n + a_{n-1}\overline{z}^{n-1} + \cdots + a_1 \overline{z} + a_0 = p(\overline{z}) \ , \end{aligned}$$

což dokazuje, že $\overline{z}$ je kořen polynomu $p(x)$.

Je-li naopak $\overline{z}$ kořen polynomu $p(x)$, pak jsme právě dokázali, že také $\overline{\overline{z}} = z$ je kořen polynomu $p(x)$. □

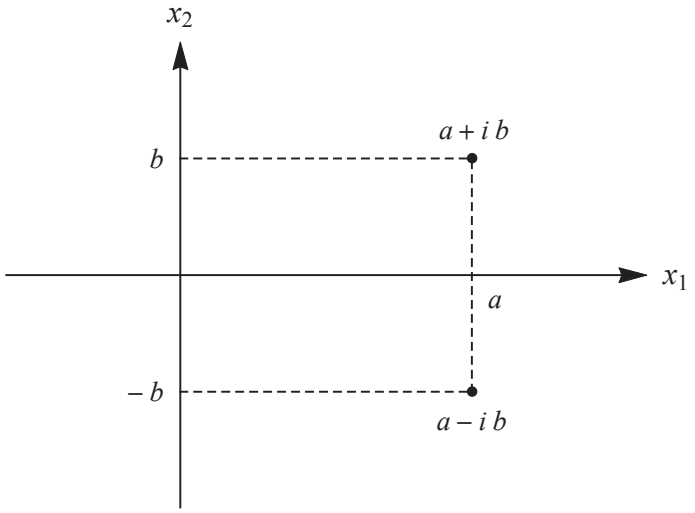
1.2.5. *Komplexní rovina.* Reálná čísla znázorňujeme na reálné ose. Komplexní číslo $z = a + ib$ můžeme znázornit jako bod (a, b) v rovině s kartézskými souřadnicemi. V takovém případě mluvíme o *komplexní rovině*. Také se můžete setkat s názvem *Gaussova rovina* a v anglicky psaných učebnicích s názvem *Argand plane*, případně *Argand diagram*.

Na obrázku je kromě čísla $z = a + ib$ znázorněné také číslo komplexně sdružené k z, tj. číslo $\overline{z} = a - ib$. Geometricky je komplexně sdružené číslo $\overline{z}$ symetrické s číslem z vzhledem k reálné ose.

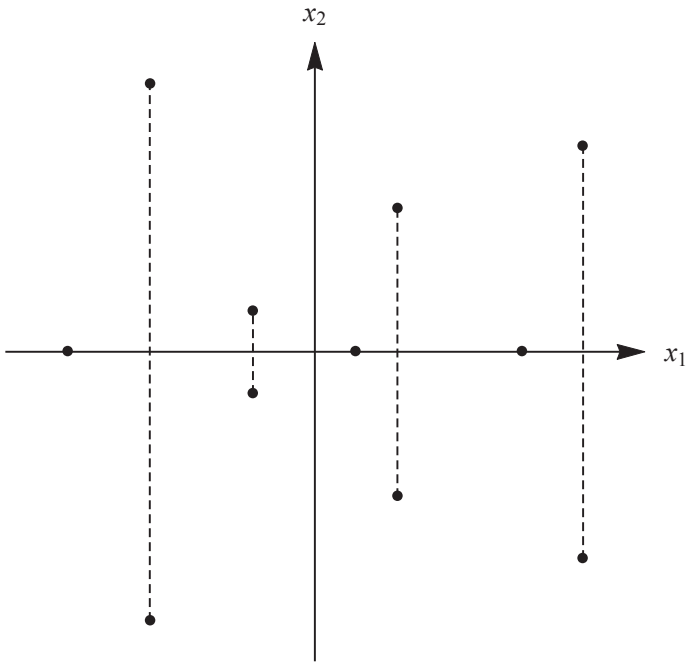
Obrázek 12 ukazuje geometrický význam věty 1.9 o komplexním sdružování kořenů polynomů s reálnými koeficienty – množina všech kořenů je symetrická vzhledem k reálné ose.

Dále si na obrázku 13 ukážeme geometrický význam sčítání komplexních čísel. Jsou-li $z = a + ib$ a $w = c + id$ komplexní čísla, pak součet $z + w = (a + c) + i(b + d)$ odpovídá bodu se souřadnicemi $(a + c, b + d)$ a ten dostaneme jako koncový bod součtu polohového vektoru bodu (a, b) odpovídajícího z a polohového vektoru bodu (c, d) odpovídajícího w.

1.2.6. *Polární souřadnice v rovině.* Geometrický význam násobení je o něco složitější. Pro jeho pochopení je vhodnější použít k zápisu bodů v rovině *polární souřadnice*. V rovině s kartézskými souřadnicemi můžeme každý bod $P = (a, b)$ různý od počátku souřadnic jednoznačně určit pomocí vzdálenosti $r > 0$ bodu P od počátku a orientovaného úhlu α, který dostaneme tak, že kladnou x_1-ovou poloosu otáčíme kolem počátku souřadnic proti směru hodinových ručiček až do polopřímky s počátkem v bodě $(0, 0)$ a procházející bodem P. Dvojici čísel (r, α) nazýváme *polární*

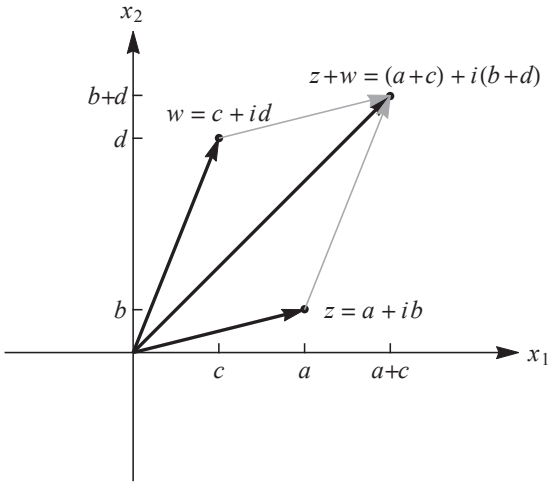


Obrázek 11. Geometrické znázornění komplexního čísla v rovině



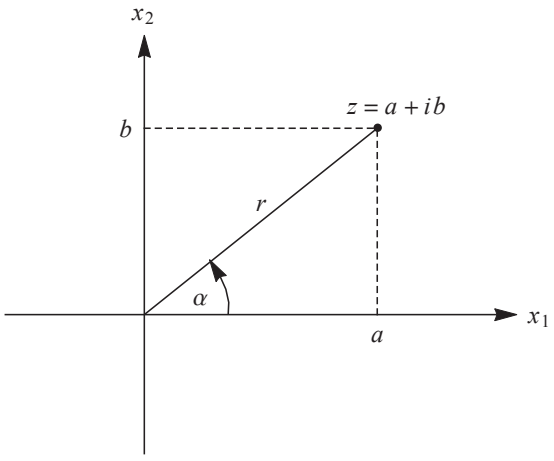
Obrázek 12. Komplexní kořeny polynomu s reálnými koeficienty

souřadnice bodu P, viz. obrázek 14. Protože otočením o plný úhel 2π neboli 360 stupňů dostaneme zpět kladnou poloosu x_1, není úhel α určený jednoznačně. Různé



OBRÁZEK 13. Součet komplexních čísel

možné hodnoty α se liší o nějaký celočíselný násobek 2π. V případě, že $P = (0, 0)$ je počátek souřadnic, je $r = 0$ a úhel α není definován.



OBRÁZEK 14. Polární souřadnice bodu v rovině

Z polárních souřadnic (r, α) bodu $P \neq (0, 0)$ vypočteme jeho kartézské souřadnice (a, b) jako

$$a = r\cos\alpha, \quad b = r\sin\alpha \ .$$

Naopak z kartézských souřadnic (a, b) bodu $P \neq (0, 0)$ dostaneme jeho polární souřadnice pomocí vztahů

$$r = \sqrt{a^2 + b^2}, \quad \cos\alpha = \frac{a}{\sqrt{a^2 + b^2}}, \quad \sin\alpha = \frac{b}{\sqrt{a^2 + b^2}} \ .$$

Protože funkce sinus a kosinus mají periodu 2π, plyne odtud znovu, že úhel α je určený jednoznačně až na celočíselný násobek 2π.

1.2.7. *Goniometrický tvar komplexního čísla.* Bod P odpovídá komplexnímu číslu $z = a + ib$. Vyjádříme-li jeho kartézské souřadnice (a, b) pomocí polárních, dostaneme

$$z = a + ib = r\cos\alpha + i\, r\sin\alpha = r(\cos\alpha + i\sin\alpha) \ .$$

Vyjádření $z = r(\cos\alpha + i\sin\alpha)$ nazýváme *goniometrický tvar* komplexního čísla $z \neq 0$.

- číslo r nazýváme *absolutní hodnota* čísla z a označujeme jej $|z|$,
- úhel α nazýváme *argument* komplexního čísla z a označujeme jej $\arg z$.

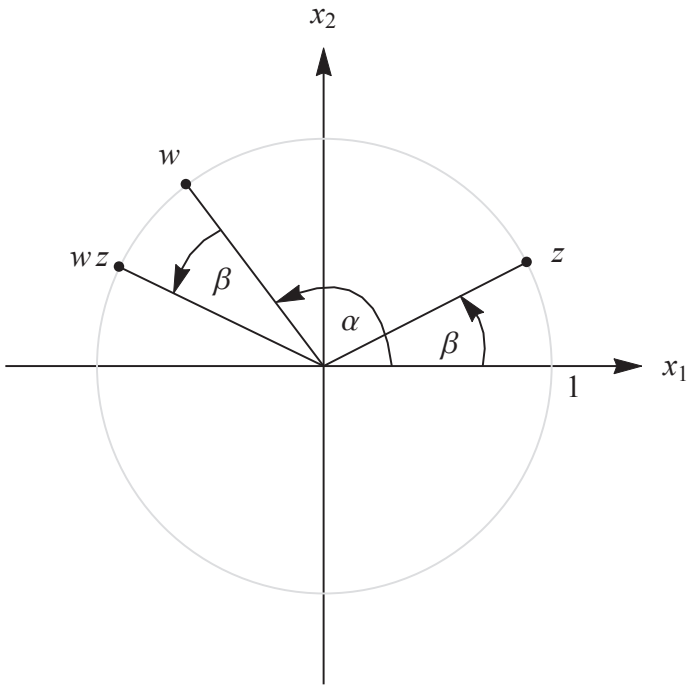
Platí tedy

$$|z| = \sqrt{a^2 + b^2}, \quad \cos(\arg z) = \frac{a}{\sqrt{a^2 + b^2}}, \quad \sin(\arg z) = \frac{b}{\sqrt{a^2 + b^2}} \ ,$$

také $\arg z$ může nabývat různých hodnot, které se ale vždy liší o celočíselný násobek 2π. Protože platí (poslední pátá rovnost pod Definicí 1.5), že $z\,\overline{z} = a^2 + b^2$, dostáváme pro absolutní hodnotu čísla z vyjádření

- $|z|^2 = z\,\overline{z}$.

1.2.8. *Geometrický význam násobení komplexních čísel.* Body na jednotkové kružnici odpovídají komplexním číslům $\cos\alpha + i\sin\alpha$. Takovým číslům říkáme *komplexní jednotky.*



Obrázek 15. Součin komplexních jednotek

Pro součin dvou komplexních jednotek $w = \cos\alpha + i\sin\alpha$ a $z = \cos\beta + i\sin\beta$ platí

$$\begin{aligned} w\,z &= (\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) \\ &= \cos\alpha\cos\beta - \sin\alpha\sin\beta + i(\cos\alpha\sin\beta + \sin\alpha\cos\beta) \\ &= \cos(\alpha+\beta) + i\sin(\alpha+\beta)\ , \end{aligned}$$

v poslední rovnosti jsme použili vzorce pro sinus a kosinus součtu dvou úhlů.

Součin dvou komplexních jednotek je tedy opět komplexní jednotka, pro kterou platí

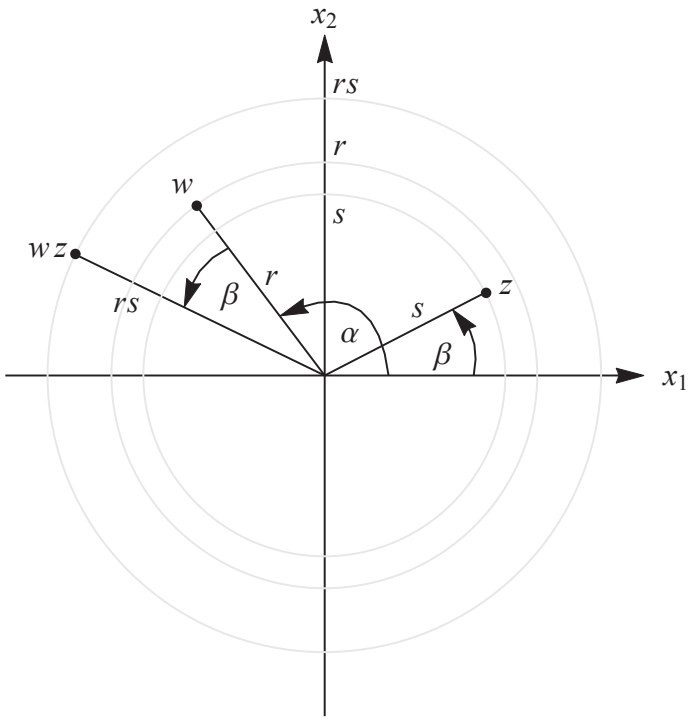
- $\arg(w\,z) = \arg w + \arg z$,

rovnost platí až na celočíselný násobek 2π.

Jednoduchou indukcí podle n pak snadno dokážeme důležitou *Moivreovu větu*:

Věta 1.10. *Pro každý úhel α a každé přirozené číslo n platí*

$$(\cos\alpha + i\sin\alpha)^n = \cos(n\alpha) + i\sin(n\alpha)\ .$$



Obrázek 16. Součin komplexních čísel

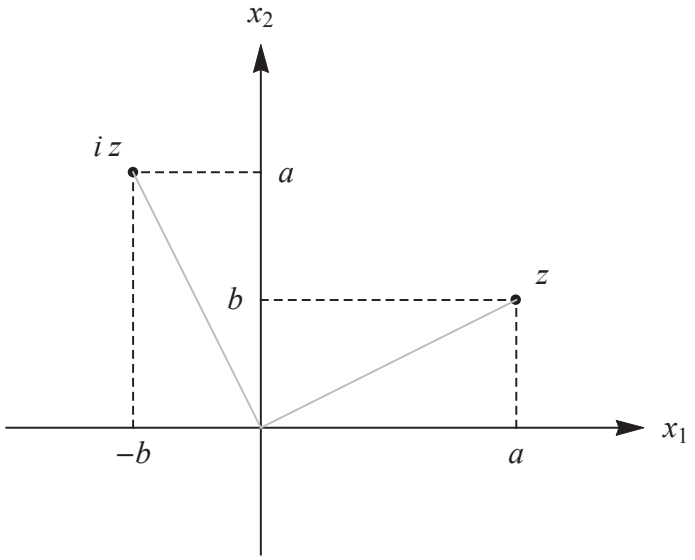
Jsou-li nyní $w = r(\cos\alpha + i\sin\alpha)$ a $z = s(\cos\beta + i\sin\beta)$ libovolná dvě nenulová komplexní čísla, pak pro jejich součin platí

$$\begin{aligned} w\,z &= r(\cos\alpha + i\sin\alpha)s(\cos\beta + i\sin\beta) \\ &= rs(\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) \\ &= rs(\cos(\alpha+\beta) + i\sin(\alpha+\beta))\ . \end{aligned}$$

Pro absolutní hodnotu a argument součinu $w\,z$ tak platí

- $|w\,z| = |w|\,|z|$,
- $\arg(wz) = \arg w + \arg z$.

V jednoduchém speciálním případě, kdy $w = i = \cos(\pi/2) + i\sin(\pi/2)$ dostáváme, že $|iw| = |i|\,|w| = |w|$ a $\arg(iz) = \arg i + \arg z = \frac{\pi}{2} + \arg z$. Vynásobit číslo z číslem i tak znamená pootočit číslo z kolem počátku souřadnic o pravý úhel proti směru hodinových ručiček. To můžeme také snadno nahlédnout z algebraického tvaru $z = a + ib$, neboť $i\,z = i(a + ib) = -b + ia$.



Obrázek 17. Součin komplexního čísla s imaginární jednotkou

Dokážeme si ještě dvěma způsoby *trojúhelníkovou nerovnost* pro komplexní čísla, která říká, že pro libovolná dvě čísla $z = a + ib$ a $w = c + id$ platí

- $|z + w| \leq |z| + |w|$.

K algebraickému důkazu trojúhelníkové nerovnosti využijeme další dvě jednoduché vlastnosti absolutní hodnoty komplexních čísel. Pro každé komplexní číslo $z = a + ib$ platí

- $|z| = |\overline{z}|$,
- $\mathrm{Re}\, z \leq |z|$.

První rovnost plyne přímo z definice absolutní hodnoty, dokážeme druhou. Je-li $z = a + ib$, pak platí

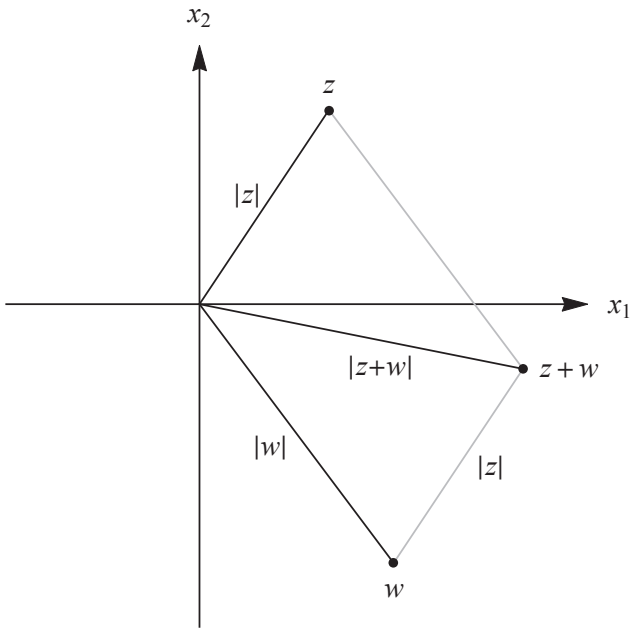
$$a \leq |a| = \sqrt{a^2} \leq \sqrt{a^2 + b^2} = |z| \ .$$

Pro každou rovnost nebo nerovnost v následujícím výpočtu (s výjimkou poslední rovnosti) si najděte v předchozím textu tu vlastnost komplexních čísel, kterou používáme.

$$\begin{aligned} |z+w|^2 &= (z+w)(\overline{z+w}) = (z+w)(\overline{z}+\overline{w}) = z\overline{z}+z\overline{w}+w\overline{z}+w\overline{w} \\ &= |z|^2 + z\overline{w} + w\overline{z} + |w|^2 = |z|^2 + z\overline{w} + \overline{z\overline{w}} + |w|^2 \\ &= |z|^2 + 2\,\mathrm{Re}\,(z\overline{w}) + |w|^2 \le |z|^2 + 2\,|z\overline{w}| + |w|^2 = |z|^2 + 2\,|z|\,|\overline{w}| + |w|^2 \\ &= |z|^2 + 2\,|z|\,|w| + |w|^2 = |z|^2 + 2\,|z|\,|w| + |w|^2 = (|z| + |w|)^2 \ . \end{aligned}$$

Dokázali jsme tak $|z+w|^2 \le (|z|+|w|)^2$ a po odmocnění dostáváme trojúhelníkovou nerovnost pro komplexní čísla.

Pomocí geometrického významu sčítání komplexních čísel trojúhelníkovou nerovnost snadno nahlédneme z obrázku.



Obrázek 18. Trojúhelníková nerovnost pro komplexní čísla

1.2.9. *Řešení binomické rovnice* $z^n = 1$. Začneme řešením rovnice $z^5 = 1$. Tuto rovnici zřejmě splňuje číslo $z_0 = 1$. Z Moivreovy věty plyne, že komplexní jednotka

$$z_1 = \cos\left(\frac{2\pi}{5}\right) + i\sin\left(\frac{2\pi}{5}\right)$$

je další kořen rovnice $z^5 = 1$, neboť $z_1^5 = \cos(2\pi) + i\sin(2\pi) = 1$.

Položíme-li $z_2 = z_1^2$, platí $z_2^5 = \left(z_1^2\right)5 = z_1^{10} = 1$ a dosttáváme tak další kořen z_2. Moivreova věta říká, že

$$z_2 = z_1^2 = \left(\cos\left(\frac{2\pi}{5}\right) + i\sin\left(\frac{2\pi}{5}\right)\right)^2 = \cos\left(\frac{2\cdot 2\pi}{5}\right) + i\sin\left(\frac{2\cdot 2\pi}{5}\right) \ .$$

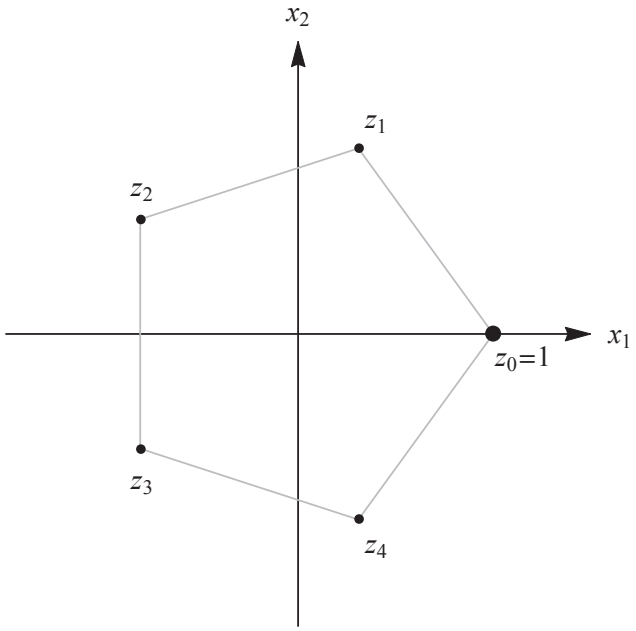
Analogicky najdeme další dva kořeny

$$\begin{aligned} z_3 &= \cos\left(\frac{3\cdot 2\pi}{5}\right) + i\sin\left(\frac{3\cdot 2\pi}{5}\right) \ , \\ z_4 &= \cos\left(\frac{4\cdot 2\pi}{5}\right) + i\sin\left(\frac{4\cdot 2\pi}{5}\right) \ . \end{aligned}$$

Našli jsme tak pět navzájem různých kořenů $z_0 = 1, z_1, \ldots, z_4$. Polynom $z^5 - 1$ má stupeň 5, podle Důsledku 1.8 rovnice $z^5 - 1 = 0$ více kořenů mít nemůže. A protože $z_0 = 1 = \cos(0\cdot 2\pi/5) + i\sin(0\cdot 2\pi/5)$, můžeme všechny kořeny zapsat jako

$$z_k = \cos\left(\frac{k\cdot 2\pi}{5}\right) + i\sin\left(\frac{k\cdot 2\pi}{5}\right), \quad \text{pro} \quad k = 0,1,2,3,4 \ .$$

Znázorníme-li je v komplexní rovině, dostaneme vrcholy pravidelného pětiúhelníku, který je vepsaný do jednotkové kružnice a jeden z vrcholů je číslo 1.



Obrázek 19. Kořeny rovnice $z^5 = 1$

Na dalším obrázku vidíme kořeny rovnic $z^3 = 1$ a $z^8 = 1$. Rovnice $z^3 = 1$ má kořeny

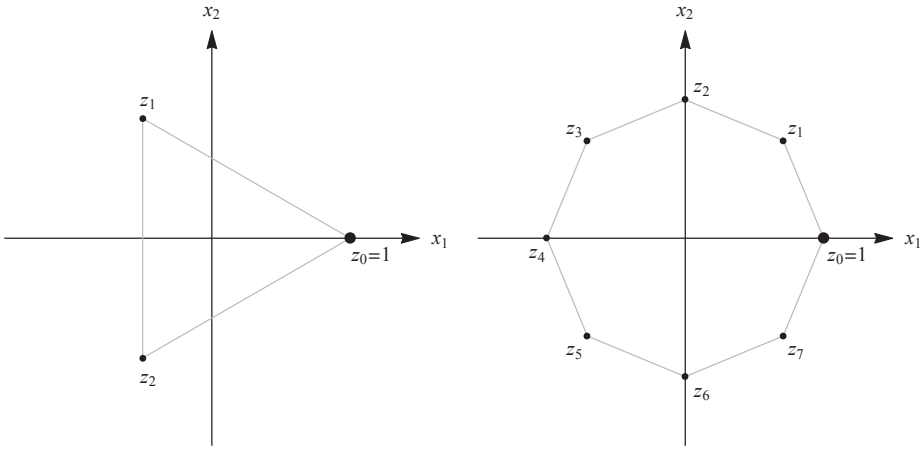
$$z_k = \cos\left(\frac{k\cdot 2\pi}{3}\right) + i\sin\left(\frac{k\cdot 2\pi}{3}\right), \quad \text{pro} \quad k = 0,1,2 \ ,$$

které tvoří vrcholy rovnostranného trojúhelníku vepsaného do jednotkové kružnice tak, aby jedním z vrcholů bylo číslo 1.

Rovnice $z^8 = 1$ má kořeny

$$z_k = \cos\left(\frac{k\cdot 2\pi}{8}\right) + i\sin\left(\frac{k\cdot 2\pi}{8}\right), \quad \text{pro} \quad k = 0,1,\ldots,7 \ ,$$

které tvoří vrcholy pravidelného osmiúhelníku vepsaného do jednotkové kružnice tak, aby jedním z vrcholů bylo číslo 1.



Obrázek 20. Kořeny rovnic $z^3 = 1$ a $z^8 = 1$

Obecně má rovnice $z^n = 1$ celkem n navzájem různých kořenů

$$z_k = \cos\left(\frac{k \cdot 2\pi}{n}\right) + i \sin\left(\frac{k \cdot 2\pi}{n}\right), \quad \text{pro} \quad k = 0, 1, \ldots, n-1 \ ,$$

které tvoří vrcholy pravidelného n-úhelníku vepsaného do jednotkové kružnice tak, aby jedním z vrcholů bylo číslo 1. Kořeny rovnice $z^n = 1$ také nazýváme *n-té odmocniny z* 1.

1.2.10. *Řešení binomické rovnice $z^n = w$ pro libovolné w.* Začneme případem $w = i = \cos(\pi/2) + i \sin(\pi/2)$. Je-li navíc $n = 2$, řešíme rovnici

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

Také v tomto případě nám Moivreova věta napoví jeden kořen

$$z_0 = \cos\left(\frac{\pi}{4}\right) + i \sin\left(\frac{\pi}{4}\right) \ .$$

Druhý kořen snadno získáme z prvního:

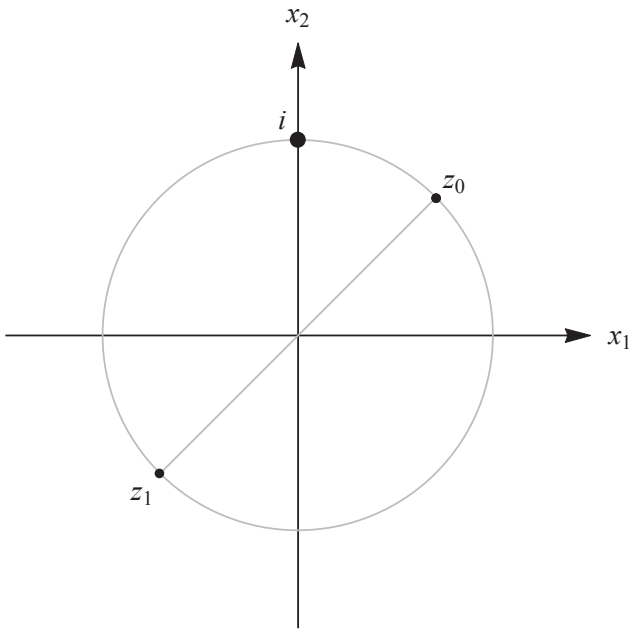
$$z_1 = -z_0 = -\cos\left(\frac{\pi}{4}\right) - i \sin\left(\frac{\pi}{4}\right) = \cos\left(\frac{\pi}{4} + \pi\right) + i \sin\left(\frac{\pi}{4} + \pi\right) \ .$$

Pokud si z_1 přepíšeme jako

$$z_1 = \cos\left(\frac{\frac{\pi}{2} + 2\pi}{2}\right) + i \sin\left(\frac{\frac{\pi}{2} + 2\pi}{2}\right) \ ,$$

můžeme oba kořeny rovnice $z^2 = \cos(\pi/2) + i \sin(\pi/2)$ vyjádřit jednou formulkou

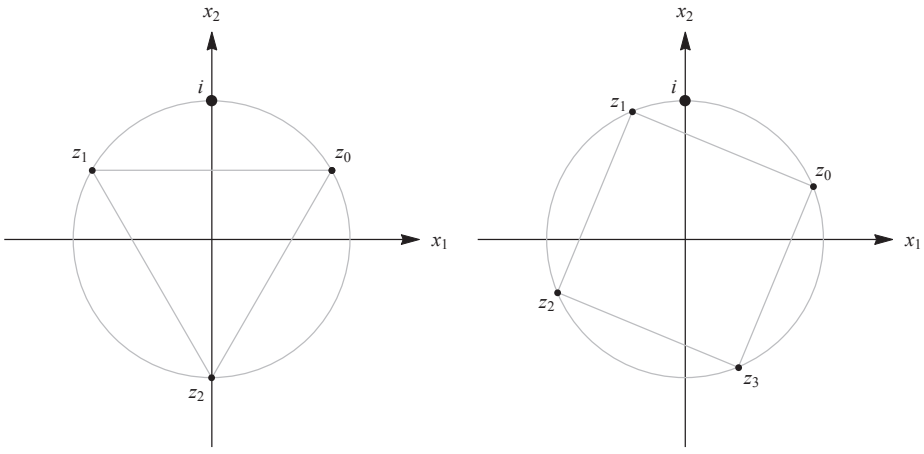
$$z_k = \cos\left(\frac{\frac{\pi}{2} + k\,2\pi}{2}\right) + i \sin\left(\frac{\frac{\pi}{2} + k\,2\pi}{2}\right) \quad \text{pro} \quad k = 0, 1 \ .$$



Obrázek 21. Kořeny rovnice $z^2 = i$

Podobně najdeme kořeny rovnic $z^3 = i$ a $z^4 = i$. V obou případech vyjdeme z toho, že pravá strana $i = \cos(\pi/2) + i\sin(\pi/2)$. Rovnice $z^3 = \cos(\pi/2) + i\sin(\pi/2)$ má kořeny

$$z_k = \cos\left(\frac{\frac{\pi}{2} + k\,2\pi}{3}\right) + i\sin\left(\frac{\frac{\pi}{2} + k\,2\pi}{3}\right) \quad \text{pro} \quad k = 0, 1, 2 \ .$$



Obrázek 22. Kořeny rovnic $z^3 = i$ a $z^4 = i$

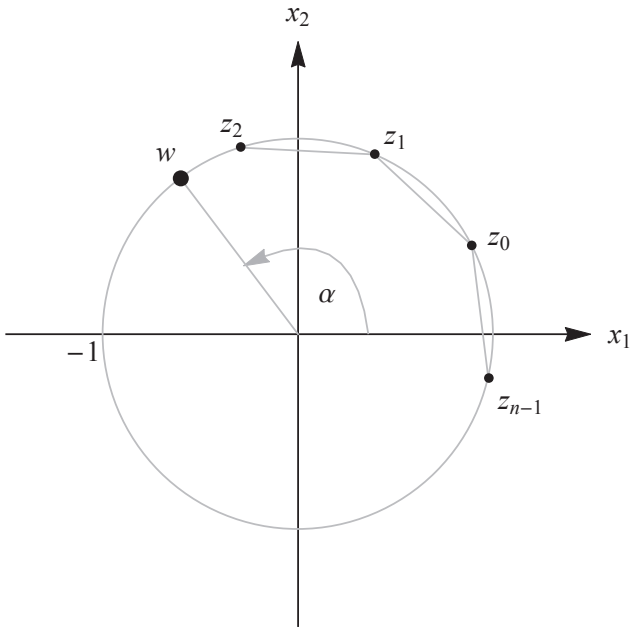
Rovnice $z^4 = \cos(\pi/2) + i\sin(\pi/2)$ má kořeny

$$z_k = \cos\left(\frac{\frac{\pi}{2} + k\,2\pi}{4}\right) + i\sin\left(\frac{\frac{\pi}{2} + k\,2\pi}{4}\right) \quad \text{pro} \quad k = 0, 1, 2, 3 \ .$$

V obou případech snadno provedeme zkoušku pomocí Moivreovy věty.

Na základě analogie můžeme nyní najít všechny kořeny rovnice $z^n = w$ pro jakoukoliv komplexní jednotku $w = \cos\alpha + i\sin\alpha$.

$$z_k = \cos\left(\frac{\alpha + k\,2\pi}{n}\right) + i\sin\left(\frac{\alpha + k\,2\pi}{n}\right) \quad \text{pro} \quad k = 0, 1, 2, \ldots, n-1 \ .$$



Obrázek 23. Kořeny rovnice $z^n = \cos\alpha + i\sin\alpha$

Pomocí Moivreovy věty ověříme, že každé číslo z_k je kořenem rovnice $z^n = \cos\alpha + i\sin\alpha$:

$$\begin{aligned} z_k^n &= \left(\cos\left(\frac{\alpha + k\,2\pi}{n}\right) + i\sin\left(\frac{\alpha + k\,2\pi}{n}\right)\right)^n \\ &= \cos\left(n\,\frac{\alpha + k\,2\pi}{n}\right) + i\sin\left(n\,\frac{\alpha + k\,2\pi}{n}\right) \\ &= \cos\left(\alpha + k\,2\pi\right) + i\sin\left(\alpha + k\,2\pi\right) \\ &= \cos\alpha + i\sin\alpha \ . \end{aligned}$$

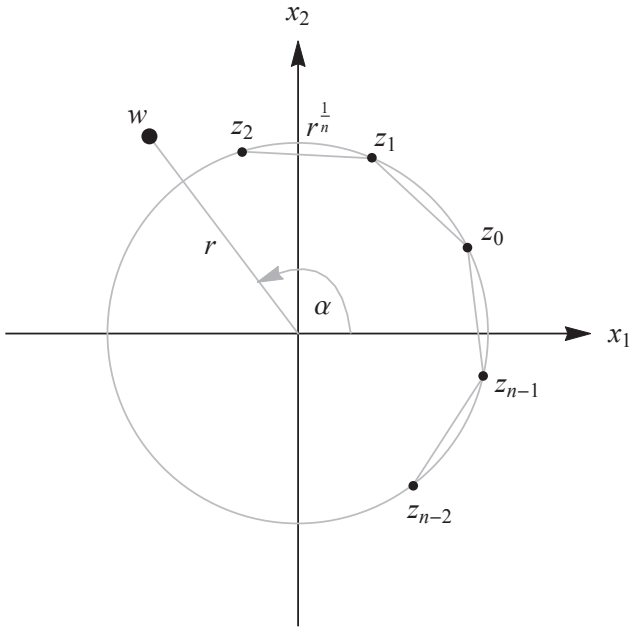
Čísla z_k jsou navíc navzájem různá pro $k = 0, 1, \ldots, n-1$, neboť se argumenty libovolných dvou z těchto čísel liší o méně než 2π.

Nakonec najdeme kořeny rovnice $z^n = w$ pro libovolnou nenulovou pravou stranu $w = r(\cos\alpha + i\sin\alpha)$. Pro každý kořen z_k rovnice $z^n = w$ musí platit

$$|z_k|^n = |z_k^n| = |w| = r \ ,$$

odkud plyne $|z_k| = \sqrt[n]{r}$. Všechny kořeny rovnice $z^n = w$ tak musí mít absolutní hodnotu rovnou $\sqrt[n]{r}$. Stejně jako v předchozím případě $|w| = 1$ ověříme pomocí Moivreovy věty, že kořeny rovnice $z^n = r(\cos\alpha + i\sin\alpha)$ jsou

$$z_k = \sqrt[n]{r}\left(\cos\left(\frac{\alpha + k\,2\pi}{n}\right) + i\sin\left(\frac{\alpha + k\,2\pi}{n}\right)\right) \quad \text{pro} \quad k = 0, 1, 2, \ldots, n-1 \ .$$



Obrázek 24. Kořeny rovnice $z^n = w$

1.2.11. *Eulerova formule.* Dříve nebo později se setkáte s *Eulerovo formulí*, která říká, že pro každé reálné číslo α platí

$$e^{i\alpha} = \cos\alpha + i\sin\alpha \ .$$

K důkazu této formule potřebujete vědět, jak se definuje *Eulerovo číslo* e, které je iracionální (stejně jako π) a jeho přibližná hodnota je $2,718$. O něco později se pak dozvíte, jak spočítat mocninu $e^{i\alpha}$ s čistě imaginárním exponentem $i\alpha$.

V této chvíli můžeme Eulerovu formuli použít jako pohodlnější zápis komplexních jednotek $\cos\alpha + i\sin\alpha$. Dříve dokázané vlastnosti součinu dvou komplexních čísel můžeme pomocí Eulerovy formule zapsat jako pravidla pro počítání s mocninami, které v případě reálných exponentů znáte ze střední školy.

Vzorec pro součin dvou komplexních jednotek pak můžeme zapsat jako

$$e^{i\alpha}\,e^{i\beta} = e^{i(\alpha+\beta)} \ .$$

Podobně jednoduše lze zapsat Moivreovu větu:

$$\left(e^{i\alpha}\right)^n = e^{i(n\alpha)} \ .$$

Goniometrický tvar nenulového čísla $w = r(\cos\alpha + i\sin\alpha)$ je potom

$$z = r\,e^{i\alpha} \ ,$$

kde $r = |w|$ a $\alpha = \arg w$.

Součin dvou komplexních čísel $w = r\,e^{i\alpha}$ a $z = s\,e^{i\beta}$ můžeme zapsat ve tvaru

$$wz = r\,e^{i\alpha}\,s\,e^{i\beta} = (rs)e^{i(\alpha+\beta)} \ ,$$

odkud přímo plynou už dříve uvedené formulky pro absolutní hodnotu a argument součinu dvou komplexních čísel, které říkají, že $|wz| = rs = |w|\,|z|$ a $\arg(wz) = \alpha + \beta = \arg w + \arg z$.

Cvičení

1. Spočítejte reálnou a imaginární část komplexních čísel

$$(1+i)(2-3i)\,, \quad \frac{1+i}{2-3i}\,, \quad (1-i)^4 \ .$$

2. Pro $z = 1 - i$ a $w = 2 + 3i$ spočítejte

$$z + w\,, \quad z - w\,, \quad zw, \quad \frac{z}{w}\,, \quad \overline{z}\,\overline{w}, \quad \overline{wz} \ .$$

3. Najděte reálné a imaginární části kořenů rovnice

$$z^2 = i \ .$$

4. Najděte kořeny kvadratické rovnice

$$z^2 - (3+i)z + (2+i) = 0 \ .$$

5. Dokažte, že $1 + i$ je kořenem kubické rovnice

$$z^3 + z^2 + (5-7i)z - (10+2i) = 0$$

a najděte zbývající dva kořeny této rovnice.

6. Dokažte, že pro libovolná dvě nenulová komplexní čísla z, w platí

$$\arg\left(\frac{z}{w}\right) = \arg z - \arg w \ .$$

7. Najděte absolutní hodnotu a argument čísel $1+i$ a $\sqrt{3}+i$. Najděte reálnou a imaginární složku čísla

$$\frac{1+i}{\sqrt{3}+i}$$

a dokažte, že

$$\cos\frac{\pi}{12} = \frac{\sqrt{3}+1}{2\sqrt{2}}, \quad \text{a} \quad \sin\frac{\pi}{12} = \frac{\sqrt{3}11}{2\sqrt{2}} \ .$$

8. Najděte všechny kořeny rovnice

$$x^8 = -1 \ .$$

9. Pomocí Moivreovy věty dokažte, že pro každý úhel α platí

$$\cos 5\alpha = 16\,\cos^5\alpha - 20\cos^3\alpha + 5\cos\alpha, \quad \sin 5\alpha = (16\cos^4\alpha - 12\cos^2\alpha + 1)\,\sin\alpha \ .$$

10. Najděte vyjádření $\cos 3\alpha$ a $\sin 3\alpha$ pomocí $\cos\alpha$ a $\sin\alpha$.

11. Dokažte, že pro každou komplexní jednotku $z = \cos\alpha + i\sin\alpha$ platí

$$2\cos\alpha = z + \frac{1}{z}\,, \quad 2i\,\sin\alpha = z - \frac{1}{z} \ .$$

12. Dokažte, že je-li $w \neq 1$ kořen rovnice $z^3 = 1$, pak platí

$$1 + w + w^2 = 0 \ .$$

13. Dokažte, že pro komplexní jednotku

$$z = \cos \frac{2\pi}{5} + i \sin \frac{2\pi}{5}$$

platí

$$1 + z + z^2 + z^3 + z^4 = 0 \ .$$

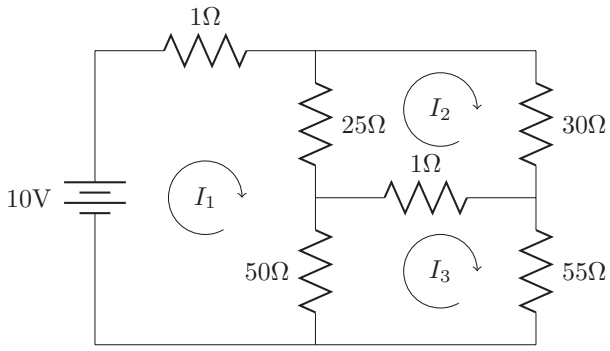
2. Řešení soustav lineárních rovnic

Cíl. *Naučíme se řešit soustavy lineárních rovnic Gaussovo eliminační metodou. Ukážeme si jak parametricky vyjádřit množinu všech řešení takové soustavy. A upozorníme na problémy, které přináší řešení velkých soustav lineárních rovnic na počítačích.*

2.1. **Úlohy vedoucí na soustavy lineárních rovnic.**

Mnoho nejrůznějších úloh lze převést na řešení soustavy lineárních rovnic. Pro ilustraci uvedeme pět jednoduchých příkladů z různých oborů.

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



Obrázek 25. Elektrický obvod z části 2.1.1

Použijeme metodu elementárních smyček. Spočívá v tom, že obvod nějak rozdělíme na elementární smyčky a v každé smyčce si libovolně zvolíme směr procházejícího proudu. Proudy protékající jednotlivými elementárními smyčkami označíme I_1, I_2, I_3 podle obrázku. Použijeme druhý Kirchhoffův zákon, který říká, že součet orientovaných napětí na jednotlivých odporech v uzavřené smyčce se rovná součtu napětí na zdrojích v této smyčce. Pro každou smyčku tak získáme (ještě s pomocí Ohmova zákona) jednu rovnici:

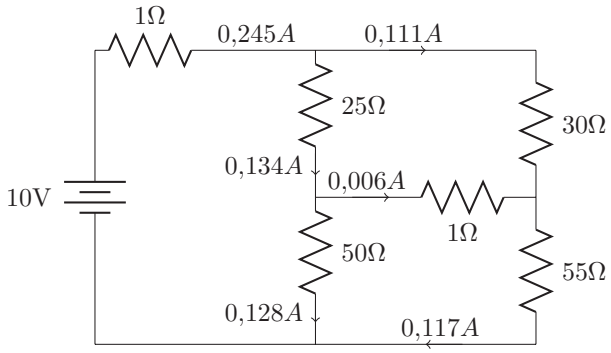
$$\begin{aligned} 1I_1 + 25(I_1 - I_2) + 50(I_1 - I_3) &= 10 \\ 25(I_2 - I_1) + 30I_2 + 1(I_2 - I_3) &= 0 \\ 50(I_3 - I_1) + 1(I_3 - I_2) + 55I_3 &= 0 \ . \end{aligned}$$

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.

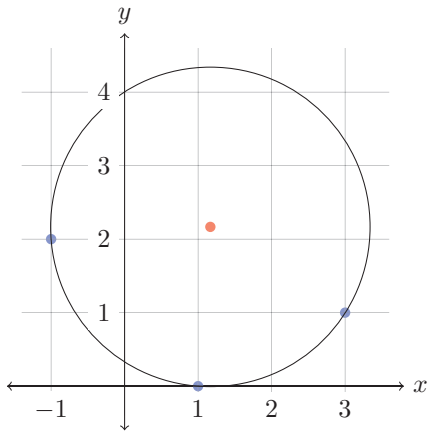
2.1.2. *Prokládání kružnice danými body.* Chceme najít kružnici v rovině procházející body $(1, 0)$, $(-1, 2)$, $(3, 1)$. (Například víme, že nějaký objekt se pohybuje po kruhové dráze, máme změřeny tři polohy a chceme určit střed obíhání.)

Rovnice kružnice v rovině má tvar

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



Obrázek 26. Proudy v elektrickém obvodu z části 2.1.1



Obrázek 27. Kružnice procházející danými třemi body

Dosazením daných třech bodů získáme soustavu lineárních rovnic

$$\begin{aligned} 1 + a + c &= 0 \\ 5 - a + 2b + c &= 0 \\ 10 + 3a + b + c &= 0 \ . \end{aligned}$$

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 kružnice, rovnici můžeme upravit na tvar

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

ze 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.

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

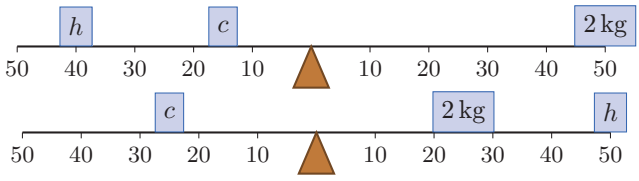
Chceme tedy najít hodnoty x, y, z, v, které splňují soustavu rovnic. To vede na rovnice

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

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

Reálný význam mají pouze nezáporná řešení. Nezajímají nás tedy všechna řešení soustavy, ale pouze ta řešení, která splňují dodatečné omezující podmínky $x \geq 0$, $y \geq 0$, $z \geq 0$, $v \geq 0$. S těmito omezujícími podmínkami dostáváme *soustavu lineárních rovnic a nerovností*. Množiny všech řešení takových soustav hrají významnou roli v matematickém oboru nazývaném *lineární programování* nebo *lineární optimalizace*. V těchto úlohách se maximalizuje hodnota nějaké lineární funkce definované na množině všech řešení soustavy lineárních rovnic a nerovností. Úlohy lineárního programování jsou nejjednodušší třídou a nejpoužívanějším typem *optimalizačních úloh*, rozsáhlého oboru s aplikacemi v nejrůznějších oblastech lidského konání.

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

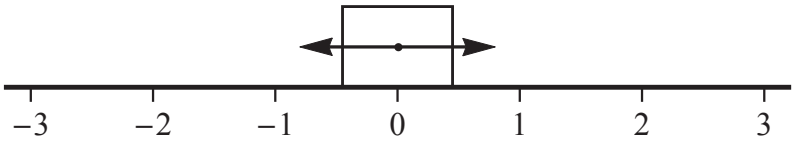


Obrázek 28. Neznámá závaží

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

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

kterou snadno vyřešíme.



Obrázek 29. Pohyb hlavy čtečky

2.1.5. *Pohyb hlavy disku.* Objekt jednotkové hmotnosti se pohybuje bez tření po přímce, na počátku je v poloze 0 a má nulovou rychlost.

Po dobu 8 vteřin na objekt působí vnější síly $f(t)$. Vnější síla je konstantní vždy během jedné vteřiny, tj. $f(t) = x_j$ pro $j - 1 \leq t < j$ a $j = 1, 2, \ldots, 8$. Chceme dosáhnout toho, aby se po 8 vteřinách poloha objektu rovnala b_1 a jeho rychlost byla b_2. Vektor neznámých sil $(x_1, \ldots, x_8)$ proto musí splňovat soustavu

$$\begin{aligned} \frac{15}{2}x_1 + \frac{13}{2}x_2 + \frac{11}{2}x_3 + \frac{9}{2}x_4 + \frac{7}{2}x_5 + \frac{5}{2}x_6 + \frac{3}{2}x_7 + \frac{1}{2}x_8 &= b_1 \\ x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 &= b_2 \ . \end{aligned}$$

2.2. **Soustavy lineárních rovnic a aritmetické vektory.**

2.2.1. *Soustavy lineárních rovnic.*

Definice 2.1. *Lineární rovnice o n neznámých* s reálnými koeficienty je rovnice

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b \ ,$$

kde všechny koeficienty $a_1, a_2, \ldots, a_n$ a číslo b jsou daná reálná čísla a $x_1, x_2, \ldots, x_n$ jsou neznámé.

Soustava m lineárních rovnic o n neznámých je soustava

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

s reálnými koeficienty a_{ij}, reálnými pravými stranami b_i a neznámými $x_1, x_2, \ldots, x_n$.

Koeficient a_{ij} je koeficient v i-té rovnici u j-té neznámé x_j. První z indexů ij je index rovnice, druhý je index neznámé.

Jedno řešení soustavy lineárních rovnic o n neznámých budeme zapisovat jako uspořádanou n-tici čísel. To předpokládá nějaké pevné uspořádání neznámých. Z kontextu bude toto uspořádání zřejmé, neznámé jsou většinou značeny $x_1, \ldots, x_n$. Uspořádanou n-tici čísel nazýváme *n-složkový aritmetický vektor.*

2.2.2. *Aritmetické vektory.*

Definice 2.2. *Aritmetickým vektorem nad $\mathbb{R}$ s n složkami* rozumíme uspořádanou n-tici reálných čísel $(x_1, x_2, \ldots, x_n)$.

Později uvidíme, že za vektor lze považovat i funkci, matici, atd. Přívlastek *aritmetický* používáme proto, abychom zdůraznili, že máme na mysli uspořádané n-tice čísel.

Aritmetické vektory budeme psát sloupcově. Například 3-složkový vektor zapíšeme

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

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

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

V první kapitole jsme si připomněli, že 2-složkový aritmetický vektor můžeme interpretovat jako souřadnice bodu nebo jako souřadnice vektoru v rovině se souřadným systémem. Podobně 3-složkové aritmetické vektory mohou geometricky odpovídat bodům nebo vektorům v prostoru.

Na základě analogie můžeme říkat, že 4-složkové aritmetické vektory $(a_1, a_2, a_3, a_4)^T$ odpovídají bodům nebo vektorům ve čtyřdimenzionálním prostoru s nějakým souřadným systémem, přestože čtyřdimenzionální prostor si už vizuálně představit neumíme. Podobně pro každé $n \in \mathbb{N}$ můžeme n-složkové aritmetické vektory interpretovat jako body nebo jako vektory v prostoru dimenze n.

2.2.3. *Operace s aritmetickými vektory.* Každý reálný aritmetický vektor můžeme násobit reálným číslem a aritmetické vektory se stejným počtem složek můžeme sčítat. Obě operace provádíme „po složkách“.

Definice 2.3. 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

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

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

$$t \cdot \mathbf{u} = t\mathbf{u} = t \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} tu_1 \\ tu_2 \\ \vdots \\ tu_n \end{pmatrix} \ .$$

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

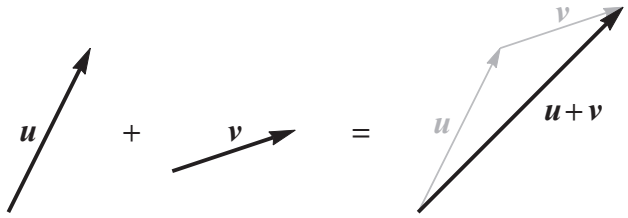
$$-\mathbf{u} = (-1) \cdot \mathbf{u} \quad \text{a} \quad \mathbf{u} - \mathbf{v} = \mathbf{u} + (-\mathbf{v}) \ .$$

Vektor $-\mathbf{u}$ nazýváme *opačný vektor* k vektoru $\mathbf{u}$.

Příklad 2.4.

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

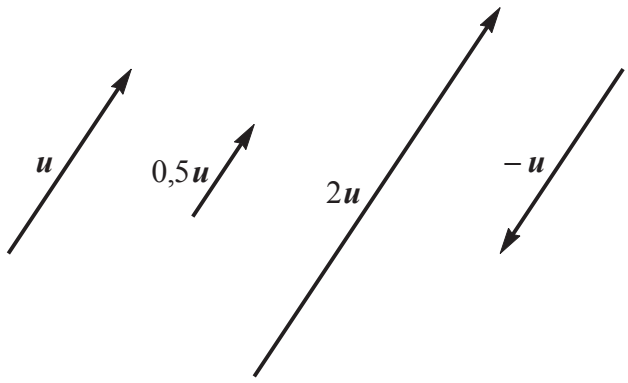
Obě operace mají přirozenou geometrickou interpretaci. Ukážeme si ji na příkladu vektorů v rovině. Stejně tak by to vyšlo v prostoru, pouze obrázky by byly méně přehledné. (Fyzikální) vektory můžeme sčítat bez systému souřadnic.



Obrázek 30. Součet vektorů v rovině

Pokud v rovině zvolíme souřadný systém, ve kterém má vektor $\mathbf{u}$ souřadnice $(u_1, u_2)^T$ a vektor $\mathbf{v}$ souřadnice $(v_1, v_2)^T$, pak jejich součet $\mathbf{u} + \mathbf{v}$ má v tomtéž souřadném systému souřadnice $(u_1 + v_1, u_2 + v_2)^T$. Sčítání aritmetických vektorů tak odpovídá sčítání (fyzikálních) vektorů.

Podobně je tomu s násobením (fyzikálních) vektorů reálným číslem. Ty také můžeme násobit reálným číslem bez nějakého systému souřadnic.



Obrázek 31. Násobky vektorů v rovině

Pokud máme v rovině zvolený souřadný systém, ve kterém má vektor $\mathbf{u}$ souřadnice $(u_1, u_2)^T$, pak pro jakékoliv reálné číslo t má vektor $t\mathbf{u}$ v témže souřadném systému souřadnice $(tu_1, tu_2)^T$. Opačný vektor $-\mathbf{u}$ má souřadnice $-(u_1, u_2)^T$.

2.3. **Příklady.** Řešíme-li ručně soustavu o několika málo rovnicích a neznámých, postupujeme obvykle tak, že postupně eliminujeme neznámé.

2.3.1. *Ekvivalentní úpravy.* Na prostém příkladu dvou lineárních rovnic o dvou neznámých si ukážeme, jak eliminaci neznámých provádět jednoduše. Používáme k tomu úpravy, které nemění množinu všech řešení soustavy. Takovým úpravám říkáme *ekvivalentní úpravy.*

Definice 2.5. *Ekvivalentní úpravou* soustavy lineárních rovnic rozumíme úpravu, která nemění množinu všech řešení.

Příklad 2.6. Vyřešíme soustavu

$$\begin{aligned} x_1 + 2x_2 &= 3 \\ 3x_1 - x_2 &= 2 \ . \end{aligned}$$

Budeme eliminovat neznámou x_1. Z první rovnice ji vyjádříme pomocí x_2:

$$x_1 = 3 - 2x_2 \ ,$$

a dosadíme do druhé rovnice, první rovnici necháme beze změny:

$$\begin{aligned} x_1 + 2x_2 &= 3 \\ 3(3 - 2x_2) - x_2 &= 2 \ . \end{aligned}$$

Po roznásobení a úpravě druhé rovnice dostaneme soustavu

$$\begin{aligned} x_1 + 2x_2 &= 3 \\ -7x_2 &= -7 \ . \end{aligned}$$

Eliminovali jsme tak neznámou x_1 z druhé rovnice. Stejné úpravy soustavy můžeme dosáhnout mnohem rychleji tak, že připočteme (-3)-násobek první rovnice k druhé a první rovnici necháme beze změny.

Soustavu pak jednoduše dořešíme. Z druhé rovnice vypočteme $x_2 = 1$ a dosadíme do první rovnice (znovu eliminace, tentokrát neznámé x_2). Dostaneme

$$x_1 = 3 - 2x_2 = 1 \ .$$

Ukazuje se, že při řešení jakékoliv soustavy lineárních rovnic vystačíme pouze se třemi jednoduchými typy ekvivalentních úprav, které nazýváme *elementární úpravy* soustavy. Jsou to

(i) prohození dvou rovnic,
(ii) vynásobení nějaké rovnice **nenulovým** číslem t,
(iii) přičtení t-násobku jedné rovnice k **jiné** rovnici .

Dokážeme, že elementární úpravy jsou skutečně ekvivalentní, tj. že nemění množinu všech řešení soustavy lineárních rovnic.

Tvrzení 2.7. *Elementární úpravy nemění množinu všech řešení soustavy lineárních rovnic.*

Důkaz. Důkaz dostaneme spojením tří jednoduchých úvah. Napřed si všimneme, že každá elementární úprava změní nejvýše jednu rovnici v soustavě.

Potom si ukážeme, že každé řešení $(x_1, x_2, \ldots, x_n)^T$ původní soustavy je také řešením jediné změněné rovnice v nové soustavě. Dokážeme si to na třetí elementární úpravě, kdy přičítáme t-násobek i-té rovnice k j-té rovnici pro nějaké $j \neq i$. Dané řešení $(x_1, x_2, \ldots, x_n)^T$ původní soustavy splňuje rovnice

$$\begin{aligned} a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n &= b_i \\ a_{j1}x_1 + a_{j2}x_2 + \cdots + a_{jn}x_n &= b_j \ , \end{aligned}$$

splňuje proto také rovnici

$$ta_{i1}x_1 + ta_{i2}x_2 + \cdots + ta_{in}x_n = tb_i \ ,$$

(tím jsme mimochodem dokázali, že každé řešení původní soustavy je také řešením nové rovnice vzniklé druhou elementární úpravou) a tedy také rovnici

$$(a_{j1} + ta_{i1})x_1 + (a_{j2} + ta_{i2})x_2 + \cdots + (a_{jn} + ta_{in})x_n = b_j + tb_i \ .$$

Vektor $(x_1, x_2, \dots, x_n)^T$ je samozřejmě také řešením všech ostatních (nezměněných) rovnic nové soustavy.

Označíme S množinu všech řešení původní soustavy a T množinu všech řešení nové soustavy. Právě jsme dokázali, že platí $S \subseteq T$ – žádné řešení původní soustavy se elementárními úpravami neztratí.

A nakonec si uvědomíme, že efekt každé elementární úpravy můžeme zvrátit jinou elementární úpravou a dostat zpět původní soustavu. V případě první úpravy stačí prohodit ještě jednou prohozené rovnice. V případě druhé úpravy stačí tutéž rovnici vynásobit inverzním číslem t^{-1} (proto je nutné předpokládat $t \neq 0$). V případě třetí úpravy přičteme $(-t)$ násobek i-té rovnice k j-té rovnici. (To předpokládá, že i-tá rovnice se třetí elementární úpravou nezměnila, proto předpoklad $j \neq i$.)

Protože původní soustavu dostaneme z nové také jednou elementární úpravou, platí rovněž $T \subseteq S$, odkud plyne rovnost $S = T$. Ta říká, že původní a nová soustava mají stejné množiny všech řešení. □

2.3.2. *Soustava s jedním řešením.* Začneme příkladem řešení soustavy tří lineárních rovnic o třech neznámých x_1, x_2, x_3 pomocí elementárních úprav.

Příklad 2.8. Vyřešíme soustavu

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

Principem eliminační metody je převést soustavu elementárními úpravami do tvaru, ze kterého se řešení snadno dopočítá. Tvar, o který se snažíme, je tzv. *odstupňovaný tvar*. Přesně bude definován později, ale neformálně řečeno odstupňovaný tvar znamená, že v každé rovnici je na začátku více nulových koeficientů než v rovnici předcházející.

Nejprve docílíme toho, že ve všech rovnicích kromě první bude nulový koeficient u x_1. Tomuto procesu se také říká eliminace neznámé x_1. Uděláme to tak, že přičteme vhodné násobky vhodné rovnice (vhodná je každá rovnice s nenulovým koeficientem u x_1) k ostatním tak, aby z ostatních rovnic neznámá x_1 „zmizela“, tj. měla v nich nulový koeficient.

V našem případě bychom mohli $(-3/2)$-násobek první rovnice přičíst k druhé a (-1)-násobek první rovnice přičíst ke třetí. Aby nám vycházely hezčí koeficienty, vynásobíme napřed třetí rovnici jednou polovinou:

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

a pak ji prohodíme s první rovnicí:

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

Nyní jsme připraveni k eliminaci neznámé x_1. Přičteme (-3)-násobek první rovnice ke druhé:

$$\begin{aligned} x_1 + 2x_2 + 5x_3 &= 8 \\ -x_2 + 3x_3 &= 9 \\ 2x_1 + 6x_2 + 5x_3 &= 0 \ . \end{aligned}$$

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 neznámé již první rovnici nebudeme měnit a budeme se zabývat pouze zbylými rovnicemi. V našem případě již zbývají pouze dvě a k eliminaci neznámé x_2 stačí přičíst 2-násobek druhé rovnice ke třetí.

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

Tím jsme dokončili *eliminační fázi* řešení soustavy a můžeme dopočítat řešení tzv. *zpětnou substitucí*, kdy postupujeme od poslední rovnice k první a postupně dosazováním získáváme hodnoty jednotlivých neznámých. V našem případě dostáváme $x_3 = 2$, $x_2 = -3$, $x_1 = 4$. Původní soustava má právě jedno řešení, a to aritmetický vektor

$$\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 4 \\ -3 \\ 2 \end{pmatrix} \ .$$

Jak jsme si už ukázali v příkladu 2.6, výpočet nějaké neznámé z jedné rovnice a dosazení výsledku do jiné je elementární úprava typu (iii). Také při zpětné sustituci používáme pouze ekvivalentní úpravy, které nemění množinu všech řešení soustavy.

Při řešení soustavy jsme mohli samozřejmě začít eliminací libovolné neznámé, také nebylo nutné třetí rovnici přehazovat s první a násobit ji napřed jednou polovinou.

Pro řešení velkých soustav tisíců rovnic o tisících neznámých potřebujeme jednotlivé kroky eliminace nějak uspořádat tak, aby je bylo možné použít kdykoliv a bez ohledu na to, jaké jsou koeficienty soustavy. Tomuto postupu se říká *Gaussova eliminační metoda* nebo zkráceně *Gaussova eliminace*.

2.3.3. *Maticový zápis.* K formulaci Gaussovy eliminace a také pro zkrácení zápisu budeme místo soustavy psát její *rozšířenou matici*. Nejprve zavedeme pojem matice.

Definice 2.9. *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 index označuje řádek, druhý sloupec.

Definice 2.10. *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 koeficientů u neznámých:

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

Vektor pravých stran je vektor $\mathbf{b} = (b_1, b_2, \dots, b_m)^T$ a *rozšířená matice soustavy* je matice typu $m \times (n+1)$

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

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 přidáme pravou stranu. Pro přehlednost se pravé strany někdy oddělují svislou čarou. Rozšířená matice se tím 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 pořadě

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

Prohození dvou rovnic se v rozšířené matici projeví prohozením odpovídajících 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 odpovídá přičtení t-násobku i-tého řádku k j-tému řádku. 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 zkrátil a zpřehlednil.

Místo „soustava rovnic s rozšířenou maticí $(A\,|\,\mathbf{b})$“ budeme někdy stručně říkat „soustava $(A\,|\,\mathbf{b})$“. V dalším textu také budeme často místo slova *neznámá* používat slovo *proměnná*.

Poznamenejme ještě, že užitím násobení matic z kapitoly 4 lze řešení soustavy rovnic s rozšířenou maticí $(A\,|\,\mathbf{b})$ zapsat jako hledání všech aritmetických 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 než maticový zápis ani nebudeme používat.

2.3.4. *Jeden parametr.* Podívejme se nyní na příklad soustavy tří 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 odpovídající 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. Neznámou x_2 lze volit libovolně a budeme jí říkat *parametr*. Parametr označíme $x_2 = t$ a vyjde $x_1 = 11 - 4x_2 - 3x_3 = 5 - 4t$. 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 také neznámou $x_1 = s$, dopočítat $x_2 = 5/4 - s/4$ a získat množinu řešení ve tvaru

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

Nevýhodou této druhé 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 aritmetických vektorů a jejich násobení reálnými čísly 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 ihned, že řešením je přímka procházející bodem $(5, 0, 2)^T$ se směrovým vektorem $(-4, 1, 0)^T$.

2.3.5. *Více parametrů.* Podíváme se na soustavu s více parametry, ze které již snad bude vidět obecný postup. Soustava bude mít pět neznámých x_1, x_2, x_3, x_4, x_5, její řešení budou 5-složkové aritmetické vektory, které odpovídají bodům (nebo vektorům) v pětidimenzionálním prostoru. Vizuální představa proto není dost dobře možná.

Elementárními úpravami rozšířené matice soustavy dostaneme

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

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

V první úpravě jsme prohodili řádky tak, 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*, neboť jejich hodnoty můžeme zvolit libovolně: $x_2 = t_2$, $x_4 = t_4$, $x_5 = t_5$ pro nějaká čísla $t_2, t_4, t_5 \in \mathbb{R}$.

Hodnoty bázových proměnných x_1, x_3 pak dopočteme zpětnou substitucí. Tím dostaneme $x_3 = -3 - 2t_5$ a $x_1 = 2 - 2t_2 + x_3 - 3t_4 = -1 - 2t_2 - 3t_4 - 2t_5$. Množinu všech řešení soustavy tak můžeme zapsat jako množinu 5-složkových aritmetických vektorů

$$\left\{ \begin{pmatrix} -1 - 2t_2 - 3t_4 - 2t_5 \\ t_2 \\ -3 - 2t_5 \\ t_4 \\ t_5 \end{pmatrix} : t_2, t_4, t_5 \in \mathbb{R} \right\} ,$$

kterou pomocí operací s aritmetickými vektory zapíšeme v parametrickém tvaru

$$\left\{ \begin{pmatrix} -1 \\ 0 \\ -3 \\ 0 \\ 0 \end{pmatrix} + t_2 \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + t_4 \begin{pmatrix} -3 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + t_5 \begin{pmatrix} -2 \\ 0 \\ -2 \\ 0 \\ 1 \end{pmatrix} : t_2, t_4, t_5 \in \mathbb{R} \right\} .$$

Později si ukážeme o něco rychlejší způsob, jak najít parametrické vyjádření množiny všech řešení soustavy lineárních rovnic.

2.4. **Řešení obecné soustavy rovnic Gaussovo eliminací.** Nyní představíme obecnou metodu řešení soustav lineárních rovnic.

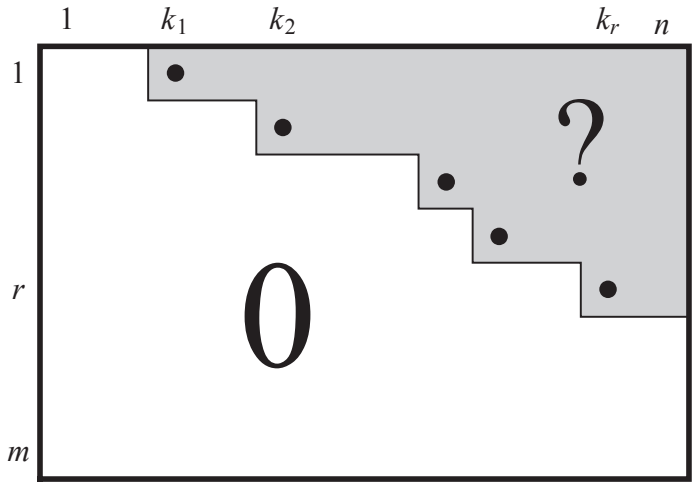
2.4.1. *Odstupňovaný tvar.* Dosud jsme při řešení soustav lineárních rovnic vystačili s ekvivalentními úpravami tří typů. A protože místo rovnic píšeme rozšířenou matici soustavy, provádíme úpravy řádků této matice. Proto jim říkáme *elementární řádkové úpravy*. Definujeme je pro jakoukoliv matici.

Definice 2.11. *Elementárními řádkovými úpravami* jakékoliv matice $A = (a_{ij})_{m\times n}$ rozumíme následující tři typy úprav:

(i) prohození dvou řádků matice,
(ii) vynásobení jednoho z řádků matice nenulovým číslem,
(iii) přičtení libovolbého násobku jednoho řádku k jinému řádku.

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

Gaussova eliminační metoda je založená na převodu jakékoliv matice do řádkově odstupňovaného tvaru pomocí elementárních řádkových úprav. Odstupňovaný tvar matice $C = (c_{ij})_{m\times n}$ jsme dosud popisovali neformálně podmínkou, že v každém nenulovém řádku matice C je na počátku (tj. zleva) více nul, než na počátku řádku nad ním. Z neformálního popisu ihned plyne, že nad žádným nenulovým řádkem nemůže být nulový řádek. V matici v řádkově odstupňovaném tvaru tak jsou všechny nenulové řádky v horní části matice a teprve pod nimi jsou řádky nulové.



Obrázek 32. Matice v řádkově odstupňovaném tvaru

Formálně definujeme matici v řádkově odstupňovaném tvaru následovně.

Definice 2.12. Matice $C = (c_{ij})_{m\times n}$ je v *řádkově odstupňovaném tvaru*, pokud existuje celé číslo $r \in \{0, 1, \dots, m\}$ takové, že řádky $r+1, \dots, m$ jsou nulové, řádky $1, \dots, r$ jsou nenulové, a platí $k_1 < k_2 < \cdots < k_r$, kde k_i je index sloupce, 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.

Lze také definovat sloupcově odstupňovaný tvar matice. Ten ale nebudeme používat, proto budeme místo řádkově odstupňovaný tvar říkat stručněji *odstupňovaný tvar*.

Příklad 2.13. 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

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

v odstupňovaném tvaru nejsou.

Gaussova eliminace převádí každou matici $A = (a_{ij})_{m\times n}$ do odstupňovaného tvaru posloupností elementárních řádkových úprav.

Eliminace jednoho sloupce (jedné proměnné) proběhne následovně.

1. Najdeme první nenulový sloupec, jeho index označíme k_1. Pokud takový sloupec neexistuje, je matice A v řádkově odstupňovaném tvaru (neboť je nulová), jsme tedy hotovi.
2. Pokud je $a_{1k_1} = 0$, prohodíme první řádek s libovolným řádkem i, ve kterém je $a_{ik_1} \neq 0$.
3. Pro každé $i = 2, 3, \ldots, m$ přičteme $(-a_{ik_1}/a_{1k_1})$-násobek prvního řádku k i-tému řádku.

(Všimněte si, že po provedení kroku 2. máme $a_{1k_1} \neq 0$ a po provedení kroku 3 máme $a_{2k_1} = a_{3k_1} = \cdots = a_{mk_1} = 0$.)

Dále postup opakujeme s maticí bez prvního řádku. V dalším kroku tedy najdeme první sloupec s indexem k_2, pro který je alespoň jedno z čísel $a_{2k_2}, \ldots, a_{mk_2}$ nenulové, řekněme $a_{jk_2} \neq 0, j \geq 2$. Prohodíme druhý a j-tý řádek a pak pro každé $i = 3, 4, \ldots, m$ přičteme $(-a_{ik_2}/a_{2k_2})$-násobek prvního řádku k i-tému řádku.

Gaussova eliminace končí buď v bodě 1, nebo ve chvíli, kdy dojdou nenulové řádky. To je i případ, kdy má matice A pouze jeden nenulový řádek.

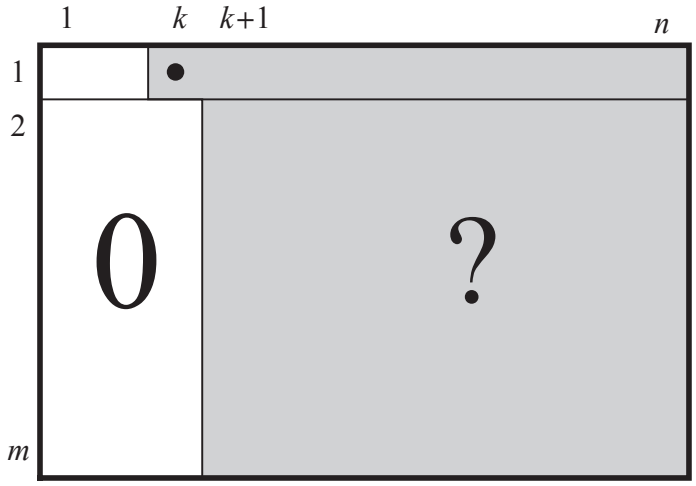
Náš popis Gaussovy eliminace není algoritmus, protože nepředepisujeme, který řádek prohodíme s prvním řádkem v kroku 2. Různé implementace Gaussovy eliminace to řeší různým způsobem, což je důvod, proč žádný konkrétní způsob nepředepisujeme. Více o tom v části 2.6 o numerické stabilitě.

Věta 2.14. *Gaussova eliminace převede každou matici $A = (a_{ij})$ typu $m \times n$ do odstupňovaného tvaru.*

Důkaz. Důkaz provedeme indukcí podle počtu řádků matice A, tj. podle m. Předpokládejme tedy, že věta platí, pokud má matice méně než m řádků, a vezměme

matici A s m řádky. Pokud ji tvoří samé nuly, pak se eliminace zastaví v bodě 1. a věta platí, protože nulová matice je v odstupňovaném tvaru. Předpokládejme tedy, že tomu tak není.

Nechť k je index prvního nenulového sloupce v matici soustavy. Označme B matici po provedení eliminace k-tého sloupce.



Obrázek 33. Gaussova eliminace po prvním cyklu

Z matice B vynecháme první řádek a na matici se zbylými $m-1$ řádky provedeme Gaussovu eliminaci. Podle indukčního předpokladu dostaneme matici C v odstupňovaném tvaru. První nenulový sloupec v matici C má index $l > k$, neboť první nenulový sloupec v celé matici A měl index k a všechny prvky v k-tém sloupci matice B pod nenulovým prvkem v prvním řádku jsou nulové. Vrátíme-li do matice C nahoru první řádek matice B, dostaneme tak opět matici v odstupňovaném tvaru.

Tato matice je výsledkem Gaussovy eliminace na původní matici A. □

Platí dokonce více – počet r nenulových řádků v matici C je maticí A určený jednoznačně, tj. nezávisí na tom, jak jsme Gaussovu eliminaci použili. Stejně tak jsou maticí A jednoznačně určené indexy $k_1, k_2, \ldots, k_r$ sloupců v matici C, které obsahují pivoty. Dokážeme si to později, příslušnou terminologii zavedeme už nyní.

Definice 2.15. Číslo r, tj. počet nenulových řádků v matici C v odstupňovaném tvaru, kterou dostaneme z matice A Gaussovo eliminací, se nazývá *hodnost matice* A a značí se $r(A)$ nebo $\operatorname{rank}(A)$. Sloupce v matici A s indexy $k_1, k_2, \ldots, k_r$ z definice 2.12 nazýváme *bázové sloupce* matice A.

2.4.2. *Eliminační fáze řešení soustavy lineárních rovnic.* Máme-li řešit soustavu m lineárních rovnic o n neznámých $x_1, \ldots, x_n$ s rozšířenou maticí $(A \,|\, \mathbf{b})$, použijeme Gaussovu eliminaci na matici $(A \,|\, \mathbf{b})$. Výsledkem je nějaká matice $(C \,|\, \mathbf{d})$ v řádkově odstupňovaném tvaru. Dostaneme tak bázové sloupce matice $(A \,|\, \mathbf{b})$. Je-li sloupec pravých stran $\mathbf{b}$ bázový, je poslední nenulový řádek matice $(C \,|\, \mathbf{d})$ tvaru

$(0\ 0\ \dots\ 0\,|\,d_r)$, kde pivot $d_r \neq 0$. Tento řádek odpovídá rovnici

$$0x_1 + 0x_2 + \cdots + 0x_n = d_r \ ,$$

která nemá žádné řešení. Původní soustava $(A\,|\,\mathbf{b})$ je proto také neřešitelná.

Pokud sloupec pravých stran není bázový sloupec matice $(A\,|\,\mathbf{b})$, tj. platí-li $1 \leq k_1 < k_2 < \cdots < k_r \leq n$, ukážeme že soustava $(A\,|\,\mathbf{b})$ je řešitelná a najdeme všechna řešení pomocí zpětné substituce.

2.4.3. *Zpětná substituce.* Označíme P množinu indexů těch sloupců od 1 do n, které neobsahují pivot, tj.

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

Množina P může být i prázdná, pokud každý sloupec rozšířené matice soustavy $(A\,|\,\mathbf{b})$ s výjimkou sloupce pravých stran obsahuje pivot. Proměnným x_p, $p \in P$, říkáme volné proměnné (nebo též parametry). Ostatní proměnné, tj.proměnné $x_{k_1}, x_{k_2}, \dots, x_{k_r}$ jsou bázové proměnné.

Nyní nahlédneme, že každá volba hodnot volných proměnných dává právě jedno řešení soustavy $(A \mid \mathbf{b})$. Matici $(C\,|\,\mathbf{d})$ po provedení Gaussovy eliminace odpovídá soustava lineárních rovnic ve tvaru

$$\begin{aligned}
c_{1,k_1}x_{k_1} + c_{1,k_1+1}x_{k_1+1} + \cdots + c_{1,n}x_n &= d_1 \\
c_{2,k_2}x_{k_2} + c_{2,k_2+1}x_{k_2+1} + \cdots + c_{2,n}x_n &= d_2 \\
&\vdots \\
c_{r,k_r}x_{k_r} + c_{r,k_r+1}x_{k_r+1} + \cdots + c_{r,n}x_n &= d_r \ ,
\end{aligned}$$

což je ekvivalentní soustavě rovnic

$$\begin{aligned}
x_{k_1} &= c_{1,k_1}^{-1}(d_1 - c_{1,k_1+1}x_{k_1+1} - \ldots - c_{1,n}x_n) \\
x_{k_2} &= c_{2,k_2}^{-1}(d_2 - c_{2,k_2+1}x_{k_2+1} - \ldots - c_{2,n}x_n) \\
&\vdots \\
x_{k_r} &= c_{r,k_r}^{-1}(d_r - c_{r,k_r+1}x_{k_r+1} - \ldots - c_{r,n}x_n) \ .
\end{aligned}$$

Poslední rovnice jednoznačně určuje hodnotu bázové proměnné x_{k_r} pomocí hodnot volných proměnných – parametrů. Po dosazení za x_{k_r} do předposlední rovnice jednoznačně spočteme $x_{k_{r-1}}$ pomocí hodnot volných proměnných – parametrů, atd. Tomuto dopočítávání hodnot bázových proměnných říkáme *zpětná substituce*. Dokázali jsme tak následující pozorování.

Pozorování 2.16. *Pokud sloupec pravých stran rovnice $(A\,|\,\mathbf{b})$ není bázový, pak pro libovolná reálná čísla $x_p \in \mathbb{R}$, $p \in P$, existují jednoznačně určená reálná čísla $x_{k_1}, x_{k_2}, \dots, x_{k_r} \in \mathbb{R}$ taková, že aritmetický vektor $(x_1, x_2, \dots, x_n)^T$ je řešením soustavy $(A\,|\,\mathbf{b})$.*

Nakonec podobně jako v částech 2.3.4 a 2.3.5 vyjádříme množinu všech řešení soustavy $(A\,|\,\mathbf{b})$ ve tvaru

$$S = \left\{ \mathbf{u} + \sum_{p \in P} t_p \mathbf{v}_p : \ t_p \in \mathbb{R} \ \text{ pro každé } \ p \in P \right\} \ ,$$

kde $\mathbf{u}$ a $\mathbf{v}_p$ pro $p \in P$ jsou vhodné n-složkové aritmetické vektory.

Dosavadní poznatky o řešení soustav lineárních rovnic si shrneme do následující věty.

Věta 2.17. *Množina všech řešení řešitelné soustavy* $(A \mid \mathbf{b})$ *o* n *neznámých je rovná množině*

$$S = \left\{ \mathbf{u} + \sum_{p \in P} t_p \mathbf{v}_p : \ t_p \in \mathbb{R} \ \ \textit{pro každé} \ \ p \in P \right\}$$

pro vhodné n*-složkové aritmetické vektory* $\mathbf{u}$ *a* $\mathbf{v}_p$*,* $p \in P$*.*

V kapitole 5 si ukážeme mnohem elegantnější a kratší důkaz polední věty. Z něho bude také vidět význam aritmetických vektorů $\mathbf{u}$ a $\mathbf{v}_p$, $p \in P$.

2.4.4. *Shrnutí.* Obecnou soustavu m 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. pokud existuje rovnice typu $0x_1+0x_2+\cdots+0x_n = b \neq 0$, skončíme s tím, že soustava je neřešitelná.
3. Určíme volné proměnné (parametry) – tj. proměnné odpovídající sloupcům, kde nejsou pivoty. Množinu indexů těchto sloupců označíme P.
4. Množinu všech řešení vyjádříme tvaru

$$\left\{ \mathbf{u} + \sum_{p \in P} t_p \mathbf{v}_p : \ t_p \in \mathbb{R} \ \ \text{pro každé} \ \ p \in P \right\}$$

   pro vhodné n-složkové aritmetické vektory $\mathbf{u}$ a $\mathbf{v}_p$, $p \in P$.

Všimněte si, že počet volných proměnných je roven číslu $n-r$, kde r je počet nenulových řádků matice v odstupňovaném tvaru, kterou jsme dostali z rozšířené matice řešitelné soustavy $(A \mid \mathbf{b})$ Gaussovo eliminací. Již dříve jsme definovali, že toto číslo se rovná hodnosti $\operatorname{rank}(A \mid \mathbf{b})$ rozšířené matice soustavy. Zatím sice neumíme dokázat, že hodnost matice nezávisí na tom, jaké ekvivalentní úpravy používáme k jejímu převodu do odstupňovaného tvaru, nicméně tomu tak je. Intuitivně to lze zdůvodnit tím, že v popisu množiny řešení máme $n - r$ parametrů, takže množina řešení je $(n - r)$-dimenzionální útvar, přičemž tato dimenze samozřejmě závisí jen na původní soustavě, nikoliv na konkrétním odstupňovaném tvaru.

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

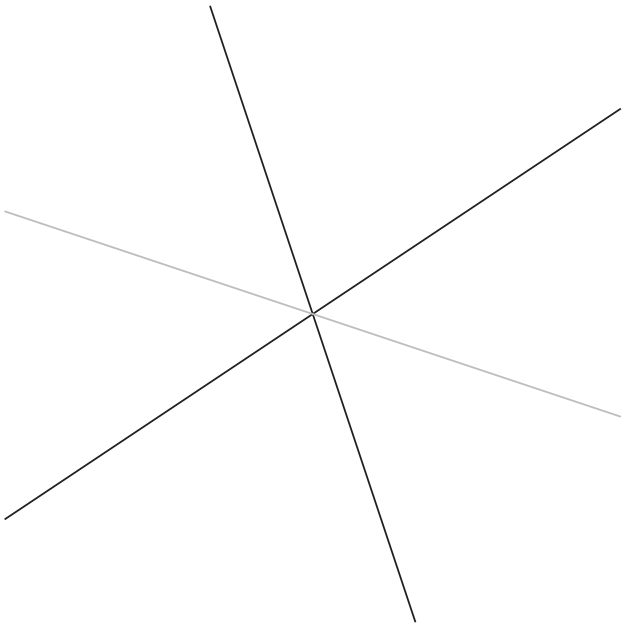
V další části této kapitoly se budeme zabývat třemi souvisejícími otázkami.

- Jak rozumět geometrii soustav lineárních rovnic?
- Co se může přihodit, budeme-li soustavy lineárních rovnic řešit na počítači?
- Jak dlouho to bude trvat?

2.5. **Geometrie soustav lineárních rovnic.**

2.5.1. *Řádkový pohled na soustavy lineárních rovnic.* V první opakovací kapitole jsme si ukázali, že v případě soustavy lineárních rovnic o dvou neznámých x_1, x_2 určuje každá rovnice nějakou přímku v rovině, pokud je aspoň jeden z koeficientů u x_1 a x_2 nenulový. Množina všech řešení je potom průnikem těchto přímek. 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 rovnice soustavy popisují alespoň dvě různé přímky a všechny tyto přímky procházejí jedním bodem.

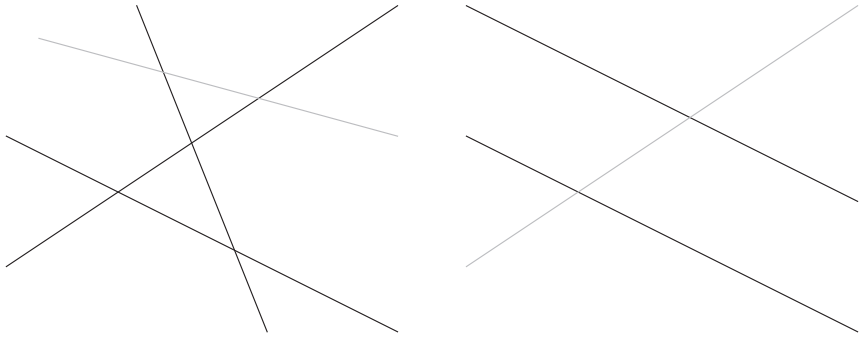


Obrázek 34. Geometrie jednoznačně řešitelné soustavy o dvou neznámých

- 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 $0x_1 + 0x_2 = 123$.

V případě soustavy lineárních rovnic o třech neznámých x_1, x_2, x_3 je každé řešení nějaký bod v trojrozměrném prostoru. Každá rovnice s aspoň jedním nenulovým koeficientem u neznámých x_1, x_2, x_3 určuje nějakou rovinu v prostoru. Množina všech řešení soustavy je tedy průnikem nějakých rovin. Pro množinu všech řešení tedy máme následující možnosti, už bez obrázků.

- Celý prostor. To nastane v triviálním případě, kdy jsou všechny rovnice v soustavě tvaru $0x_1 + 0x_2 + 0x_3 = 0$.
- Rovina.
- Přímka.



Obrázek 35. Geometrické důvody neřešitelnosti soustavy o dvou neznámých

- Bod.
- Prázdná množina. Tento případ nastane, pokud dvě rovnice určují rovnoběžné roviny, nebo jsou roviny sice po dvou různoběžné, ale nemají žádný společný bod (v tom případě musí být aspoň tři), a nebo je v soustavě triviálně neřešitelná rovnice, například $0x_1 + 0x_2 + 0x_3 = 123$.

Jedna netriviální lineární rovnice o dvou neznámých odpovídá přímce v rovině. Jedna netriviální lineární rovnice o třech neznámých odpovídá rovině v tří-dimenzionálním prostoru. Na základě analogie můžeme tvrdit, že jedna netriviální rovnice o čtyřech neznámých odpovídá 3-dimenzionálnímu rovnému útvaru ve 4-dimenzionálním prostoru. A s ještě větší odvahou můžeme prohlásit, že množina všech řešení jedné netriviální rovnice o n neznámých odpovídá nějakému $(n-1)$-dimenzionálnímu rovnému útvaru umístěnému v n-dimenzionálním prostoru. Takovému útvaru říkáme *nadrovina* v n-dimenzionálním prostoru. Množina všech řešení soustavy lineárních rovnic o n neznámých pak odpovídá průniku nějakých nadrovin v n-dimenzionálním prostoru.

2.5.2. *Sloupcový geometrický pohled.* Ukážeme si ještě jeden geometrický pohled na soustavy lineárních rovnic. Tento pohled bude v dalším textu nabývat na větším významu než původní pohled přes rovnice přímek, rovin, atd. Vezměme si jednoduchou soustavu dvou rovnic o dvou neznámých

$$\begin{aligned} -x_1 + 3x_2 &= 1 \\ 2x_1 - x_2 &= 3 \ . \end{aligned}$$

Rozšířená matice této soustavy je

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

Při řešení soustavy hledáme hodnoty proměnných x_1, x_2 tak, aby platila rovnost dvousložkových vektorů

$$\begin{pmatrix} -x_1 + 3x_2 \\ 2x_1 - x_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \end{pmatrix} \ .$$

Všimněme si, že v prvním sloupci matice soustavy jsou koeficienty u proměnné x_1 a ve druhém sloupci jsou koeficienty u proměnné x_2. Těmto vektorům říkáme

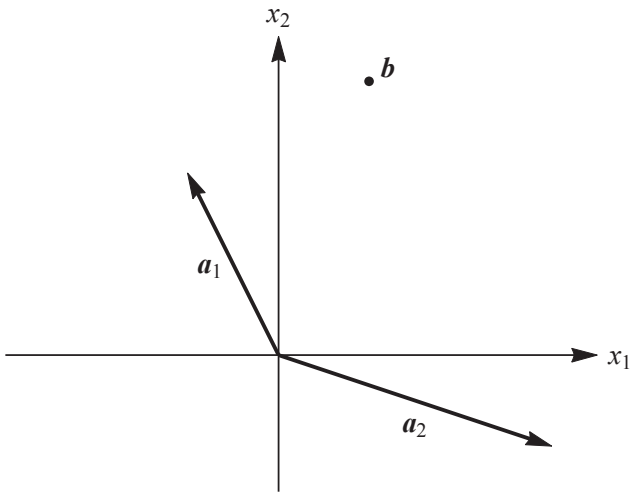
sloupcové vektory matice soustavy. Levou stranu poslední rovnosti můžeme pomocí sloupcových vektorů přepsat ve tvaru

$$\begin{pmatrix} -x_1+3x_2 \\ 2x_1-x_2 \end{pmatrix} = x_1\begin{pmatrix} -1 \\ 2 \end{pmatrix} + x_2\begin{pmatrix} 3 \\ -1 \end{pmatrix}$$

a celou soustavu jako

$$x_1\begin{pmatrix} -1 \\ 2 \end{pmatrix} + x_2\begin{pmatrix} 3 \\ -1 \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \end{pmatrix} \ .$$

Na obrázku je geometrické znázornění této soustavy. Máme dány dva vektory $\mathbf{a}_1 = (-1,2)^T$ a $\mathbf{a}_2 = (3,-1)^T$, a hledáme nějaké jejich násobky tak, abychom se součtem těchto násobků „trefili“ do bodu se souřadnicemi $(1,3)^T$, což je aritmetický vektor $\mathbf{b}$ pravých stran soustavy.



Obrázek 36. Sloupcový pohled na soustavu o dvou neznámých

Na dalším obrázku pak vidíme „geometrické“ řešení této soustavy.

Platí totiž

$$2\begin{pmatrix} -1 \\ 2 \end{pmatrix} + 1\begin{pmatrix} 3 \\ -1 \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \end{pmatrix} \ ,$$

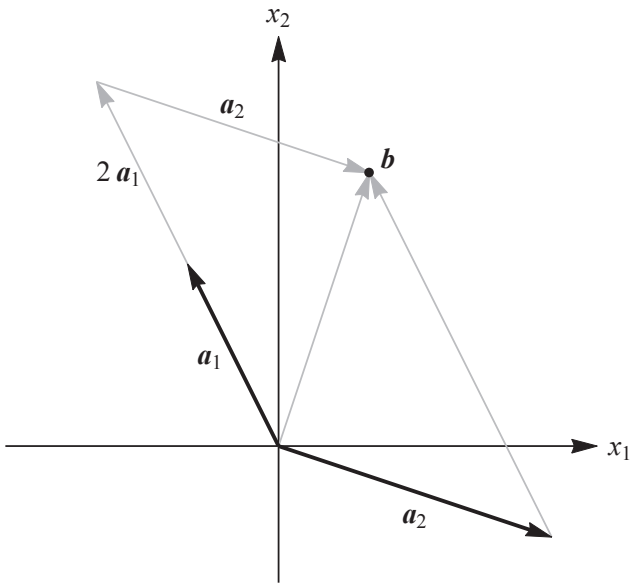
řešením je aritmetický vektor $(2,1)^T$.

Ze sloupcového pohledu na tuto soustavu můžeme získat ještě více. Levá strana soustavy může nabývat hodnot

$$\left\{ x_1\begin{pmatrix} -1 \\ 2 \end{pmatrix} + x_2\begin{pmatrix} 3 \\ -1 \end{pmatrix} : x_1, x_2 \in \mathbb{R} \right\} \ .$$

To je parametrické vyjádření roviny. Vhodnou volbou násobků vektorů $\mathbf{a}_1 = (-1,2)^T$ a $\mathbf{a}_2 = (3,-1)^T$ se tak můžeme trefit do jakéhokoliv bodu roviny a navíc právě jedním způsobem. Tento geometrický poznatek můžeme zformulovat také tak, že soustava

$$\left(\begin{array}{cc|c} -1 & 3 & b_1 \\ 2 & -1 & b_2 \end{array}\right) \ .$$



OBRÁZEK 37. Geometrické řešení soustavy o dvou neznámých

je řešitelná pro jakoukoliv pravou stranu $\mathbf{b} = (b_1, b_2)^T$ a řešení je vždy určené jednoznačně.

Ještě zajímavější je případ tří lineárních rovnic o dvou neznámých, např.

$$\begin{aligned} x_1 + 3x_2 &= -5 \\ 2x_1 + 2x_2 &= -2 \\ 3x_1 + x_2 &= 1 \ . \end{aligned}$$

Rozšířená matice této soustavy je

$$\left(\begin{array}{cc|c} 1 & 3 & -5 \\ 2 & 2 & -2 \\ 3 & 1 & 1 \end{array}\right) \ .$$

Soustavu můžeme pomocí sloupcových vektorů rozšířené matice zapsat jako

$$x_1 \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + x_2 \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} = \begin{pmatrix} -5 \\ -2 \\ 1 \end{pmatrix} \ .$$

Tentokrát hledáme koeficienty x_1 a x_2, kterými je třeba vynásobit sloupcové vektory $\mathbf{a}_1 = (1, 2, 1)^T$ a $\mathbf{a}_2 = (3, 2, 1)^T$ tak, abychom se aritmetickým vektorem $x_1\mathbf{a}_1 + x_2\mathbf{a}_2$ trefili do bodu se souřadnicemi $(-5, -2, 1)^T$.

Množina

$$\{x_1\mathbf{a}_1 + x_2\mathbf{a}_2 : x_1, x_2 \in \mathbb{R}\}$$

je parametrické vyjádření roviny v trojrozměrném prostoru, která prochází bodem $(0, 0, 0)^T$, tj. počátkem souřadnic. Můžeme se proto trefit pouze do bodů, které leží v této rovině. Pokud vektor $\mathbf{b} = (b_1, b_2, b_3)^T$ v rovině $\{x_1\mathbf{a}_1 + x_2\mathbf{a}_2 : x_1, x_2 \in \mathbb{R}\}$

neleží, soustava

$$\left(\begin{array}{cc|c} 1 & 3 & b_1 \\ 2 & 2 & b_2 \\ 3 & 1 & b_3 \end{array}\right)$$

není řešitelná. Pokud vektor $\mathbf{b}$ v této rovině leží, soustava má řešení a navíc je určené jednoznačně. Soustava je tedy řešitelná právě když vektor pravých stran $\mathbf{b}$ leží v rovině s parametrickým vyjádřením $\{x_1\mathbf{a}_1 + x_2\mathbf{a}_2 : x_1, x_2 \in \mathbb{R}\}$.

V našem konkrétním případě vektoru $(-5, -2, 1)^T$ platí

$$1 \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} - 2 \cdot \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} = \begin{pmatrix} -5 \\ -2 \\ 1 \end{pmatrix} \ ,$$

což dokazuje nejen to, že soustava s pravou stranou $(-5, -2, 1)^T$ je řešitelná, ale také, že vektor $(-5, -2, 1)^T$ leží v rovině

$$\left\{ x_1 \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + x_2 \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} : x_1, x_2 \in \mathbb{R} \right\} \ .$$

Abychom zjednodušili další vyjadřování, zavedeme následující **zcela základní** definici. Jde o jednu z nejdůležitějších definic celého dvousemestrálního kurzu lineární algebry.

Definice 2.18. Jsou-li $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ m-složkové vektory a $a_1, a_2, \ldots, a_n$ reálná čísla, pak definujeme *lineární kombinaci* vektorů $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ s koeficienty $a_1, a_2, \ldots, a_n$ jako m-složkový vektor

$$a_1\mathbf{u}_1 + a_2\mathbf{u}_2 + \cdots + a_n\mathbf{u}_n \ .$$

Soustavu

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

pak můžeme přepsat do tvaru

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

Na levé straně máme lineární kombinaci sloupcových vektorů matice soustavy s neznámými koeficienty $x_1, x_2, \ldots, x_n$. Soustava je řešitelná právě když lze sloupec pravých stran vyjádřit jako lineární kombinaci sloupcových vektorů matice soustavy. Vektory koeficientů každé takové lineární kombinace pak tvoří množinu všech řešení soustavy.

2.5.3. *Význam obou geometrických pohledů na soustavu lineárních rovnic.* Řádkový pohled nám dává představu, jak může vypadat množina všech řešení soustavy lineárních rovnic o n-neznámých. Množina všech řešení jedné rovnice je nadrovina (za předpokladu, že aspoň jeden z koeficientů u neznámých je nenulový) v n-dimenzionálním prostoru. Množina všech řešení soustavy m-lineárních rovnic o n neznámých je pak průnikem nějakých nadrovin.

Naproti tomu sloupcový pohled nám dává geometrickou představu, kdy je soustava lineárních rovnic $A\mathbf{x} = \mathbf{b}$ řešitelná. Je to právě když lze sloupcový vektor pravých stran $\mathbf{b}$ vyjádřit jako lineární kombinaci sloupcových vektorů matice soustavy A. Geometrický význam této podmínky v případě soustavy dvou nebo tří rovnic o dvou neznámých jsme si ukázali výše.

2.6. **Praktické problémy při numerickém řešení velkých soustav rovnic.**

2.6.1. *Numerická stabilita.* Při řešení soustav lineárních rovnic na počítači často reprezentujeme reálná čísla s nějakou předem určenou přesností. Takových čísel, které můžeme reprezentovat v počítači pomocí plovoucí desetinné čárky, je ale pouze konečně mnoho, jakkoliv obrovský ten počet je. Může se přihodit, že výsledek nějaké aritmetické operace se dvěma reprezentovatelnými čísly už reprezentovat nejde a počítač jej musí zaokrouhlit.

Problémem je, zaokrouhlování koeficientů není ekvivalentní úprava soustavy. Na konci algoritmu tak sice *dostaneme přesné řešení, ale jiné soustavy.* Otázkou obrovské důležitosti je jak moc se liší přesné řešení soustavy pozměněné zaokrouhlováním od přesného řešení původní soustavy. Těmito otázkami se mimo jiné zabývá *numerická lineární algebra.* Základní poznatek zní, 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

$$\left(\begin{array}{cc|c} -10^{-4} & 1 & 2 \\ 1 & 1 & 3 \end{array}\right),$$

jejímž přesným řešením je

$$\left(\frac{1}{1{,}0001}, \frac{2{,}0003}{1{,}0001}\right)^T .$$

Pokud použijeme aritmetiku s třemi platnými ciframi, Gaussova eliminace nám dá

$$\left(\begin{array}{cc|c} -10^{-4} & 1 & 2 \\ 1 & 1 & 3 \end{array}\right) \sim \left(\begin{array}{cc|c} -10^{-4} & 1 & 2 \\ 0 & 10^4 & 2 \cdot 10^4 \end{array}\right)$$

a zpětnou substitucí dostaneme řešení $(0, 2)^T$, 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 koeficientem 1 u proměnné x_2 a pravou stranou 3 ve druhé rovnici.

Tomuto problému lze někdy předejít tak, že vždy před eliminací jedné proměnné prohodíme řádky tak, aby pivot byl co největší (v absolutní hodnotě). Tomu se říká *částečná pivotace.* V našem příkladu bychom napřed prohodili oba řádky a teprve pak eliminovali první sloupec:

$$\left(\begin{array}{cc|c} -10^{-4} & 1 & 2 \\ 1 & 1 & 3 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 1 & 3 \\ -10^{-4} & 1 & 2 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 1 & 3 \\ 0 & 1 & 2 \end{array}\right) .$$

Dostaneme tak řešení $(1,2)^T$, které se rovná správnému řešení zaokrouhlenému na tři desetinná místa. Lépe to se zaokrouhlováním na tři desetinná místa nejde.

Částečná pivotace ale nezamezí všem problémům s numerickou stabilitou. Příkladem může být soustava

$$\left(\begin{array}{cc|c} -10 & 10^5 & 2\cdot 10^5 \\ 1 & 1 & 3 \end{array}\right),$$

která vznikne z předchozí vynásobením první rovnice číslem 10^5. Řešení při použití aritmetiky se třemi platnými ciframi vyjde opět $(0,2)^T$ a částečná pivotace tomuto problému nezamezí (řádky jsou již od začátku ve správném pořadí). U tohoto příkladu je problém ve značném rozdílu ve velikosti čísel v prvním řádku a druhém řádku.

Těmto i dalším typům problémů lze zamezit *úplnou pivotací*, při níž prohodíme před každým cyklem eliminace zbylé 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. Místo první soustavy bychom tak řešili soustavu

$$\left(\begin{array}{cc|c} 1 & -10^{-4} & 2 \\ 1 & 1 & 3 \end{array}\right).$$

Gaussova eliminace se zaokrouhlováním na tři platná místa by proběhla následovně:

$$\left(\begin{array}{cc|c} 1 & -10^{-4} & 2 \\ 1 & 1 & 3 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & -10^{-4} & 2 \\ 0 & 1 & 1 \end{array}\right)$$

a zpětnou substitucí bychom dostali $x_1 = 1$ (prohazovali jsme sloupce, tak musíme také prohodit proměnné) a $x_2 = 2$, což je tak blízko přesnému řešení původní soustavy jak je to jenom při zaokrouhlování na tři platná místa možné.

Prohledávání matice v každém cyklu tak, aby byl pivot co největší, je časově hodně náročné, proto se mu algoritmy pro numerické řešení velkých soustav lineárních rovnic snaží vyhnout, pokud to jenom trochu lze. V takovém případě se v eliminační fázi používají jiné algoritmy, které nejsou založené na Gaussově eliminaci, jsou ale numericky stabilnější. Jeden z nich si ukážeme na konci prvního semestru.

2.6.2. *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 $(1,-1)^T$.

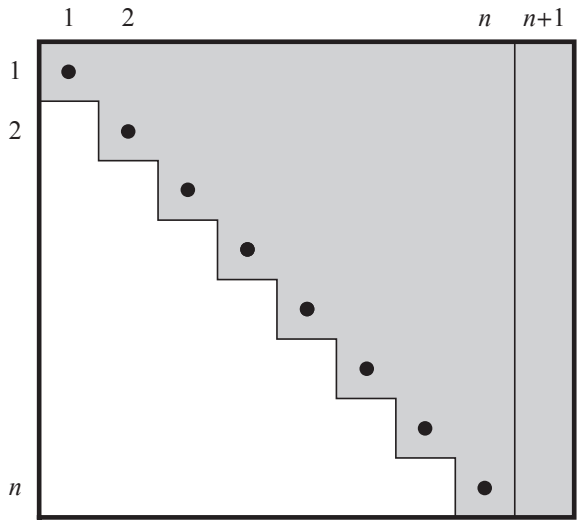
Pokud číslo 0,067 jen nepatrně změníme na hodnotu 0,066, řešení se změní na $(-666,\, 834)^T$. Důvodem tohoto drastického rozdílu je, že přímky určené rovnicemi jsou téměř rovnoběžné, takže malá změna jedné z nich může posunout průnik daleko od původního. V našem příkladu se směrnice obou přímek liší zhruba o $3{,}6\cdot 10^{-6}$.

Soustavám, jejichž 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 matematický model, který vedl k soustavě, navrhnout jiný experiment, apod., abychom se vyhnuli špatně podmíněným soustavám.

2.7. **Jak dlouho to bude trvat.** Máme-li řešit velkou soustavu lineárních rovnic na počítači, potřebujeme nějakou představu, jak dlouho bude výpočet trvat – vteřinu, den, měsíc, do vánoc? Doba výpočtu samozřejmě závisí na konstrukci počítače. Nicméně jakousi představu nám může dát odhad počtu aritmetických operací, které je třeba při výpočtu provést.

Počet operací se obvykle udává v jednotce *flop*, což je zkratka od *floating-point operation* používaná i v češtině. Každá z operací sčítání, odčítání, násobení a dělení dvou čísel představuje jeden flop. My budeme raději používat termín *aritmetická operace*. Případné prohazování řádků nepočítáme.

Pro zjednodušení se omezíme na řešení soustav n lineárních rovnic o n neznámých, které mají jednoznačné řešení. To znamená, že množina všech řešení nemá žádný volný parametr, neboli že každá proměnná je bázová. Po Gaussově eliminaci rozšířené matice $(A \mid \mathbf{b})$ tak vyjde v každém řádku jeden pivot, a protože je soustava řešitelná, není sloupec pravých stran bázový. Žádný pivot tedy neleží v $(n+1)$-ním sloupci. Pivoty jsou proto v matici v odstupňovaném tvaru na místech s indexy 11, 22, 33, ..., nn. Ve skutečnosti toto je případ, který vyžaduje nejvíce aritmetických operací.



Obrázek 38. Rozšířená matice soustavy po Gaussově eliminaci

Zvlášť spočteme počet aritmetických operací nutných pro Gaussovu eliminaci a zvlášť pro zpětnou substituci. Důvod pro toto rozdělení uvidíme později. Některé kroky výpočtu si můžete doplnit jako cvičení.

Při Gaussově eliminaci používáme aritmetické operace pouze v kroku 3. Spočítáme, kolik aritmetických operací je maximálně třeba pro krok 3., tj. pro jeden cyklus Gaussovy eliminace.

Chceme-li vynulovat první prvek ve druhém řádku, musíme napřed spočítat podíl a_{21}/a_{11}, to je jedno dělení. Pak musíme spočítat $n-1$ součinů $(a_{21}/a_{11})a_{1i}$ pro $i = 2, 3, \ldots, n$ a jeden součin $(a_{21}/a_{11})b_1$ pro pravou stranu. To je celkem nejvýše $n+1$ násobení/dělení. Může jich být méně, pokud je některé z čísel a_{1i}nebo b_i rovné 0.

Nakonec spočteme $n-1$ součtů $-(a_{21}/a_{11})a_{1i}+a_{2i}$ pro $i=2,3,\dots,n$. Pro $i=1$ jej počítat nemusíme, protože předem víme, že vyjde 0. Nakonec přidáme ještě jeden součet $-(a_{21}/a_{11})b_1+b_2$ na pravé straně. Celkem potřebujeme nejvýše n sčítání/odčítání.

Dohromady vynulování prvku a_{21} pod pivotem na místě $(1,1)$ v matici typu $n\times(n+1)$ vyžaduje nejvýše $n+1$ násobení/dělení a n sčítání/odčítání. Je-li $a_{21}=0$, nemusíme tyto operace vůbec provádět.

Musíme vynulovat všech $n-1$ prvků v prvním sloupci, to znamená, že na třetí krok Gaussovy eliminace potřebujeme nejvýše

$$(n-1)(n+1)=n^2-1 \text{ násobení/dělení a } (n-1)n=n^2-n \text{ sčítání/odčítání .}$$

Druhý cyklus Gaussovy eliminace provádíme s maticí bez prvního řádku a nemusíme se starat o první sloupec, který už je celý nulový. Potřebujeme na něj nejvýše

$$(n-1)^2-1 \text{ násobení/dělení a } (n-1)^2-(n-1) \text{ sčítání/odčítání .}$$

Ve třetím cyklu je to nejvýše

$$(n-2)^2-1 \text{ násobení/dělení a } (n-2)^2-(n-2) \text{ sčítání/odčítání, atd.}$$

Poslední cyklus Gaussovy eliminace nuluje prvek pod pivotem na místě $(n-1,n-1)$ a stojí nás nejvýše

$$2^2-1 \text{ násobení/dělení a } 2^2-2 \text{ sčítání/odčítání .}$$

Dohromady tak celá Gaussova eliminace vyžaduje nejvýše

$$\sum_{k=2}^{n} k^2-(n-1) \text{ násobení/dělení .}$$

Nyní využijeme vzorečky, jejich důkaz (matematickou indukcí) je ponechán jako cvičení:

$$\sum_{k=1}^{n} k^2=\frac{n^3}{3}+\frac{n^2}{2}+\frac{n}{6} \quad \text{a} \quad \sum_{k=1}^{n} k=\frac{n^2}{2}+\frac{n}{2} \ .$$

Gaussova eliminace vyžaduje nejvýše

$$\sum_{k=2}^{n} k^2-(n-1)=\frac{n^3}{3}+\frac{n^2}{2}+\frac{n}{6}-1-(n-1)=\frac{n^3}{3}+\frac{n^2}{2}-\frac{5n}{6} \text{ násobení/dělení .}$$

Počet operací $+/-$ je pak nejvýše

$$\sum_{k=2}^{n} k^2-\sum_{k=2}^{n} k=\frac{n^3}{3}+\frac{n^2}{2}+\frac{n}{6}-1-\left(\frac{n^2}{2}+\frac{n}{2}-1\right)=\frac{n^3}{3}-\frac{n}{3} \ .$$

Výpočet náročnosti Gaussovy eliminace si shrneme do následujcího tvrzení.

Tvrzení 2.19. *Gaussova eliminace rozšířené matice soustavy n lineárních rovnic o n neznámých vyžaduje nejvýše*

$$\frac{2n^3}{3}+\frac{n^2}{2}-\frac{7n}{6}\approx\frac{2n^3}{3}$$

aritmetických operací.

Pro velká n je první člen dominantní. Gaussova eliminace soustavy s 10000 rovnicemi o 10000 neznámých tak vyžaduje zhruba $(2/3)10^{12} \approx (2/3)2^{40}$ aritmetických operací (neboť $10^3 \approx 2^{10}$).

Pro odhad náročnosti zpětné substituce si připomeňme tvar soustavy po proběhlé Gaussově eliminaci v případě, že pivoty jsou na místech 11, 22, ..., nn:

$$\begin{aligned} c_{11}x_1 + c_{12}x_2 + c_{13}x_3 + \cdots + c_{1,n-1}x_{n-1} + c_{1n}x_n &= d_1 \\ c_{22}x_2 + c_{23}x_3 + \cdots + c_{2,n-1}x_{n-1} + c_{2n}x_n &= d_2 \\ &\vdots \\ c_{n-1,n-1}x_{n-1} + c_{n-1,n}x_n &= d_{n-1} \\ c_{n,n}x_n &= d_n \ . \end{aligned}$$

Při zpětné substituci tak postupně dopočítáváme

$$\begin{aligned} x_n &= c_{nn}^{-1}d_n \\ x_{n-1} &= c_{n-1,n-1}^{-1}(d_{n-1} - c_{n-1,n}x_n) \\ &\vdots \\ x_2 &= c_{22}^{-1}(d_2 - c_{23}x_3 - \cdots - c_{2,n-1}x_{n-1} - c_{2n}x_n) \\ x_1 &= c_{11}^{-1}(d_1 - c_{12}x_2 - c_{13}x_3 - \cdots - c_{1,n-1}x_{n-1} - c_{1n}x_n) \end{aligned}$$

a to vyžaduje

$$\sum_{k=1}^{n} k = \frac{n^2}{2} + \frac{n}{2} \quad \text{násobení/dělení a} \quad \sum_{k=1}^{n-1} = \frac{n^2}{2} - \frac{n}{2} \quad \text{sčítání/odčítání} \ .$$

Tvrzení 2.20. *Zpětná substituce vyžaduje při řešení soustavy n lineárních rovnic o n neznámých nejvýše n^2 aritmetických operací.*

Nyní je vidět, že pro velká n je počet operací nutných pro zpětnou substituci zanedbatelný vzhledem k počtu operací nutných pro Gaussovu eliminaci.

Cvičení

1. Najděte kvadratický polynom $p(x) = ax^2 + bx + c$, pro který platí $p(0) = 3$, $p(1) = 1$, $p(2) = 2$.

2. Dokažte, že prohození dvou řádků matice lze docílit zbylými dvěmi elementárními řádkovými úpravami.

3. Matematickou indukcí podle n dokažte, že pro každé číslo $n \geq 1$ platí

$$\sum_{k=1}^{n} k = 1 + 2 + 3 + \cdots + n = \frac{n^2}{2} + \frac{n}{2} \ .$$

4. Matematickou indukcí podle n dokažte, že pro každé číslo $n \geq 1$ platí

$$\sum_{k=1}^{n} k^2 = 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6} \ .$$

5. Spočtěte, kolik aritmetických operací je nejvýše třeba pro Gaussovu eliminaci soustavy m rovnic o n neznámých pro libovolná m, n.

6. Spočtěte, kolik aritmetických operací je nejvýše třeba pro zpětnou substituci při řešení soustavy m rovnic o n neznámých pro libovolná m, n.

Shrnutí druhé kapitoly

(1) *Soustava m lineárních rovnic o n neznámých* s reálnými koeficienty je soustava

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

(2) Soustavy lineárních rovnic řešíme pomocí *ekvivalentních úprav*. To jsou úpravy, které nemění množinu všech řešení soustavy.

(3) Vystačíme s ekvivaletními úpravami tří typů, kterým říkáme *elementární úpravy*:
   (i) prohození dvou rovnic,
   (ii) vynásobení nějaké rovnice **nenulovým** číslem t,
   (iii) přičtení t-násobku jedné rovnice k **jiné** rovnici.

(4) Každé řešení soustavy lineárních rovnic s n neznámými je uspořádaná n-tice $(x_1, x_2, \ldots, x_n)$ reálných čísel. Uspořádanou n-tici reálných čísel nazýváme *aritmetický vektor nad $\mathbb{R}$ s n složkami*. Aritmetické vektory chápeme jako sloupce čísel, kvůli úspoře místa je ale zapisujeme také $(x_1, x_2, \ldots, x_n)^T$. Množinu všech n-složkových aritmetických vektorů nad $\mathbb{R}$ označujeme $\mathbb{R}^n$, nazýváme ji také *reálný aritmetický prostor dimenze n*.

(5) Aritmetické vektory *sčítáme po složkách*

$$(x_1, x_2, \ldots, x_n)^T + (y_1, y_2, \ldots, y_n)^T = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)^T$$

a *násobíme reálným číslem* také po složkách

$$t(x_1, x_2, \ldots, x_n)^T = (tx_1, tx_2, \ldots, tx_n)^T \ .$$

(6) Postup při řešení soustavy lineárních rovnic zapisujeme přehledně pomocí matic. *Matice* nad $\mathbb{R}$ typu $m \times n$ je obdélníkové schéma reálných čísel s m řádky a n sloupci. Zapisujeme ji symbolicky $A = (a_{ij})_{m\times n}$, číslo a_{ij} je prvek matice v i-tém řádku a j-tém sloupci.

(7) Soustava lineárních rovnic z bodu (1) určuje dvě matice. *Matice soustavy* je matice koeficientů u neznámých:

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

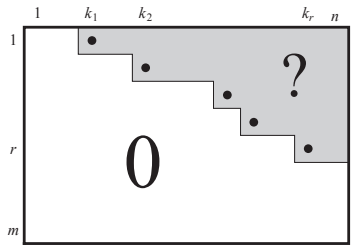
(8) Přidáme-li k matici soustavy *vektor pravých stran* $(b_1, b_2, \ldots, b_m)^T$, dostaneme *rozšířenou matici soustavy*

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

(9) Elementárním úpravám soustavy lineárních rovnic odpovídají *elementární řádkové úpravy* rozšířené matice soustavy. Definujeme je ale pro jakoukoliv matici A a jsou to
   (i) prohození dvou řádků matice,
   (ii) vynásobení jednoho z řádků matice **nenulovým** číslem,
   (iii) přičtení libovolného násobku jednoho řádku k **jinému** řádku.

(10) *Gaussova eliminace* je postup, jak každou matici převést do odstupňovaného tvaru.

(11) Matice $C = (c_{ij})_{m\times n}$ je v odstupňovaném tvaru, pokud v každém nenulovém řádku matice C je na počátku (tj. zleva) více nul, než na počátku řádku nad ním. Grafické znázornění matice v odstupňovaném tvaru je



Formálně definujeme, že matice $C = (c_{ij})_{m\times n}$ je v *řádkově odstupňovaném tvaru*, pokud existuje celé číslo $r \in \{0, 1, \dots, m\}$ takové, že řádky $r+1, \dots, m$ jsou nulové, řádky $1, \dots, r$ jsou nenulové, a platí $k_1 < k_2 < \cdots < k_r$, kde k_i je index sloupce, ve kterém je první nenulové číslo v i-tém řádku.

Prvkům c_{i,k_i}, $i = 1, 2, \dots, r$, tj. prvním nenulovým prvkům v jednotlivých řádcích, říkáme *pivoty*.

(12) Gaussova eliminace spočívá v následujících krocích:
   1. Najdeme první nenulový sloupec, jeho index označíme k_1. Pokud takový sloupec neexistuje, je matice A v řádkově odstupňovaném tvaru (neboť je nulová), a jsme hotovi.
   2. Pokud je $a_{1k_1} = 0$, prohodíme první řádek s libovolným řádkem i, ve kterém je $a_{ik_1} \neq 0$.
   3. Pro každé $i = 2, 3, \dots, m$ přičteme $(-a_{ik_1}/a_{1k_1})$-násobek prvního řádku k i-tému řádku.
   4. Postup opakujeme s maticí bez prvního řádku.

(13) Gaussovo eliminací převedeme každou matici $A = (a_{ij})_{m\times n}$ do odstupňovaného tvaru $C = (c_{ij})_{m\times n}$. Různým použitím Gaussovy eliminace můžeme dostat různé odstupňované tvary, neboť v kroku 2. máme možnost volit index i. Bez důkazu jsme si řekli, že počet nenulových řádků r a indexy $k_1 < k_2 < \cdots < k_r$ z formální definice odstupňovaného tavru vyjdou vždy stejně, jsou určené jednoznačně maticí A.

(14) Číslo r nazýváme *hodnost matice* A a značíme je $\operatorname{rank}(A)$. Sloupce s indexy $k_1, k_2, \dots, k_r$ nazýváme *bázové sloupce* matice A.

(15) Soustavu lineárních rovnic řešíme ve třech krocích. *Eliminační fáze* spočívá v převedení rozšířené matice soustavy do odstupňovaného tvaru Gaussovo eliminací. Je-li sloupec pravých stran bázový sloupec rozšířené matice soustavy, nemá soustava řešení.

(16) Pokud sloupec pravých stran není bázový, následuje *zpětná substituce*. Napřed určíme *bázové proměnné* $x_{k_1}, x_{k_2}, \dots, x_{k_r}$, zbývající proměnné jsou *volné proměnné* a jejich hodnoty můžeme zvolit libovolně. Poté odzadu postupně spočteme hodnoty bázových proměnných $x_{k_r}, x_{k_{r-1}}, \dots, x_1$ pomocí volných proměnných.

(17) Nakonec zapíšeme množinu všech řešení soustavy v *parametrickém tvaru*

$$\left\{ \mathbf{u} + \sum_{p \in P} t_p \mathbf{v}_p : \ t_p \in \mathbb{R} \ \text{ pro každé } \ p \in P \right\}$$

pro vhodné n-složkové aritmetické vektory $\mathbf{u}$ a $\mathbf{v}_p$, $p \in P$, kde P je množina indexů volných proměnných-parametrů. Každé volné proměnné x_p odpovídá jeden vektor $\mathbf{v}_p$.

(18) Řešení soustavy lineárních rovnic lze chápat geometricky dvěma různými způsoby. Množina všech řešení soustavy je průnik množin řešení jednotlivých rovnic. Množina všech řešení jedné lineární rovnice o n neznámých je *nadrovina*, tj. „rovný útvar“ dimenze $n-1$ v prostoru $\mathbb{R}^n$ dimenze n. To v případě, že aspoň jeden z koeficientů u neznámých je nenulový. V triviálním případě, kdy jsou všechny koeficienty u neznámých nulové, je množina všech řešení buď prázdná nebo celý prostor $\mathbb{R}^n$. Pokud soustava lineárních rovnic obsahuje aspoň jednu netriviální rovnici, je množina jejích řešení průnikem nadrovin.

(19) Pro sloupcový pohled na řešení soustavy lineárních rovnic potřebujeme klíčový pojem lineární kombinace. Jsou-li $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n$ aritmetické vektory s m složkami a $a_1, a_2, \dots, a_n$ reálná čísla, pak *lineární kombinací vektorů* $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n$ *s koeficienty* $a_1, a_2, \dots, a_n$ nazýváme vektor

$$a_1\mathbf{u}_1 + a_2\mathbf{u}_2 + \cdots + a_n\mathbf{u}_n \in \mathbf{T}^m \ .$$

(20) Řešení soustavy lineární rovnic $(A|\mathbf{b})$ spočívá v nalezení všech možných lineárních kombinací sloupcových vektorů $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n$ matice soustavy A, které se rovnají vektoru pravých stran $\mathbf{b}$. Soustava je tedy řešitelná právě když sloupec pravých stran lze vyjádřit jako lineární kombinaci sloupcových vektorů matice soustavy.

(21) Řešíme-li soustavu lineárních rovnic na počítači, je třeba mít na paměti, že v počítači lze uložit přesně pouze konečně mnoho čísel. Může se stát, že při některých krocích výpočtu je nutné výsledky zaokrouhlit, aby se do počítače „vešly“. Zaokrouhlování koeficientů ale není ekvivalentní úprava. Počítač nám sice dá nějaké řešení, je to ale řešení jiné soustavy. *Numerická stabilita*, tj. vztah mezi přesným řešením a řešením získaným na počítači, je základním problémem *numerické lineární algebry*.

(22) Některé soustavy mají jinou nepříjemnou vlastnost - drobná změna některého koeficientu nebo prvku na pravé straně způsobí velkou změnu řešení. Takovým soustavám se říká *špatně podmíněné*. Pokud koeficienty soustavy získáváme měřením, tak se na řešení špatně podmíněné soustavy nelze vůbec spolehnout. Tento problém nelze odstranit ani numericky velmi stabilním algoritmem.

(23) Pro hrubý odhad doby, jakou bude trvat řešení velké soustavy lineárních rovnic o mnoha neznámých na počítači, je dobré odhadnout počet aritmetických operací, které výpočet vyžaduje. Gaussova eliminace soustavy n

lineárních rovnic o n neznámých potřebuje nejvýše $(2/3)n^3$ operací. Zpětná substituce jich potřebuje nejvýše n^2. Pro velká n je časová náročnost zpětné substituce zanedbatelná.

Klíčové znalosti z druhé kapitoly nezbytné pro průběžné sledování přednášek s pochopením

(1) Aritmetické vektory a počítání s nimi.
(2) Pojem lineární kombinace vektorů.
(3) Matice, zejména vědět že prvek a_{ij} leží v i-tém řádku a j-tém sloupci.
(4) Definice řádkově odstupňovaného tvaru matice.
(5) Fakt, že Gaussova eliminace převede každou matici do řádkově odstupňovaného tvaru.
(6) Umět řešit soustavy lineárních rovnic a vyjádřit množinu všech řešení v parametrickém tvaru.
(7) Rozumět řádkovému a sloupcovému pohledu na řešení soustavy lineárních rovnic.

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. Pomocí detailní analýzy řešení jednoduchých rovnic si uvědomíme, jaké vlastnosti počítání s reálnými čísly nám umožňují takové rovnice řešit.

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 oběma 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

$$(x + 11) + (-11) = 18 + (-11) \ .$$

Dalším krokem je přezávorkování levé strany a výpočet součtu na pravé straně:

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

Teď můžeme závorku vypočítat:

$$x + 0 = 7 \ .$$

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

$$x = 7 \ .$$

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. Sčítání a násobení je binární operací na množině T. Binární se rozumí jakékoliv zobrazení, které každé uspořádané dvojici prvků z T jednoznačně přiřadí prvek T.

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 se od předchozích liší v tom, 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 $a \cdot x = b$, například $3 \cdot x = 12$. Postup řešení je následující.

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

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 soustavy lineárních rovnic používáme ještě dvě další vlastnosti. Ty lze vidět například z úprav, které automaticky používáme, přičítáme-li 2-násobek rovnice $x+3y = 10$ k rovnici $(-2)x+4y = 15$. V úpravách již využíváme (S1) a (N1), takže nepíšeme závorky.

$$\begin{aligned} 2(x+3y)+(-2)x+4y &= 2\cdot 10+15\\ 2x+2\cdot 3y+(-2)x+4y &= 35\\ 2x+6y+(-2)x+4y &= 35\\ 2x+(-2)x+6y+4y &= 35\\ (2+(-2))x+(6+4)y &= 35\\ 0x+10y &= 35\\ 0+10y &= 35\\ 10y &= 35 \ . \end{aligned}$$

Kromě již formulovaných vlastností jsme využili tyto:

(D) („oboustranná distributivita“) Pro libovolná čísla $a, b, c \in \mathbb{R}$ platí

$$a \cdot (b+c) = a \cdot b + a \cdot c \quad \text{a} \quad (b+c) \cdot a = b \cdot a + c \cdot a \ .$$

(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 tělesa je těleso kvaternionů, o kterém se zmíníme na konci kapitoly.

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 operaci* $\cdot$. V následujícím tvrzení ukážeme, že oba neutrální prvky jsou určené 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 jako je běžné u reálných čísel budeme součin $a \cdot b$ často zapisovat jako ab. Také budeme dodržovat konvenci, že násobení má přednost před sčítáním. Dále 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) $-a = (-1)a$ *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 dokázat.

(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 a axiomu (N4). Takže $0 = b$ podle bodu (4).

(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 bod (6).

(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 všech těles jsou ve cvičeních.

3.3. **Tělesa $\mathbb{Z}_p$.**

Důležitým příkladem těles jsou tělesa $\mathbb{Z}_p$, kde p je prvočíslo. Tato a jiná konečná tělesa se používají například v informatice při návrhu kódů, které umožňují spolehlivý přenos informace kanálem se šumem, nebo při návrhu rychlých algoritmů pro počítání s celočíselnými polynomy.

3.3.1. *Dělení se zbytkem.* Počítání v tělesech $\mathbb{Z}_p$ je založené na dělení se zbytkem. Následující tvrzení shrnuje to, co jste se naučili už na prvním stupni základní školy.

Tvrzení 3.4. *Pro každé přirozené číslo $n \in \mathbb{N}$ a každé celé číslo $a \in \mathbb{Z}$ existují jednoznačně určená čísla $q \in \mathbb{Z}$ a $r \in \{0, 1, 2, \dots, n-1\}$ taková, že platí*

$$a = nq + r \ .$$

Rovnost $a = nq + r$ můžeme také chápat jako zkoušku, kterou ověřujeme, že spočítaný celočíselný podíl a zbytek při dělení a číslem n jsou správně.

Příklad 3.5.

$$\begin{array}{rlll} 12 : 5 = 2, & \text{zbytek } 2, & \text{neboť} & 12 = 5 \cdot 2 + 2 \\ -32 : 7 = -5, & \text{zbytek } 3, & \text{neboť} & -32 = 7(-5) + 3 \\ 62 : 8 = 7, & \text{zbytek } 6, & \text{neboť} & 62 = 8 \cdot 7 + 6 \ . \end{array}$$

Tvrzení 3.4 dokazovat nebudeme. Z prvního stupně základní školy dokonce znáte algoritmus, jak čísla q a r spočítat. Pro nás bude důležité číslo r, kterému říkáme *zbytek při dělení čísla a číslem n*, a budeme jej označovat

$$a \bmod n \ .$$

3.3.2. *Modulární počítání.* Libovolná dvě celá čísla a, b můžeme sečíst a vynásobit *modulo* n:

$$a \oplus b = (a + b) \bmod n, \quad a \odot b = (a \cdot b) \bmod n \ .$$

Na levých stranách jsou nově definované operace modulárního sčítání a násobení, které definujeme, a na pravých stranách jsou běžné operace v $\mathbb{Z}$. Výsledkem operace $a \oplus b$ je zbytek při dělení běžného součtu $a + b$ číslem n. Podobně modulární součin $a \odot b$ je zbytek při dělení běžného součinu ab číslem n. Například při počítání *modulo* 5 platí

$$1 \oplus 4 = 0, \ 3 \oplus 4 = 2, \ 2 \odot 2 = 4, \ 2 \odot 3 = 1, \ 3 \odot 3 = 4, \ 7 \odot 8 = 1, \dots \ .$$

Zbytek při dělení číslem n je vždy v množině $\{0, 1, \dots, n-1\}$. Tuto „množinu možných zbytků při dělení číslem n“ budeme označovat $\mathbb{Z}_n$. Nadále budeme předpokládat $n \geq 2$, aby množina $\mathbb{Z}_n$ měla aspoň dva prvky.

Běžné sčítání celých čísel je komutativní, platí

$$a + b = b + a$$

pro libovolná dvě čísla $a, b \in \mathbb{Z}$. Proto se také rovnají zbytky při dělení obou čísel číslem $n \in \mathbb{N}$:

$$(a + b) \bmod n = (b + a) \bmod n \ ,$$

což dokazuje rovnost $a \oplus b = b \oplus a$. Sčítání modulo n je tedy komutativní. Zcela stejně ověříme komutativitu násobení modulo n.

Dokázat asociativitu obou operací je o něco složitější. Napřed si ukážeme jednoduché pomocné tvrzení, že při modulárním sčítání (nebo násobení) se výsledek nezmění, pokud kterýkoliv ze sčítanců (nebo činitelů) nahradíme číslem se stejným zbytkem modulo n.

Lemma 3.6. *Pro libovolné přirozené číslo n a celá čísla a, b, d taková, že $a \bmod n = d \bmod n$, platí při počítání modulo n rovnosti*

(1) $a \oplus b = d \oplus b$,
(2) $a \odot b = d \odot b$.

Důkaz. Protože modulární sčítání a násobení je definováno pomocí zbytků modulo n, označíme si $r = a \bmod n = d \bmod n$ a $s = c \bmod n$. Existují tedy celá čísla u, v, w, pro která platí

$$a = nu + r, \quad d = nw + r, \quad b = nv + s \ .$$

(1) Pak platí

$$a + b = (nu + r) + (nv + s) = n(u + v) + (r + s) \ .$$

Nyní najdeme zbytek $t \in \{0, 1, \ldots, n-1\}$ při dělení čísla $r + s$ číslem n. Pro zbytek t platí rovnost $(r + s) = nq + t$, kde q je nějaké celé číslo. Po dosazení do posledního výrazu předchozího výpočtu dostaneme

$$\begin{aligned} a + b &= n(u + v) + (r + s) = n(u + v) + (nq + t) \\ &= n(u + v + q) + t \ , \end{aligned}$$

což dokazuje, že $a \oplus b = (a + b) \bmod n = t$. Stejně tak z

$$\begin{aligned} d + b &= (nw + r) + (nv + s) = n(w + v) + (r + s) \\ &= n(w + v) + (nq + t) = n(w + v + q) + t \end{aligned}$$

plyne $d \oplus b = t$ a tedy $d \oplus b = t = a \oplus b$.

(2) V případě násobení označíme $t = (rs) \bmod n$, což znamená, že $rs = nq + t$ pro nějaké celé číslo q. Pak spočteme

$$\begin{aligned} ab &= (nu + r)(nv + s) = n^2uv + nus + nvr + rs \\ &= n(nuv + us + vr) + (nq + t) = n(nuv + us + vr + q) + t \end{aligned}$$

a tedy $a \odot b = (ab) \bmod n = t$. Rovněž

$$\begin{aligned} db &= (nw + r)(nv + s) = n(nwv + ws + rv) + (rs) \\ &= n(nwv + ws + rv + q) + t \ , \end{aligned}$$

což dokazuje rovnost $d \odot b = t = a \odot b$.

□

Lemma 3.6 můžeme použít ke dvěma různým účelům. Při složitějším výpočtu modulo n lze jakýkoliv sčítanec nebo činitel nahradit jeho zbytkem modulo n a výsledek se nezmění.

Příklad 3.7. Budeme počítat modulo 3:

$$(587 \odot 422) \oplus (724 \odot 128) = (2 \odot 2) \oplus (1 \odot 2) = 1 \oplus 2 = 0 \ .$$

Pokud stejný výpočet děláme modulo 7, dostaneme

$$(587 \odot 422) \oplus (724 \odot 128) = (6 \odot 2) \oplus (3 \odot 2) = 5 \oplus 6 = 4 \ .$$

Lemma 3.6 můžeme také použít k důkazu obecných vlastností počítání modulo n. Z definice $a \oplus b = (a + b) \bmod n$ totiž plyne, že obě čísla $a \oplus b = (a + b) \bmod n$ a $a + b$ (běžné sčítání) mají stejný zbytek modulo n. Pro libovolná tři celá čísla a, b, c proto platí

$$(a \oplus b) \oplus c = (a + b) \oplus c = ((a + b) + c) \bmod n \ ,$$

v druhé rovnosti jsme použili definici sčítání modulo n. Celý výpočet lze proto provést pomocí běžného sčítání celých čísel a teprve na konci spočítat zbytek modulo n. Stejně tak platí

$$a \oplus (b \oplus c) = a \oplus (b + c) = (a + (b + c)) \bmod n \ .$$

Vzhledem k tomu, že běžné sčítání celých čísel je asociativní, plyne odtud také asociativita modulárního sčítání:

$$(a \oplus b) \oplus c = a \oplus (b \oplus c) \ .$$

Zcela stejně ověříme asociativitu modulárního násobení:

$$(a \odot b) \odot c = ((ab)c) \bmod n = (a(bc)) \bmod n = a \odot (b \odot c)$$

a distributivitu:

$$a \odot (b \oplus c) = (a(b + c)) \bmod n = (ab + ac) \bmod n = (a \odot b) \oplus (a \odot c) \ .$$

Nulový prvek pro sčítání modulo n neexistuje. Přirozeným kandidátem je číslo 0, nicméně pro každé $a \in \mathbb{Z}$ platí

$$a \oplus 0 = (a + 0) \bmod n = a \bmod n \ \in \ \mathbb{Z}_n = \{0, 1, \ldots, n - 1\}$$

a odtud dostáváme, že $a \oplus 0 = a$ právě když $a = a \bmod n$ a to nastane právě když $a \in \mathbb{Z}_n$. Z analogického důvodu není ani číslo 1 jednotkovým prvkem pro násobení modulo n, nicméně pro každé $a \in \mathbb{Z}_n$ platí $a \odot 1 = a$.

Omezíme-li sčítání a násobení modulo n na prvky množiny $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, bude výsledek obou operací také v $\mathbb{Z}_n$. Sčítání a násobení modulo n jsou proto binární operace také na množině $\mathbb{Z}_n$. Právě jsme si ukázali, že pro každé $a \in \mathbb{Z}_n$ platí $a \oplus 0 = a = a \odot 1$, pro sčítání a násobení modulo n na množině $\mathbb{Z}_n$ nulový a jednotkový prvek existují. Zbývá vyjasnit existenci opačných a inverzních prvků.

Pro každý nenulový prvek $a \in \mathbb{Z}_n$ platí $n - a \in \mathbb{Z}_n$, a protože

$$a \oplus (n - a) = n \bmod n = 0 \ ,$$

je prvek $n - a$ opačný k prvku a. Vzhledem k tomu, že $0 \oplus 0 = 0$, je nulový prvek opačný k sobě samému. Opačný prvek proto existuje ke každému $a \in \mathbb{Z}_n$. Označíme jej $\ominus a$. Pro každé $a \in \mathbb{Z}_n$ ale platí rovnost $(\ominus a) \bmod n = (-a) \bmod n$. Podle lemma 3.6 tak můžeme při modulárním počítání také každý výskyt prvku $\ominus a$ nahradit běžným opačným prvkem $-a$ a výsledek se nezmění.

Příklad 3.8. Budeme počítat modulo 6:

$$321 \odot (\ominus 223) \ominus 115 = 321 \odot (-223) \oplus (\ominus 115) = 3 \odot 5 \oplus (-115) = 3 \oplus 5 = 2 \ .$$

Existence inverzních prvků k nenulovým prvkům v $\mathbb{Z}_n$ je složitější a budeme se jí podrobněji zabývat za chvilku. Dosavadní poznatky si shrneme v následujícím tvrzení.

Tvrzení 3.9. *Pro každé přirozené číslo $n \geq 2$ jsou operace sčítání a násobení modulo n binární operace na množině $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ a splňují všechny axiomy tělesa s výjimkou axiomu (N3) o existenci inverzního prvku ke každému nenulovému prvku $a \in \mathbb{Z}_n$.*

3.3.3. *Existence inverzních prvků v $\mathbb{Z}_n$.* Nadále budeme při počítání modulo n používat běžné označné operací $+$, $-$, $\cdot$, přičemž budeme $\cdot$ obvykle vynechávat. Skutečnost, že počítáme modulo n je dána sdělením, že počítáme v $\mathbb{Z}_n$.

Zkusíme zjistit, existuje-li v $\mathbb{Z}_3$ inverzní prvek k prvku 2. Uděláme to zkusmo, spočteme všechny součiny $2x$ pro $x \in \mathbb{Z}_3$.

x	0	1	2
$2x$	0	2	1

.

Zjistili jsme, že v $\mathbb{Z}_3$ je 2 inverzní prvek k 2. A protože v $\mathbb{Z}_3$ platí také $1 \cdot 1 = 1$ (což platí v každém $\mathbb{Z}_n$), našli jsme inverzní prvek ke každému nenulovému prvku $a \in \mathbb{Z}_3$. To znamená, že počítání v $\mathbb{Z}_3$ splňuje i axiom (N3) a $\mathbb{Z}_3$ je těleso.

Zkusíme stejným způsobem najít inverzní prvek ke 2 v $\mathbb{Z}_4$:

x	0	1	2	3
$2x$	0	2	0	2

.

K číslu 2 tedy v $\mathbb{Z}_4$ inverzní prvek neexistuje a $\mathbb{Z}_4$ proto není těleso. Jiný důvod, proč $\mathbb{Z}_4$ není těleso spočívá také v rovnosti $2 \cdot 2 = 0$, protože v libovolném tělese musí být součinn dvou nenulových prvků různý od 0 - viz vlastnost (6) v tvrzení 3.3. Na základě posledního argumentu můžeme ihned dokázat následující tvrzení.

Tvrzení 3.10. *Je-li $n \geq 2$ složené číslo, pak $\mathbb{Z}_n$ s operacemi sčítání a násobení modulo n není těleso.*

Důkaz. Protože předpokládáme, že n je složené číslo, můžeme jej napsat jako běžný součin $n = ab$, kde obě čísla a, b jsou kladná, nenulová, a menší než n. Patří proto do $\mathbb{Z}_n$. Pro jejich součin modulo n pak platí $ab = n \bmod n = 0$. Počítání v $\mathbb{Z}_n$ tak nemá vlastnost (6) v tvrzení 3.3, která musí platit v každém tělese, a proto $\mathbb{Z}_n$ tělesem není. □

Zkusíme-li přesto najít v $\mathbb{Z}_4$ inverzní prvek k 3, vyjde

x	0	1	2	3
$3x$	0	3	2	1

.

Inverzní prvek k 3 v $\mathbb{Z}_4$ existuje. Číslo 2 je jediný nenulový prvek v $\mathbb{Z}_4$, ke kterému inverzní prvek neexistuje.

Pokročíme dále k $\mathbb{Z}_5$:

x	0	1	2	3	4
$2x$	0	2	4	1	3

,

x	0	1	2	3	4
$4x$	0	4	3	2	1

.

V $\mathbb{Z}_5$ proto platí $2 \cdot 3 = 1$ a $4 \cdot 4 = 1$, a protože také $1 \cdot 1 = 1$, inverzní prvky existují ke všem nenulovým prvkům $\mathbb{Z}_5$ a $\mathbb{Z}_5$ proto tělesem je. Tělesa $\mathbb{Z}_3$ a $\mathbb{Z}_5$ jsou speciálním případem konečných tělesech popsaných v následující větě.

Věta 3.11. *Pro libovolné prvočíslo p je množina $\mathbb{Z}_p$ spolu s operacemi sčítání a násobení modulo p těleso.*

Důkaz. Z tvrzení 3.9 už víme, že $\mathbb{Z}_p$ splňuje všechny axiomy tělesa s výjimkou axiomu (N3).

Myšlenka důkazu existence inverzních prvků v $\mathbb{Z}_p$ vychází z pozorování, že ve všech dosud uvedených příkladech, kdy inverzní prvek k nenulovému $a \in \mathbb{Z}_n$ existoval, bylo zobrazení

$$x \mapsto ax : \mathbb{Z}_n \to \mathbb{Z}_n$$

vzájemně jednoznačné. Dokážeme, že v případě $\mathbb{Z}_p$, kdy p je prvočíslo, je pro každý nenulový prvek $a \in \mathbb{Z}_p$ toto zobrazení prosté.

Pokud pro nějaké dva prvky $x, y \in \mathbb{Z}_p$ platí, že $ax = ay$ v $\mathbb{Z}_p$, mají oba (běžné) součiny ax a ay stejný zbytek r při dělení prvočíslem p. Existují tedy celá čísla u, v, pro která platí

$$ax = pu + r \quad \text{a} \quad ay = pv + r \ .$$

Odečtením rovností dostaneme $a(x - y) = p(u - v)$. Z této rovnosti plyne, že prvočíslo p dělí (běžný) součin $a(x - y)$. Protože je to prvočíslo, musí dělit aspoň jednoho z činitelů a nebo $x - y$. Číslo a dělitelné prvočíslem p být nemůže, neboť $a \in \{1, 2, \ldots, p - 1\}$. Prvočíslo p tedy dělí rozdíl $x - y$. Protože $x, y \in \mathbb{Z}_p = \{0, 1, \ldots, p - 1\}$, pro absolutní hodnotu $|x - y|$ platí $0 \leq |x - y| < p$. Jedinou možností dělitelnou p je tedy $|x - y| = 0$ a proto $x = y$.

Zobrazení

$$x \mapsto ax : \mathbb{Z}_p \to \mathbb{Z}_p$$

je tedy prosté. Protože je množina $\mathbb{Z}_p$ konečná, je zobrazení $x \mapsto ax$ také na celou množinu $\mathbb{Z}_p$. Proto existuje $x \in \mathbb{Z}_p$ takové, že v $\mathbb{Z}_p$ platí $ax = 1$. □

Příklad 3.12. 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 v tělese $\mathbb{Z}_5$ platí $2^{-1} = 3$, 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. na konci této kapitoly 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 3.13. 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 přímo zeptat jakým číslem je v $\mathbb{Z}_7$ třeba vynásobit 5, 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 $4/5$ 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.

Než se pustíme do řešení soustavy lineárních rovnic s koeficienty v $\mathbb{Z}_{11}$ v následujícím příkladu, připravíme si tabulku inverzních prvků v tělese $\mathbb{Z}_{11}$:

x	1	2	3	4	5	6	7	8	9	10
x^{-1}	1	6	4	3	9	2	8	7	5	10

Příklad 3.14. 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 $(-4)2^{-1} = 7 \cdot 6 = 9$. 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

$$\frac{-7}{2} = (-7) \cdot 2^{-1} = 4 \cdot 6 = 2 \ ,$$

nebo rychleji například takto:

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

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. Hodnoty volných proměnných zvolíme libovolně $x_4 = t_4$ a $x_5 - t_5$ a zpětnou substitucí dopočteme hodnoty bázových proměnných

$$\begin{aligned} x_3 &= 9 - 10x_4 = 9 + (-10)t_4 = 9 + t_4, \\ x_2 &= 3 - 3x_3 - x_4 - 2x_5 = 3 + 8(9 + t_4) + 10t_4 + 9t_5 \\ &= 3 + 6 + 8t_4 + 10t_4 + 9t_5 = 9 + 7t_4 + 9t_5, \\ x_1 &= 7 - 2x_2 - 6x_3 - x_4 - 5x_5 = 7 - 2(9 + 7t_4 + 9t_5) + 5(9 + t_4) - t_4 - 5t_5 \\ &= 7 - 18 - 3t_4 - 7t_5 + 1 + 5t_4 - t_4 - 5t_5 = 1 + t_4 + 10t_5 \ . \end{aligned}$$

Obecné řešení soustavy se tedy rovná

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 1 \\ 9 \\ 9 \\ 0 \\ 0 \end{pmatrix} + t_4 \begin{pmatrix} 1 \\ 7 \\ 1 \\ 1 \\ 0 \end{pmatrix} + t_5 \begin{pmatrix} 10 \\ 9 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

a množina všech řešení soustavy je

$$\left\{ \begin{pmatrix} 1 \\ 9 \\ 9 \\ 0 \\ 0 \end{pmatrix} + t_4 \begin{pmatrix} 1 \\ 7 \\ 1 \\ 1 \\ 0 \end{pmatrix} + t_5 \begin{pmatrix} 10 \\ 9 \\ 0 \\ 0 \\ 1 \end{pmatrix} : t_4, t_5 \in \mathbb{Z}_{11} \right\} .$$

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

Definice 3.15. 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 nejméně je třeba sečíst jednotkový prvek, abychom dostali 0. Pokud sčítáním 1 nikdy nedostaneme nulový prvek, charakteristika je 0.

Věta 3.16. *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

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

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 v něm dělíme nulou. V tělese s charakteristikou 2 se nelze bratrsky rozdělit.

3.5. **Další příklady těles.**

3.5.1. *Čtyřprvkové těleso.* Pokud n není prvočíslo, pak $\mathbb{Z}_n$ není těleso. Tedy například $\mathbb{Z}_4$ není těleso. Není splněný axiom (N3), prvek 2 nemá inverzní prvek. Můžeme také použít větu 3.16, protože charakteristika by byla 4, což pro těleso není možné.

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, přičemž s koeficienty počítáme jako v tělese $\mathbb{Z}_2$. Např.

$$\alpha + (\alpha+1) = (1+1)\alpha + 1 = 1 \ .$$

Při násobení polynomy vynásobíme přirozeným způsobem (s koeficienty opět počítáme jako v $\mathbb{Z}_2$) a případný člen α^2 nahradíme součtem $\alpha+1$. Například

$$\begin{aligned}(\alpha+1)(\alpha+1) &= \alpha^2 + (1+1)\alpha + 1 = \\ &= \alpha^2 + 1 = (\alpha+1) + 1 = \alpha \ .\end{aligned}$$

Náhradu členu α^2 součtem $\alpha+1$ lze chápat také jako zbytek při dělení polynomu α^2 polynomem $\alpha^2+\alpha+1$. Násobení ve 4-prvkovém tělese $GF(4)$ lze tedy chápat také jako běžné násobení polynomů s koeficienty v $\mathbb{Z}_2$ modulo polynom $\alpha^2+\alpha+1$. Stejně tak je možné i sčítání považovat za běžné sčítání polynomů modulo $\alpha^2+\alpha+1$. Pro polynom $\alpha^2+\alpha+1$ je důležité, že jej nelze vyjádřit jako součin dvou polynomů menšího stupně. Této analogii prvočísel mezi polynomy říkáme *nerozložitelné polynomy.*

3.5.2. *Další konečná tělesa.* Těleso s n prvky existuje právě tehdy, když n je mocnina prvočísla. Důkaz uvidíte později v kurzu algebry. Pro každé prvočíslo p a přirozené číslo k dokonce existuje jediné těleso, které má p^k prvků. lze jej sestrojit 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.

Každé těleso s p^k prvky má charakteristiku p.

3.5.3. *Charakteristika a konečnost.* Každé těleso charakteristiky 0 má nekonečně mnoho prvků, protože čísla $0, 1, 1+1, 1+1+1$ jsou všechna navzájem různá. Lze 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. Příklad uvádět nebudeme, řekneme si pouze, že každé těleso charakteristiky p „obsahuje“ těleso $\mathbb{Z}_p$ (opět viz cvičení).

3.5.4. *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 čtvrtého stupně, nebo při důkazu neexistence konstrukce kvadratury kruhu, trisekce úhlu nebo zdvojení krychle kružítkem a pravítkem.

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

$$a + ib + jc + kd \ ,$$

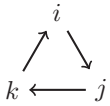
kde $a, b, c, d \in \mathbb{R}$ a i, j, k jsou *kvaternionové jednotky.* Sčítání je definováno přirozeně, tedy

$$(a+ib+jc+kd)+(a'+ib'+jc'+kd') = (a+a')+i(b+b')+j(c+c')+k(d+d') \ .$$

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 kvaternionovou jednotku s kladným znaménkem, a násobení proti směru znaménko obrací. Tedy

$$\begin{aligned}(a+ib+jc+kd)\cdot(a'+ib'+jc'+kd') &= \\ = aa'+iab'+jac'+kad'+iba'+i^2bb'+ijbc'+ikbd'+& \\ +jca'+jicb'+j^2cc'+jkcd'+kda'+kidb'+kjdc'+k^2dd' &= \\ = aa'+iab'+jac'+kad'+iba'-bb'+kbc'-jbd'+& \\ +jca'-kcb'-cc'+icd'+kda'+jdb'-idc'-dd' &= \\ = (aa'-bb'-cc'-dd')++i(ab'+ba'+cd'-dc')+& \\ +j(ac'-bd'+ca'+db')+k(ad'+bc'-cb'+da')\ .&\end{aligned}$$

Kvaterniony typu $a+ib+j0+k0$ můžeme sčítat a násobit jako komplexní čísla, neboť

$$(a+ib+j0+k0)+(a'+ib'+j0+k0)=(a+a')+i(b+b')+j0+k0$$

a rovněž

$$(a+ib+j0+k0)\cdot(a'+ib'+j0+k0)=aa'-bb'+i(ab'+ba')+j0+k0\ .$$

Těleso kvaternionů je tedy rozšířením tělesa komplexních čísel stejně jako je těleso komplexních čísel rozšířením tělesa reálných čísel.

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. Pátrání po tom, jak osa a úhel složené rotace závisí na osách a úhlech původních rotací které skládáme, vedlo k objevu kvaternionů.

Délkou kvaternionu $a+ib+jc+kd$ 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. Přímo z definice také plyne, že je-li $a+ib+jc+kd$ jednotkový kvaternion, pak také $-a-ib-jc-kd$ je jednotkový kvaternion.

Je-li $a^2+b^2+c^2=1$, pak 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 jednotkového kvaternionu

$$\cos(\alpha/2)+(ia+jb+kc)\sin(\alpha/2)\ .$$

Tak například otočení o úhel $\pi/2$ kolem první souřadné osy zapíšeme jako kvaternion

$$\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}\ .$$

Otočení kolem osy z o úhel $\pi/2$ v kladném směru zapíšeme pomocí kvaternionu

$$\frac{\sqrt{2}}{2}+k\frac{\sqrt{2}}{2}\ .$$

Jednotkový kvaternion

$$\cos(\alpha/2)+(ia+jb+kc)\sin(\alpha/2)$$

popisuje stejnou rotaci jako jednotkový kvaternion

$$-\cos(\alpha/2) - (ia + jb + kc)\sin(\alpha/2) \ .$$

Pro každou rotaci máme proto na výběr dva možné jednotkové kvaterniony. 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 3.17. Složíme rotaci kolem osy x o úhel $\pi/2$ s rotací kolem osy z o úhel $\pi/2$. Osu a úhel složené rotace najdeme jako součin kvaternionů

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

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 **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 **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. Dokažte, že pro libovolné $n \geq 2$ platí, že k prvku $a \in \mathbb{Z}_n$ existuje inverzní prvek v $\mathbb{Z}_n$ právě když je číslo a nesoudělné s n (tj. největší společný dělitel čísel a, n se rovná 1).

5. Dokažte, že v libovolném tělese **T** charakteristiky 2 platí $a = -a$ pro libovolný prvek $a \in T$.

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

7. 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
- $\{a + b\sqrt[3]{2} : a, b \in \mathbb{Q}\}$
- $\{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$
- $\{a + b\sqrt{2} + c\sqrt{3} : a, b, c \in \mathbb{Q}\}$
- $\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$

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

9. 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.

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

11. V tělese kvaternionů najděte prvek inverzní k nenulovému kvaternionu $a+ib+jc+kd$.

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

Shrnutí třetí kapitoly

(1) Binární operace na množině T je zobrazení z $T \times T$ do T.
(2) *Těleso* **T** je **množina** T **spolu se dvěmi binárními operacemi** $+$ a $\cdot$ na T splňující následující axiomy
   (S1) pro každé $a, b, c \in T$ platí $(a + b) + c = a + (b + c)$,
   (S2) existuje prvek $0 \in T$ takový, že pro každé $a \in T$ platí $a + 0 = a$,
   (S3) pro každý prvek $a \in T$ existuje $-a \in T$ takový, že $a + (-a) = 0$,
   (S4) pro každé $a, b \in T$ platí $a + b = b + a$,
   (N1) pro každé $a, b, c \in T$ platí $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,
   (N2) existuje prvek $1 \in T$ takový, že pro každé $a \in T$ platí $a \cdot 1 = a$,
   (N3) pro každý prvek $a \in T$, $a \neq 0$, existuje $a^{-1} \in T$ takový, že $a \cdot a^{-1} = 1$,
   (N4) pro každé $a, b \in T$ platí $a \cdot b = b \cdot a$,
   (D) pro každé $a, b, c \in \mathbb{R}$ platí $a \cdot (b + c) = a \cdot b + a \cdot c$.
   (nT) T má aspoň dva prvky.
   Vlastnostem počítání v tělese říkáme *axiomy tělesa*.
(3) Z axiomů tělesa vyplývají následující běžné vlastnosti obou operací, které proto platí v každém tělese **T**:
   - nulový prvek je určený jednoznačně,
   - rovnice $a + x = b$ má vždy právě jedno řešení, speciálně opačný prvek $-a$ je prvkem $a \in T$ určený jednoznačně,
   - jednotkový prvek je určený jednoznačně,
   - 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,
   - $0a = 0$ pro libovolný prvek $a \in T$,
   - je-li $ab = 0$, pak buď $a = 0$ nebo $b = 0$,
   - $-a = (-1)a$ pro každý prvek $a \in T$,
   - z rovnosti $a + b = a + c$ plyne $b = c$,
   - z rovnosti $ab = ac$ a předpokladu $a \neq 0$ vyplývá $b = c$,
   - $0 \neq 1$.
(4) Klasické číselné obory Q, $\mathbb{R}$ a $\mathbb{C}$ jsou tělesa.
(5) Pro každé přirozené číslo $n \geq 2$ definujeme *součet modulo* n dvou celých čísel a, b jako zbytek při dělení běžného součtu $a+b$ číslem n. Zbytek bereme vždy z množiny $\mathbb{Z}_p = \{0, 1, \ldots, n-1\}$.
(6) Analogicky definujeme *součin modulo* n jako zbytek při dělení běžného součinu ab číslem n.
(7) Pro každé prvočíslo p je množina všech „zbytků“ $\mathbb{Z}_p$ spolu s operacemi sčítání a násobení modulo n těleso. Jsou to příklady konečných těles. K důkazu je nutné ověřit platnost všech axiomů tělesa.
(8) Existuje-li kladné celé číslo n takové, že v tělese **T** platí
$$\underbrace{1 + 1 + \cdots + 1}_{n} = 0 \ ,$$
pak nejmenší takové kladné číslo nazýváme *charakteristika* tělesa **T**.
   Pokud žádné takové kladné celé číslo n neexistuje, tak říkáme že těleso **T** má *charakteristiku* 0.
(9) Charakteristika každého tělesa je buď 0 nebo prvočíslo.
(10) Klasické číselné obory $\mathbb{Q}$, $\mathbb{R}$ a $\mathbb{C}$ mají charakteristiku 0, konečné těleso $\mathbb{Z}_p$ má charakteristiku p. Každé konečné těleso má nenulovou charakteristiku.

Klíčové znalosti z třetí kapitoly nezbytné pro průběžné sledování přednášek s pochopením

(1) Znát axiomy tělesa a umět počítat v tělesech.
(2) Umět počítat v tělesech $\mathbb{Z}_p$ a umět řešit soustavy lineárních rovnic nad tělesy $\mathbb{Z}_p$.

4. Matice

Cíl. *Ukážeme si základní operace s maticemi. Jednoduché jsou operace sčítání matic a součin čísla s maticí. Složitější operací je součin dvou matic. Jednoduchá geometrická zobrazení můžeme popsat pomocí matic. Každá matice určuje nějaké zobrazení. Definice součinu dvou matic má přirozené vysvětlení pomocí složeného zobrazení. Naučíme se provádět elementární řádkové úpravy pomocí násobení elementárními maticemi zleva. Pak si ukážeme, že k některým maticím existují inverzní matice a naučíme se je počítat. Nakonec si ukážeme další praktická použití matic.*

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 odvodíme základní vlastnosti počítání s maticemi.

K pochopení násobení matic nahlédneme, že matice přirozeným způsobem určují zobrazení. Pomocí matic lze 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 2.2 a 2.9 tím, že prvky mohou být z libovolného pevně zvoleného tělesa.

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

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

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

Definice 4.2. Jsou-li $A = (a_{ij})$ a $B = (b_{ij})$ matice stejného typu $m \times n$ nad stejným tělesem $\mathbf{T}$, pak definujeme

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

Součet matic různých typů nebo nad různými tělesy není definován.

Matice $A = (a_{ij})$ a $B = (b_{ij})$ považujeme za stejné, pokud mají stejný typ $m \times n$ a také mají stejné prvky na odpovídajících pozicích. Formálněji, pro každé $i \in \{1, 2, \dots, m\}$ a každé $j \in \{1, 2, \dots, n\}$ platí $a_{ij} = b_{ij}$. Rovnost mezi dvěma maticemi tak znamená mn rovností mezi jejich prvky na stejných místech.

Příklad 4.3. Nad tělesem $\mathbb{Z}_5$ platí

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

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

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

Tvrzení 4.4. *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 matic se dokáží podobně. □

Analogicky k definici t-násobku aritmetického vektoru definujeme t-násobek matice.

Definice 4.5. Je-li $A = (a_{ij})$ matice typu $m \times n$ nad tělesem $\mathbf{T}$ a $t \in \mathbf{T}$, pak definujeme

- *t-násobek matice A* jako matici $t \cdot A = tA = (ta_{ij})_{m\times n}$.

Zdůrazněme, že výraz At jsme nedefinovali, t-násobek matice A píšeme vždy tA.

Příklad 4.6. Nad tělesem $\mathbb{Z}_5$ platí

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

Z axiomů počítání v tělese plyne ihned následující tvrzení.

Tvrzení 4.7. *Pro matice $A = (a_{ij})$ a $B = (b_{ij})$ téhož typu $m \times n$ nad stejným tělesem $\mathbf{T}$ a pro libovolné dva prvky $s, t \in \mathbf{T}$ platí*

(1) $s(tA) = (st)A$,
(2) $1A = A$,
(3) $-A = (-1)A$,
(4) $(s + t)A = sA + tA$,
(5) $s(A + B) = sA + sB$.

Důkaz. Dokážeme například vlastnost (5). Protože předpokládáme, že matice A, B jsou nad stejným tělesem $\mathbf{T}$ a mají stejný typ $m \times n$, je součet $A + B$ definován a má typ $m \times n$. Proto také matice $s(A + B)$ má typ $m \times n$. Stejný typ mají také matice sA a sB, proto také součet $sA + sB$ je definován a má typ $m \times n$.

Prvek na místě (i, j) v matici $s(A + B)$ se rovná $s(a_{ij} + b_{ij})$. Prvek na témže místě (i, j) v matici $sA + sB$ se rovná $sa_{ij} + sb_{ij}$. Z axiomu distributivity (D) pro počítání v tělesech plyne $s(a_{ij} + b_{ij}) = sa_{ij} + sb_{ij}$.

Prvky na stejných místech v maticích $s(A+B)$ a $sA+sB$ se rovnají, platí proto rovnost matic $s(A + B) = sA + sB$.

Ostatní rovnosti se dokáží stejným způsobem. □

Obě definované operace vůbec neberou v úvahu tabulkovou strukturu matice, jsou definované „po prvcích“. První operací, která není tohoto typu, je transponování.

Definice 4.8. *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 $i \in \{1, 2, \ldots, m\}$ a $j \in \{1, 2, \ldots, n\}$.

Zavedené označení A^T je v souladu s dříve používaným značením $(a_1, \ldots, a_n)^T$ pro sloupcový vektor.

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

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

Transponování matic má následující tři jednoduché vlastnosti.

Tvrzení 4.9. *Pro matice $A = (a_{ij})$ a $B = (b_{ij})$ téhož typu $m \times n$ nad stejným tělesem $\mathbf{T}$ a pro libovolný prvek $s \in \mathbf{T}$ platí*

(1) $\left(A^T\right)^T = A$,
(2) $(A + B)^T = A^T + B^T$,
(3) $(sA)^T = s\,A^T$.

Důkaz. Dokážeme pouze vlastnost (1). Matice A^T má typ $n \times m$ a matice $\left(A^T\right)^T$ má proto typ $m \times n$, stejný jako matice A.

Prvek na libovolném místě (i, j) matice $\left(A^T\right)^T$ se rovná prvku na místě (j, i) matice A^T a ten se rovná prvku na místě (i, j) matice A, tj. prvku a_{ij}. Tím je rovnost $\left(A^T\right)^T = A$ dokázána. □

4.2. **Součin matic.**

V případě součinu matic je někdy vhodnější nahlížet na matici jako na posloupnost sloupcových aritmetických vektorů, nikoliv jako na soubor prvků uspořádaných do obdélníku. V tom případě matici $A = (a_{ij})_{m\times n}$ nad tělesem $\mathbf{T}$ zapisujeme jako

$$A = (\mathbf{a}_1|\mathbf{a}_2|\ldots|\mathbf{a}_n) \ ,$$

kde pro každé $j = 1, 2, \ldots, n$ vektor $\mathbf{a}_j = (a_{1j}, a_{2j}, \ldots, a_{mj})^T$ je m-složkový sloupcový aritmetický vektor.

Například reálnou matici

$$A = \left(\begin{array}{c|c|c|c} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \end{array}\right)$$

zapíšeme také jako $A = (\mathbf{a}_1|\mathbf{a}_2|\mathbf{a}_3|\mathbf{a}_4)$, kde

$$\mathbf{a}_1 = \begin{pmatrix} 1 \\ 5 \end{pmatrix}, \quad \mathbf{a}_2 = \begin{pmatrix} 2 \\ 6 \end{pmatrix}, \quad \mathbf{a}_3 = \begin{pmatrix} 3 \\ 7 \end{pmatrix}, \quad \mathbf{a}_4 = \begin{pmatrix} 4 \\ 8 \end{pmatrix} .$$

Zapíšeme-li matici A^T transponovanou k matici $A = (a_{ij})_{m\times n}$ sloupcově, dostaneme zápis

$$A^T = (\tilde{\mathbf{a}}_1|\tilde{\mathbf{a}}_2|\cdots|\tilde{\mathbf{a}}_m) \ ,$$

kde pro každé $i = 1, 2, \ldots, m$ vektor $\tilde{\mathbf{a}}_i = (a_{i1}, a_{i2}, \ldots, a_{in})^T$ je i-tý sloupcový vektor transponované matice A^T.

Po transponování posledního zápisu (s použitím rovnosti $\left(A^T\right)^T = A$) dostaneme řádkový zápis matice A

$$A = \begin{pmatrix} \tilde{\mathbf{a}}_1^T \\ \tilde{\mathbf{a}}_2^T \\ \vdots \\ \tilde{\mathbf{a}}_m^T \end{pmatrix} ,$$

kde $\tilde{\mathbf{a}}_i^T = (a_{i1}, a_{i2}, \dots, a_{in})$ je i-tý řádkový vektor matice A.

4.2.1. *Součin matice s vektorem.* Nejdříve definujeme součin matice s vektorem a poté součin dvou matic.

Definice 4.10. Je-li $A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ matice typu $m \times n$ nad tělesem $\mathbf{T}$ a $\mathbf{b} = (b_1, b_2, \dots, b_n)^T$ (sloupcový) aritmetický vektor s n-složkami z tělesa $\mathbf{T}$, pak definujeme *součin matice A s vektorem* $\mathbf{b}$ jako

$$A\mathbf{b} = b_1\mathbf{a}_1 + b_2\mathbf{a}_2 + \cdots + b_n\mathbf{a}_n \ .$$

Součin $A\mathbf{b}$ je tedy lineární kombinace sloupcových vektorů $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n$ s koeficienty $b_1, b_2, \dots, b_n$. Výsledkem je m-složkový vektor nad $\mathbf{T}$.

Příklad 4.11. Spočteme součin nad $\mathbb{R}$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = 1 \begin{pmatrix} 1 \\ 4 \\ 7 \end{pmatrix} + 2 \begin{pmatrix} 2 \\ 5 \\ 8 \end{pmatrix} + 3 \begin{pmatrix} 3 \\ 6 \\ 9 \end{pmatrix} = \begin{pmatrix} 14 \\ 32 \\ 50 \end{pmatrix} \ .$$

Pomocí součinu matice s vektorem můžeme kompaktně zapsat soustavu lineárních rovnic

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

nad tělesem $\mathbf{T}$. Je-li $A = (a_{ij})_{m\times n} = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ matice této soustavy, pak n-složkový vektor $\mathbf{x} = (x_1, x_2, \dots, x_n)^T \in \mathbf{T}^n$ je řešením této soustavy právě když

$$A\mathbf{x} = x_1\mathbf{a}_1 + x_2\mathbf{a}_2 + \cdots + x_n\mathbf{a}_n = \mathbf{b} \ .$$

Soustavu proto můžeme zapsat jako

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

Od této chvíle budeme pro soustavu lineárních rovnic používat téměř výhradně tento zápis.

4.2.2. *Součin dvou matic.*

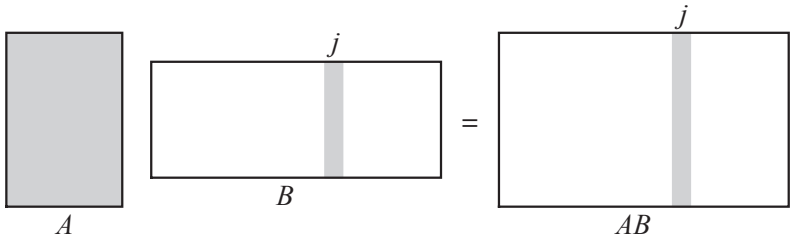
Definice 4.12. Je-li A matice typu $m \times n$ a $B = (\mathbf{b}_1|\mathbf{b}_2|\cdots|\mathbf{b}_p)$ matice typu $n \times p$, obě nad stejným tělesem $\mathbf{T}$, pak *součinem matic A* a B rozumíme matici

$$AB = (A\mathbf{b_1}|A\mathbf{b}_2|\cdots|A\mathbf{b}_p) \ ,$$

tj. j-tý sloupec součinu matic AB se rovná součinu matice A s j-tým sloupcem matice B.

Součin AB je tedy definován, pokud počet sloupců matice A je rovný počtu řádků matice B. Jinak definován není. To znamená, že je-li $m \neq p$, součin BA definován není, přestože součin AB definován je.

Na obrázku vidíme grafické znázornění součinu matic.



Obrázek 39. Sloupce v součinu matic

Každý sloupec v součinu AB je nějakou lineární kombinací sloupců matice A. Z definice také plyne, že součin matice typu $m \times n$ s maticí typu $n \times p$ je matice typu $m \times p$.

Příklad 4.13. Spočteme součin dvou reálných matic

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \end{pmatrix} .$$

Součin je definován neboť počet sloupců v levém činiteli se rovná počtu řádků v pravém činiteli. První sloupec v součinu se rovná

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \begin{pmatrix} 1 \\ 5 \end{pmatrix} = 1 \begin{pmatrix} 1 \\ 3 \\ 5 \end{pmatrix} + 5 \begin{pmatrix} 2 \\ 4 \\ 6 \end{pmatrix} = \begin{pmatrix} 11 \\ 23 \\ 35 \end{pmatrix} .$$

Analogicky spočteme další tři sloupcové vektory součinu:

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \begin{pmatrix} 2 \\ 6 \end{pmatrix} = \begin{pmatrix} 14 \\ 30 \\ 46 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \begin{pmatrix} 3 \\ 7 \end{pmatrix} = \begin{pmatrix} 17 \\ 37 \\ 57 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \begin{pmatrix} 4 \\ 8 \end{pmatrix} = \begin{pmatrix} 20 \\ 44 \\ 68 \end{pmatrix} .$$

Platí tedy

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \end{pmatrix} = \begin{pmatrix} 11 & 14 & 17 & 20 \\ 23 & 30 & 37 & 44 \\ 35 & 46 & 57 & 68 \end{pmatrix} .$$

Všimněme si, že v opačném pořadí obě matice vynásobit nelze, jejich součin není definován.

Při ručním výpočtu součinu dvou matic je často výhodnější použít následující tvrzení, které říká jak přímo spočítat jednotlivé prvky v součinu matic.

Tvrzení 4.14. *Jsou-li $A = (a_{ij})_{m\times n}$ a $B = (b_{jk})_{n\times p}$ matice nad tělesem $\mathbf{T}$, pak prvek na místě (i,k) v součinu AB se rovná*

$$a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj} = \sum_{j=1}^{n} a_{ij}b_{jk} = \tilde{\mathbf{a}}_i^T \mathbf{b}_k \ .$$

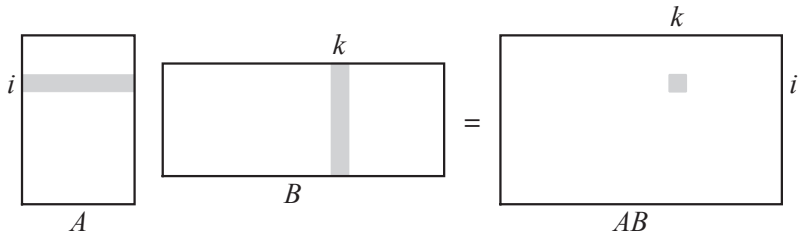
Důkaz. Prvek na místě (i,k) v součinu AB leží v k-tém sloupci, který se rovná $A\mathbf{b}_k$. Protože

$$A\mathbf{b}_k = b_{1k}\mathbf{a}_1 + b_{2k}\mathbf{a}_2 + \cdots + b_{nk}\mathbf{a}_n \ ,$$

i-tá složka vektoru $A\mathbf{b}_k$ se rovná

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

□



Obrázek 40. Prvky v součinu dvou matic

Prvek na místě (i,k) v součinu AB se tak rovná součinu i-tého řádku matice A s k-tým sloupcem matice B. V případě reálných matic tento součin nazýváme *standardní skalární součin* řádkového vektoru $\tilde{\mathbf{a}}_i^T$ se sloupcovým vektorem $\mathbf{b}_k$ matice B.

Příklad 4.15. Nad tělesem $\mathbb{R}$ máme

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

Poslední příklad ukazuje, že i v případě, kdy jsou oba součiny AB a BA definované, tak nemusí mít stejný typ. Následující příklad navíc ukazuje, že dokonce i v případě, kdy jsou oba součiny AB a BA definované a mají stejný typ, může platit $AB \neq BA$.

Příklad 4.16. Opět počítáme s reálnými maticemi.

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 10 & 5 \\ 24 & 11 \end{pmatrix} \ ,$$

zatímco

$$\begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 7 & 12 \\ 9 & 14 \end{pmatrix} \ .$$

Poučka k zapamatování tedy zní:

násobení matic není komutativní.

Jsou pro to dokonce tři různé důvody. Může být definován pouze jeden ze součinů AB a BA. Pokud jsou definovány oba, mohou mít různý typ. A pokud mají stejný typ, může platit $AB \neq BA$.

Spočítáme ještě jeden součin větších matic.

Příklad 4.17. Počítáme opět nad $\mathbb{R}$.

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

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

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

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

4.2.3. *Další vlastnosti operací s maticemi.* Mnohé další vlastnosti počítání v tělesech se na počítání s maticemi přenáší.

Tvrzení 4.18. *Jsou-li $A = (a_{ij})$ a $B = (b_{ij})$ matice téhož typu $m \times n$, $C = (c_{jk})$ matice typu $n \times p$, a $D = (d_{kl})$, $E = (e_{kl})$ matice téhož typu $p \times q$, pak platí*

$$(A + B)C = AC + BC, \qquad C(D + E) = CD + CE \ .$$

Důkaz. Dokážeme první rovnost. Součet matic $A + B$ má typ $m \times n$ a proto součin $(A + B)C$ má typ $m \times p$. Stejný typ $m \times p$ mají také oba součiny AC a BC a proto i jejich součet $AC + BC$. Obě matice $(A + B)C$ a $AC + BC$ mají tedy stejný typ.

Prvek na místě (i, k) v součinu $(A + B)C$ se podle tvrzení 4.14 rovná

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

Prvky na místě (i, k) v součinech AC a BC a v součtu $AC + BC$ se postupně rovnají

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

Tím je rovnost $(A + B)C = AC + BC$ dokázána. □

Druhou rovnost v předchozím tvrzení stejně jako všechny další vlastnosti počítání s maticemi lze dokázat pomocí stejné osnovy:

(1) přesvědčíme se, že všechny operace na obou stranách jsou definované,
(2) ověříme, že na obou stranách vyjdou matice stejného typu,
(3) dokážeme, že každý prvek ve výsledné matici vlevo se rovná prvku na tomtéž místě ve výsledné matici vpravo,
(4) krok 3. je založený na definici příslušných operací s maticemi a vlastnostech počítání v tělese.

Důležitou asociativitu násobení matic dokážeme v následujícím tvrzení.

Tvrzení 4.19. *Jsou-li $B = (b_{ij})$ matice typu $m \times n$, $C = (c_{jk})$ matice typu $n \times p$, a $D = (d_{kl})$ matice typu $p \times q$, pak platí*

$$(BC)D = B(CD) \ .$$

Důkaz. Součin BC je definovaný a má typ $m \times p$, proto je definovaný také součin $(BC)D$, který má typ $m \times q$. Podobně ověříme, že také součin $B(CD)$ je definovaný a má tentýž typ $m \times q$.

Zvolíme libovolné $i \in \{1, 2, \ldots, m\}$ a $l \in \{1, 2, \ldots, q\}$ a spočítáme prvek na místě (i, l) v matici $(BC)D$. Prvek na místě (i, k) v součinu $BC = (e_{ik})$ se rovná

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

Prvek na místě (i, l) v součinu $(BC)D$ se potom rovná

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

K výpočtu prvku na místě (i, l) v součinu $B(CD)$ napřed spočítáme prvek na místě (j, l) v součinu $(CD) = (f_{jl})$:

$$f_{jl} = \sum_{k=1}^{p} c_{jk}d_{kl} \ .$$

Prvek na místě (i, l) v součinu $B(CD)$ se potom rovná

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

Obě dvojité sumy, ke kterým jsme dospěli, se rovnají neboť v nich sčítáme stejné prvky $(b_{ij}c_{jk})d_{kl} = b_{ij}(c_{jk}d_{kl})$, pouze v jiném pořadí.

Nahlédnout to můžeme například tak, že si každý sčítanec $b_{ij}c_{jk}d_{kl}$ napíšeme na místo (j, k) v matici G typu $n \times p$. V případě první dvojité sumy $\sum_{k=1}^{p} \sum_{j=1}^{n} b_{ij}c_{jk}d_{kl}$ je napřed sečteme po sloupcích matice G a pak sečteme součty sloupců. V případě druhé dvojité sumy $\sum_{j=1}^{n} \sum_{k=1}^{p} b_{ij}c_{jk}d_{kl}$ je napřed sečteme po řádcích matice G a pak sečteme součty řádků. Vzhledem ke komutativitě sčítání v tělese $\mathbf{T}$ je v obou případech výsledkem součet všech prvků matice G.

Tím jsme dokázali, že prvky na témže místě v maticích $(BC)D$ a $B(CD)$ se rovnají, což dokazuje rovnost matic $(BC)D = B(CD)$. □

Další vlastnosti součinu matic jsou v následujícím tvrzení, jehož důkaz ponecháme jako cvičení.

Tvrzení 4.20. *Pro libovolné matice A typu $m \times n$ a B typu $n \times p$, a každý prvek s tělesa $\mathbf{T}$ platí*

- $s(AB) = (sA)B = A(sB)$,
- $(AB)^T = B^T A^T$.

V následujícím příkladu využijeme řadu vlastností operací s maticemi.

Příklad 4.21. Čtvercová matice $A = (a_{ij})$ řádu n se nazývá *symetrická*, pokud $a_{ij} = a_{ji}$ pro libovolné $i, j \in \{1, 2, \ldots, n\}$. Ekvivalentně, A je symetrická, pokud $A^T = A$. Pomocí vlastností z tvrzení 4.20 a tvrzení 4.9 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 první vlastnost z tvrzení 4.20, když jsme například nepsali závorky ve výrazu $2AA^T$.

Víme už, jak vypadají sloupce a jednotlivé prvky v součinu AB. V následujícím tvrzení popíšeme jak v součinu AB vypadají řádky.

Tvrzení 4.22. *Jsou-li $A = (a_{ij})$ matice typu $m \times n$ a $B = (b_{jk})$ matice typu $n \times p$, pak pro každé $i = 1, 2, \ldots, m$ se i-tý řádek v součinu AB rovná lineární kombinaci řádků matice B s koeficienty v i-tém řádku matice A. Formálně, i-tý řádek v součinu AB se rovná*

$$a_{i1}\tilde{\mathbf{b}}_1^T + a_{i2}\tilde{\mathbf{b}}_2^T + \cdots + a_{in}\tilde{\mathbf{b}}_n^T = \tilde{\mathbf{a}}_i^T B \ .$$

Důkaz. Podle definice transponované matice se i-tý řádek v matici AB rovná i-tému sloupci transponované matice $(AB)^T$. Z druhé rovnosti v předchozím tvrzení 4.20 dostáváme $(AB)^T = B^T A^T$.

Z definice součinu matic plyne, že i-tý sloupec v součinu $B^T A^T$ se rovná lineární kombinaci sloupců matice $B^T = (\tilde{\mathbf{b}}_1 | \tilde{\mathbf{b}}_2 | \cdots | \tilde{\mathbf{b}}_n)$ s koeficienty v i-tém sloupci $\tilde{\mathbf{a}}_i = (a_{i1}, a_{i2}, \ldots, a_{in})^T$ matice A^T, tj. rovná se

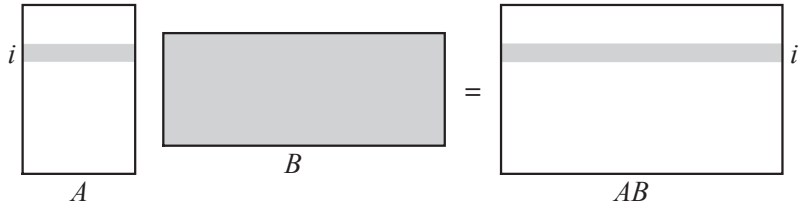
$$B^T \tilde{\mathbf{a}}_i = a_{i1}\tilde{\mathbf{b}}_1 + a_{i2}\tilde{\mathbf{b}}_2 + \cdots + a_{in}\tilde{\mathbf{b}}_n \ .$$

Přechodem k transponovaným maticím na obou stranách poslední rovnosti a s využitím vlastností transponování z tvrzení 4.9 dostaneme rovnost

$$a_{i1}\tilde{\mathbf{b}}_1^T + a_{i2}\tilde{\mathbf{b}}_2^T + \cdots + a_{in}\tilde{\mathbf{b}}_n^T = (B^T \tilde{\mathbf{a}}_i)^T = \tilde{\mathbf{a}}_i^T B \ .$$

□

Na obrázku vidíme grafické znázornění řádků v součinu AB. Každý řádek v součinu matic je nějakou lineární kombinací řádků pravého činitele.



Obrázek 41. Řádky v součinu matic

Příklad 4.23. Podívejme se ještě jednou na součin v příkladu 4.17.

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

Podle předchozího tvrzení je první řádek výsledku součet 1-násobku řádkového vektoru $\tilde{\mathbf{b}}_1^T = (3, 5, 2, 4)$, 0-násobku $\tilde{\mathbf{b}}_2^T = (1, 1, -3, 2)$ a (-1)-násobku $\tilde{\mathbf{b}}_3^T = (0, 2, -2, 1)$, to je $(3, 3, 4, 3)$. Druhý řádek výsledku je součtem prvních dvou řádků 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.

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

Definice 4.24. *Jednotková matice řádu n nad tělesem* $\mathbf{T}$ je čtvercová matice $I_n = (a_{ij})_{n\times n}$, kde $a_{ii} = 1$ pro každé $i \in \{1, 2, \dots, n\}$, a $a_{ij} = 0$ kdykoliv $i \neq j$, pro $i, j \in \{1, 2, \dots, n\}$. 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 zapisujeme pomocí symbolu δ_{ij}, tzn. *Kroneckerovo delta*. Ten se rovná 1, pokud $i = j$, a 0 jinak. Těleso, ve kterém počítáme, musí být zřejmé z kontextu.

Tvrzení 4.25. *Pro každou matici A typu $m \times n$ platí*

$$I_m A = A = A I_n \ .$$

Důkaz. Druhá rovnost plyne z definice součinu matic, první rovnost z tvrzení 4.22. □

4.2.5. *Blokové násobení matic.* Někdy je výhodné nahlížet na matici jako rozdělenou do bloků a operace, zejména násobení, provádět blokově. Optimalizované algoritmy pro výpočet součinu dvou matic využívají blokové násobení spíše než vyjádření jednotlivých prvků součinu pomocí tvrzení 4.14. Velikost bloků je volena s ohledem na velikost *cache* v počítači.

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 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}, …, A_{1s}, A_{21}, …, A_{rs}.

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

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}, …, B_{st}:

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

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

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

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.

Někdy lze výpočet součinu dvou matic zjednodušit, pokud si všimneme, že matice mají přirozenou blokovou strukturu složenou z jednoduchých bloků.

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

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

Všimneme si, že matice A má blokovou strukturu

$$A = \left(\begin{array}{cc|ccc} 1 & 0 & 2 & 3 & 4 \\ 0 & 1 & 5 & 0 & 6 \\ \hline 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array}\right) .$$

Označíme-li pravý horní blok

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

můžeme násobit po blocích

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

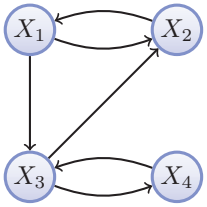
$$= \left(\begin{array}{c|c} I_2 & 2B \\ \hline 0 & I_3 \end{array}\right) = \begin{pmatrix} 1 & 0 & 4 & 6 & 1 \\ 0 & 1 & 3 & 0 & 5 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} .$$

4.3. **Dvě aplikace.** 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. Mocniny matic využijeme v následujících dvou ukázkách použití násobení matic.

4.3.1. *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.



Informaci o spojeních mezi městy uložíme 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 $a_{ij} = 0$ v opačném případě.

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

Nyní se zamyslíme, jaký je význam prvku na místě (i, k) v matici A^2. Tento prvek je rovný $a_{i1}a_{1k} + a_{i2}a_{2k} + a_{i3}a_{3k} + a_{i4}a_{4k}$. Všimněte si, že j-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 v ostatních případech. Prvek na místě (i, k) 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

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

4.3.2. *Rekurentní rovnice.* Asi jste se již setkali s Fibonacciho posloupností definovanou předpisem

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

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

Z definice posloupnosti nahlédneme, že dvojice sousedních členů splňuje vztah

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

Označíme-li C matici 2×2 vystupující v této rovnosti, vidíme že

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

a indukcí podle i dostaneme

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

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

$$a_i = \frac{\varphi^i}{\sqrt{5}} - \frac{(1-\varphi)^i}{\sqrt{5}} \ ,$$

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

4.4. **Speciální typy matic.** V dalším textu budeme často používat následující speciální typy matic.

Definice 4.27. Čtvercovou matici $A = (a_{ij})$ nazýváme

- *diagonální*, pokud $a_{ij} = 0$ kdykoliv $i \neq j$,
- *permutační*, má-li v každém řádku a každém sloupci právě jeden prvek 1 a ostatní 0,
- *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.*

Následující tvrzení ukazuje, že součin dvou matic jednoho z uvedených typů je opět matice téhož typu.

Tvrzení 4.28. *Jsou-li $A = (a_{ij})$ a $B = (b_{jk})$ čtvercové matice téhož řádu n, pak jejich součin AB je*

(1) *diagonální, jsou-li obě matice A, B diagonální,*
(2) *permutační matice, jsou-li obě matice A, B permutační,*
(3) *horní trojúhelníková matice, jsou-li obě matice A, B horní trojúhelníkové,*
(4) *horní trojúhelníková s prvky 1 na hlavní diagonále, jsou-li obě matice A, B horní trojúhelníkové s prvky 1 na hlavní diagonále,*
(5) *dolní trojúhelníková matice, jsou-li obě matice A, B dolní trojúhelníkové,*
(6) *dolní trojúhelníková s prvky 1 na hlavní diagonále, jsou-li obě matice A, B dolní trojúhelníkové s prvky 1 na hlavní diagonále.*

Důkaz. K důkazu (1) použijeme vyjádření prvků v součinu matic $AB = (c_{ik})$ podle tvrzení 4.14. Prvek c_{ik} v součinu AB se rovná

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

Předpoklad, že obě matice A, B jsou diagonální, znamená $a_{ij} = 0$ kdykoliv $i \neq j$ a $b_{jk} = 0$ kdykoliv $j \neq k$. Je-li $i \neq k$, pak pro každé $j = 1, 2, \ldots, n$ je buď $i \neq j$ nebo $j \neq k$. Odtud plyne, že buď $a_{ij} = 0$ nebo $b_{jk} = 0$, což dokazuje $c_{ik} = 0$ kdykoliv $i \neq k$, součin AB je proto diagonální matice.

(2) můžeme dokázat přímo z definice 4.12 součinu matic. Pro každé $j = 1, 2, \ldots, n$ se j-tý sloupec v součinu AB rovná $A\mathbf{b}_j$. Protože B je permutační matice, obsahuje sloupec $\mathbf{b}_j$ pouze jeden prvek $b_{ij} = 1$ a ostatní prvky v j-tém sloupci jsou 0. Proto sloupec $A\mathbf{b}_j = \mathbf{a}_i$ obsahuje rovněž pouze jeden prvek rovný 1 a ostatní 0, neboť předpokládáme že A je také permutační matice.

Protože je v i-tém řádku matice B také jediný prvek rovný 1 a ostatní 0, plyne odtud, že pouze jeden sloupec součinu AB se rovná $\mathbf{a}_i$. Sloupce v součinu AB tedy dostaneme jako nějakou permutaci sloupců matice A. Jelikož v každém řádku matice A je jediný prvek 1 a ostatní prvky 0, obsahuje také každý řádek součinu AB jediný prvek 1 a ostatní 0.

(3) opět dokážeme pomocí tvrzení 4.14. Prvek na místě (i, k) v součinu $AB = (c_{ik})$ je tedy

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

Předpoklad, že obě matice A, B jsou horní trojúhelníkové znamená, že $a_{ij} = 0$ kdykoliv $i > j$ a $b_{jk} = 0$ kdykoliv $j > k$. Je-li nyní $i > k$, platí pro každé $j = 1, 2, \ldots, n$ buď $j > k$ nebo $i > j$. Součin $a_{ij}b_{jk}$ se proto rovná 0 pro každé $j = 1, 2, \ldots, n$, proto $c_{ik} = 0$ kdykoliv $i > k$. Součin $AB = (c_{ik})$ je tedy také horní trojúhelníková matice.

K důkazu (4) pouze doplníme předchozí důkaz (3) úvahou, čemu se rovná prvek c_{ii}. Je-li $j \neq i$, pak buď $i > j$ nebo $j > i$. V součtu definujícím c_{ii} je proto pouze jediný nenulový součin pro $j = i$, tj. $c_{ii} = a_{ii}b_{ii} = 1$.

Vlastnost (5) dokážeme přechodem k transponovaným maticím. Jsou-li A, B dolní trojúhelníkové matice, jsou obě transponované matice B^T a A^T horní trojúhelníkové. Podle bodu (3) je také součin $B^T A^T = (AB)^T$ horní trojúhelníková matice a proto je matice $AB = \left((AB)^T\right)^T$ dolní trojúhelníková.

Vlastnost (6) plyne analogicky ze (4). □

4.5. **Množina všech řešení soustavy lineárních rovnic.** V této části využijeme algebraické vlastnosti počítání s maticemi k dalšímu pochopení množiny všech řešení soustavy lineárních rovnic. V druhé kapitole jsme si ukázali, že množinu všech řešení soustavy

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

m lineárních rovnic o n neznámých nad tělesem $\mathbf{T}$ můžeme zapsat jako

$$\left\{ \mathbf{u} + \sum_{p \in P} t_p \mathbf{v}_p : \ t_p \in \mathbf{T} \ \text{ pro každé } \ p \in P \right\}$$

kde

- P je množina indexů volných proměnných,
- $\mathbf{u}$, $\mathbf{v}_p$, $p \in P$, jsou „vhodné“ n-složkové aritmetické vektory nad $\mathbf{T}$.

Hodnoty parametrů $t_p \in \mathbf{T}$ můžeme volit libovolně. Zvolíme-li $t_p = 0$ pro každé $p \in P$, dostaneme jedno řešení $\mathbf{x} = \mathbf{u}$. Zvolíme-li jeden z parametrů $t_p = 1$ a ostatní parametry rovné 0, dostaneme jiné řešení $\mathbf{x} = \mathbf{u} + \mathbf{v}_p$.

Pozorování 4.29. *Jsou-li* $\mathbf{u}$ *a* $\mathbf{w}$ *dvě řešení soustavy lineárních rovnic* $A\mathbf{x} = \mathbf{b}$*, pak* $\mathbf{w} - \mathbf{u}$ *je řešením soustavy* $A\mathbf{x} = \mathbf{o}$*.*

Důkaz. Protože jsou aritmetické vektory $\mathbf{u}, \mathbf{w}$ řešení soustavy $A\mathbf{x} = \mathbf{b}$, platí $A\mathbf{u} = A\mathbf{w} = \mathbf{b}$. Potom

$$A(\mathbf{w} - \mathbf{u}) = A(\mathbf{w} + (-\mathbf{u})) = A\mathbf{w} + A(-\mathbf{u}) = A\mathbf{w} + (-A\mathbf{u}) = \mathbf{b} + (-\mathbf{b}) = \mathbf{o} \ .$$

Použili jsme distributivitu násobení matic vzhledem k jejich sčítání, definici odčítání aritmetických vektorů, a první vlastnost z tvrzení 4.20. Vektor $\mathbf{w} - \mathbf{u}$ je proto řešením soustavy $A\mathbf{x} = \mathbf{o}$. □

Definice 4.30. Soustava $A\mathbf{x} = \mathbf{o}$ se nazývá *homogenní soustava lineárních rovnic* (příslušná k soustavě $A\mathbf{x} = \mathbf{b}$).

Pozorování 4.31. *Je-li* $\mathbf{u}$ *řešení soustavy* $A\mathbf{x} = \mathbf{b}$ *a* $\mathbf{v}$ *řešení příslušné homogenní soustavy* $A\mathbf{x} = \mathbf{o}$*, pak* $\mathbf{u} + \mathbf{v}$ *je také řešení soustavy* $A\mathbf{x} = \mathbf{b}$*.*

Důkaz spočívá v jednoduchém výpočtu

$$A(\mathbf{u} + \mathbf{v}) = A\mathbf{u} + A\mathbf{v} = \mathbf{b} + \mathbf{o} = \mathbf{b}$$

využívajícím opět distributivity.

Množina všech řešení homogenní soustavy $A\mathbf{x} = \mathbf{o}$ je důležitou charakteristikou matice A, která bude v dalším textu hrát významnou roli při zkoumání matic.

Definice 4.32. Množina všech řešení homogenní soustavy lineárních rovnic $A\mathbf{x} = \mathbf{o}$ se nazývá *jádro matice* A nebo také *nulový prostor matice* A. Označujeme ji $\operatorname{Ker} A$.

Z předchozích dvou jednoduchých pozorování plyne následující důležitá věta.

Věta 4.33. *Je-li* $\mathbf{u}$ *jedno pevně zvolené partikulární řešení soustavy lineárních rovnic* $A\mathbf{x} = \mathbf{b}$ *nad tělesem* $\mathbf{T}$*, pak se množina všech řešení této soustavy rovná*

$$\{\mathbf{u} + \mathbf{v} : \mathbf{v} \in \operatorname{Ker} A\} \quad = \quad \mathbf{u} + \operatorname{Ker} A \ .$$

Důkaz. Je-li $\mathbf{w}$ řešení soustavy $A\mathbf{x} = \mathbf{b}$, pak $\mathbf{w} - \mathbf{u} \in \operatorname{Ker} A$ podle pozorování 4.29 a tedy

$$\mathbf{w} = \mathbf{u} + (\mathbf{w} - \mathbf{u}) \in \{\mathbf{u} + \mathbf{v} : \mathbf{v} \in \operatorname{Ker} A\} \ .$$

Naopak pro libovolné $\mathbf{v} \in \operatorname{Ker} A$ je $\mathbf{u} + \mathbf{v}$ řešením soustavy $A\mathbf{x} = \mathbf{b}$ podle pozorování 4.31. □

4.6. **Matice jako zobrazení.**

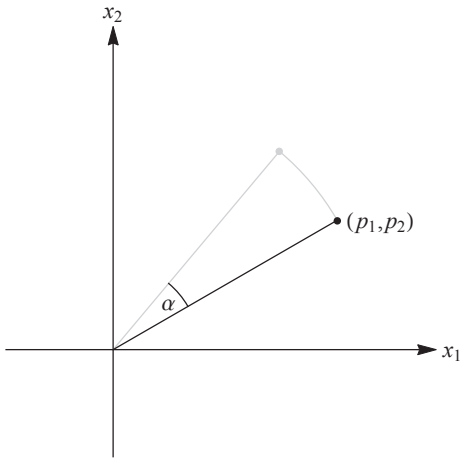
Ukážeme si nyní jak pomocí matic algebraicky popsat některá jednoduchá geometrická zobrazení v rovině.

4.6.1. *Zobrazení v rovině.* Začneme otočením kolem počátku souřadnic o úhel α v kladném směru, tj. proti směru hodinových ručiček.

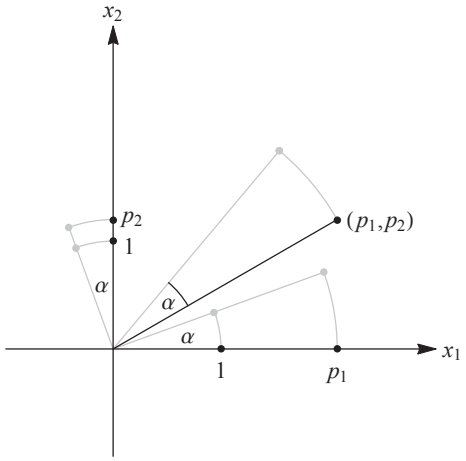
Příklad 4.34. Rovinu otočíme kolem počátku souřadnic o úhel α. Kam se pootočí bod se souřadnicemi (p_1, p_2), jaké budou jeho souřadnice po otočení?

Spočítat nové souřadnice přímo pomocí euklidovské geometrie je dost pracné. Ukážeme si algebraické řešení, na kterém lze vidět základní rysy lineárně algebraického uvažování. Místo toho, abychom počítali ihned souřadnice bodu, do kterého se pootočí bod $(p_1, p_2)^T$, se napřed zamyslíme nad tím, můžeme-li úlohu snadno vyřešit pro nějaké jiné body. Několik takových bodů vidíme na následujícím obrázku.

Snadno nahlédneme, že bod na první souřadné ose se souřadnicemi $(1, 0)^T$ se pootočí do bodu o souřadnicích $(\cos\alpha, \sin\alpha)^T$. Tím pádem také víme, že se bod $(p_1, 0)^T$ pootočí do bodu $(p_1 \cos\alpha, p_1 \sin\alpha)^T$.



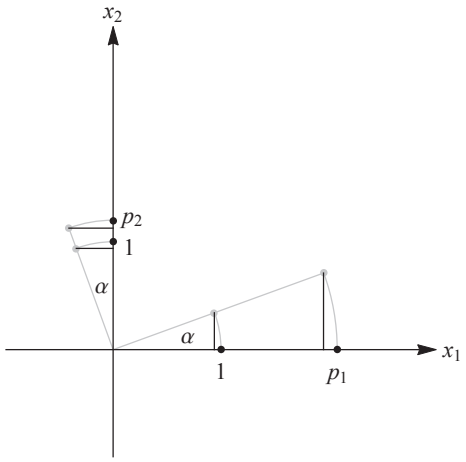
Obrázek 42. Otočení v rovině o úhel α v kladném směru



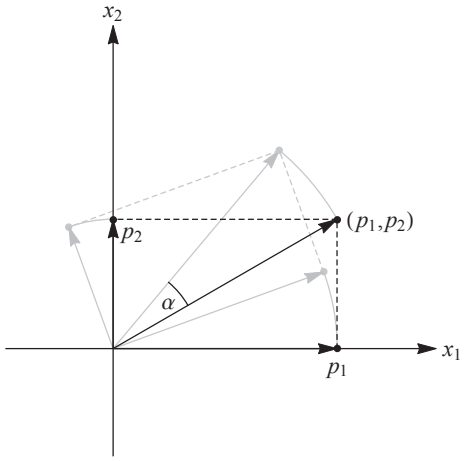
Obrázek 43. Otočení v rovině o úhel α podruhé

Podobně snadno nahlédneme, že bod na druhé souřadné ose se souřadnicemi $(0,1)^T$ se pootočí do bodu $(-\sin\alpha, \cos\alpha)^T$ a bod $(0,p_2)^T$ se pootočí do bodu $(-p_2\sin\alpha, p_2\cos\alpha)^T$.

Nyní přichází klíčový moment. Polohový vektor bodu $(p_1,p_2)^T$ je součtem polohových vektorů bodů $(p_1,0)^T$ a $(0,p_2)^T$. Tato vlastnost se otočením zachová – polohový vektor bodu, do kterého se pootočí bod $(p_1,p_2)^T$, je součtem polohových vektorů bodů, do kterých se pootočí body $(p_1,0)^T$ a $(0,p_2)^T$, tj. je součtem polohových vektorů bodů $(p_1\cos\alpha, p_1\sin\alpha)^T$ a $(-p_2\sin\alpha, p_2\cos\alpha)^T$.



OBRÁZEK 44. Otočení v rovině o úhel α potřetí



OBRÁZEK 45. Otočení v rovině o úhel α počtvrté

Bod se souřadnicemi $(p_1, p_2)^T$ se tedy pootočí do bodu se souřadnicemi

$$\begin{pmatrix} p_1 \cos\alpha \\ p_1 \sin\alpha \end{pmatrix} + \begin{pmatrix} -p_2 \sin\alpha \\ p_2 \cos\alpha \end{pmatrix} = p_1 \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix} + p_2 \begin{pmatrix} -\sin\alpha \\ \cos\alpha \end{pmatrix}$$
$$= \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} .$$

Můžeme říct, že matice

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

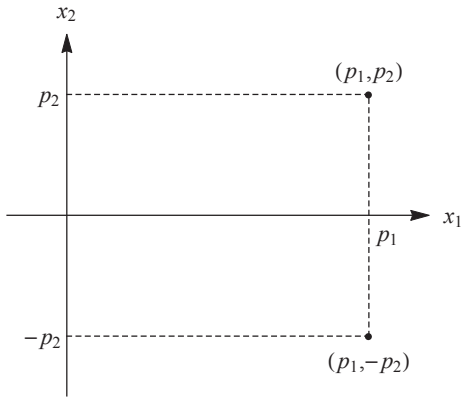
„určuje“ otočení kolem počátku souřadnic o úhel α v kladném směru. Všimněme si také, že první sloupec v matici tvoří souřadnice bodu, do kterého se zobrazí bod

$(1,0)^T$ na první souřadné ose. Podobně druhý sloupec matice tvoří souřadnice bodu, do kterého se zobrazí bod $(0,1)^T$ na druhé souřadné ose.

Také jiná geometrická zobrazení v rovině můžeme popsat pomocí vhodné matice.

Příklad 4.35. Osová symetrie vzhledem k první souřadné ose v rovině zobrazuje každý bod $(p_1,p_2)^T$ do bodu se souřadnicemi

$$\begin{pmatrix} p_1 \\ -p_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} .$$



Obrázek 46. Symetrie v rovině vzhledem k první souřadné ose

Všimněme si, že opět jsou ve sloupcích matice A obrazy bodu $(1,0)^T$ (v prvním sloupci) a bodu $(0,1)^T$ (ve druhém sloupci).

V obou příkladech jsme ze znalosti hodnot zobrazení (rotace nebo symetrie) v těchto dvou bodech mohli odvodit hodnotu zobrazení v každém dalším bodě roviny.

4.6.2. *Zobrazení určené maticí.* Pro každou matici A typu $m \times n$ nad tělesem $\mathbf{T}$ a každý n-složkový aritmetický vektor $\mathbf{x} \in \mathbf{T}^n$ je součin $A\mathbf{x} \in \mathbf{T}^m$. Matice A tak určuje zobrazení z $\mathbf{T}^n$ do $\mathbf{T}^m$ ve smyslu následující důležité definice.

Definice 4.36. Je-li A matice typu $m \times n$ nad tělesem $\mathbf{T}$, pak definujeme *zobrazení* $f_A : \mathbf{T}^n \to \mathbf{T}^m$ *určené maticí* A předpisem

$$f_A(\mathbf{x}) = A\mathbf{x}$$

pro každý aritmetický vektor $\mathbf{x} \in \mathbf{T}^n$.

Příklad 4.37. V příkladu 4.34 jsme zjistili, že rotace v rovině kolem počátku souřadnic o úhel α v kladném směru je zobrazení $f_A : \mathbb{R}^2 \to \mathbb{R}^2$ určené maticí

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

Také symetrie v rovině vzhledem k první souřané ose je podle příkladu 4.35 zobrazení určené maticí

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

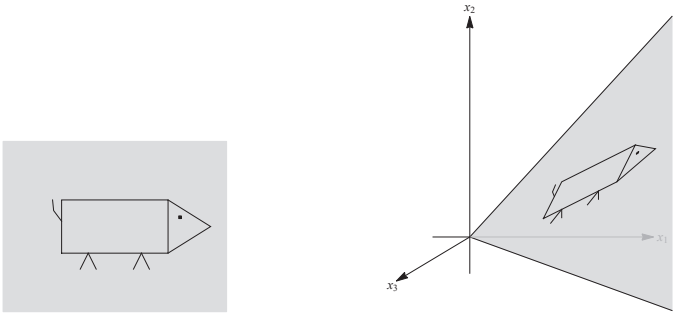
Příklad 4.38. Zobrazení $f_A : \mathbb{R}^2 \to \mathbb{R}^3$ určené maticí

$$A = \begin{pmatrix} 5 & 1 \\ 2 & 3 \\ 1 & -1 \end{pmatrix} = (\mathbf{a}_1|\mathbf{a}_2)$$

zobrazuje každý bod $(p_1, p_2)^T$ v rovině do bodu v 3-dimenzionálním prostoru se souřadnicemi

$$f_A((p_1, p_2)^T) = p_1\mathbf{a}_1 + p_2\mathbf{a}_2 \ ,$$

který leží v rovině s parametrickým vyjádřením $\{x_1\mathbf{a}_1 + x_2\mathbf{a}_2 : x_1, x_2 \in \mathbb{R}\}$.



Obrázek 47. Zobrazení určené reálnou maticí typu 3×2

Na obrázku vidíme několik bodů v rovině $\mathbb{R}^2$ a jejich obrazy v prostoru $\mathbb{R}^3$. Narozdíl od reálných funkcí jedné reálné proměnné si pro zobrazení f_A určené maticí A nemůžeme nakreslit graf, ze kterého bychom viděli hodnotu zobrazení v každém bodě definičního oboru.

Pro zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^m$ určené maticí A typu $m \times n$ nad tělesem $\mathbf{T}$ máme pouze předpis, jak pro daný vektor $\mathbf{x} = (x_1, x_2, \ldots, x_n)^T$ spočítat hodnotu zobrazení f_A v bodě $\mathbf{x}$:

$$f_A(\mathbf{x}) = A\mathbf{x} \ .$$

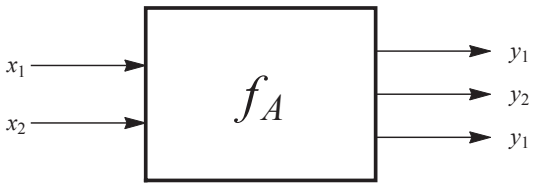
Důležité je ale také umět si představit zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^m$ jako celek, jako jeden objekt. Graf zobrazení nemáme k dispozici, můžeme ale využít blokové schéma používané v řadě inženýrských oborů. Elektroinženýr si zobrazení f_A představí jako nějaký obvod (konkrétních konstrukcí obvodu může být více), ve kterém lze měnit nějaké hodnoty x_1, x_2 na vstupu (například proudy), které ovlivní jiné hodnoty y_1, y_2, y_3 na výstupu (například napětí). Pokud si žádný obvod neumíme představit, můžeme zobrazení f_A považovat za „černou skříňku“. Na prvním obrázku je „černá skříňka“ reprezentující zobrazení z příkladu 4.38.

Zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^m$ určené obecnou maticí A typu $m \times n$ si pak můžeme představit jako na druhém obrázku:

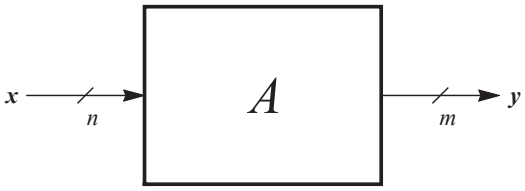
Zobrazení-černé skříňce můžeme klást dotazy typu *jaká je tvoje hodnota v prvku* $\mathbf{x} \in \mathbf{T}^n$? Je-li $A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ matice typu $m \times n$ nad tělesem $\mathbf{T}$ a $\mathbf{e}_1 = (1, 0, \ldots, 0^T) \in \mathbf{T}^n$, pak

$$f_A(\mathbf{e}_1) = 1\mathbf{a}_1 + 0\mathbf{a}_2 + \cdots + 0\mathbf{a}_n = \mathbf{a}_1 \ .$$

Sloupce v matici A tak můžeme zjistit jako hodnoty zobrazení f_A v dobře zvolených prvcích $\mathbf{T}^n$.



Obrázek 48. Zobrazení f_A určené maticí typu 3×2



Obrázek 49. Zobrazení f_A určené maticí typu $m \times n$

Definice 4.39. Je-li $\mathbf{T}$ nějaké těleso a $n \in \mathbb{N}$, pak pro každé $j = 1, 2, \ldots, n$ označíme $\mathbf{e}_j = (0, \ldots, 0, 1, 0, \ldots, 0)^T \in \mathbf{T}^n$ vektor, který má j-tou složku rovnou 1 a všechny ostatní složky rovné 0. Vektory $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$ nazýváme *prvky kanonické báze* v $\mathbf{T}^n$.

Pomocí prvků kanonické báze v $\mathbf{T}^n$ snadno dokážeme následující pozorování.

Pozorování 4.40. *Pro dvě matice A, B téhož typu $m \times n$ nad stejným tělesem $\mathbf{T}$ platí $f_A = f_B$ právě když $A = B$.*

Důkaz. Obě matice A, B zapíšeme pomocí sloupců, tj. $A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ a $B = (\mathbf{b}_1|\mathbf{b}_2|\cdots|\mathbf{b}_n)$. Z rovnosti $f_A = f_B$ plyne rovnost $\mathbf{a}_j = f_A(\mathbf{e}_j) = f_B(\mathbf{e}_j) = \mathbf{b}_j$ pro každé $j = 1, 2, \ldots, n$, matice A, B mají stejné soupce a proto se rovnají.

Opačná implikace je ještě snazší. Platí-li $A = B$, platí $\mathbf{a}_j = \mathbf{b}_j$ pro každé $j = 1, 2, \ldots, n$. Pro libovolný vektor $\mathbf{x} = (x_1, x_2, \ldots, x_n)^T \in \mathbf{T}^n$ pak platí

$$f_A(\mathbf{x}) = x_1\mathbf{a}_1 + \cdots + x_n\mathbf{a}_n = x_1\mathbf{b}_1 + \cdots + x_n\mathbf{b}_n = f_B(\mathbf{x}) \ .$$

□

Při odvození matice určující otočení v rovině kolem počátku souřadnic o úhel α v příkladu 4.34 jsme využili dvou vlastností rotace. Napřed jsme použili dvakrát skutečnost, že rotace kolem počátku zobrazí s-násobek nějakého vektoru do s-násobku obrazu tohoto vektoru. A nakonec jsme použili fakt, že rotace zobrazí součet dvou vektorů do součtu jejich obrazů. Tyto dvě vlastnosti má zobrazení určené jakoukoliv maticí.

Tvrzení 4.41. *Je-li A matice typu $m \times n$ nad tělesem $\mathbf{T}$, pak pro každé dva aritmetické vektory $\mathbf{x}, \mathbf{y} \in \mathbf{T}^n$ a každý prvek $s \in \mathbf{T}$ platí*

- $f_A(s\mathbf{x}) = s\, f_A(\mathbf{x})$,
- $f_A(\mathbf{x} + \mathbf{y}) = f_A(\mathbf{x}) + f_A(\mathbf{y})$.

Důkaz. Z první části tvrzení 4.20 dostáváme

- $f_A(s\mathbf{x}) = A(s\mathbf{x}) = s(A\mathbf{x}) = s\, f_A(\mathbf{x})$.

Podobně z definice 4.36 a distributivity násobení matic ihned plyne

- $f_A(\mathbf{x}+\mathbf{y}) = A(\mathbf{x}+\mathbf{y}) = A\mathbf{x} + A\mathbf{y} = f_A(\mathbf{x}) + f_A(\mathbf{y})$.

□

Poslední tvrzení říká, že zobrazení určená maticemi jsou velmi speciální.

4.6.3. *Zobrazení určená maticemi a součin matic.* Z definice 4.36 ihned dostaneme následující tvrzení.

Tvrzení 4.42. *Jsou-li A matice typu $m \times n$ a B matice typu $n \times p$ nad stejným tělesem $\mathbf{T}$, pak zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^m$ a $f_B : \mathbf{T}^p \to \mathbf{T}^n$ můžeme složit v pořadí $f_A f_B$ a pro složené zobrazení $f_A f_B : \mathbf{T}^p \to \mathbf{T}^m$ platí*

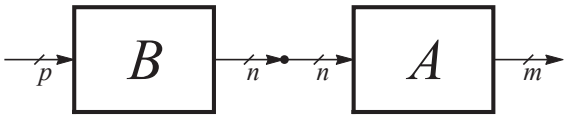
$$f_A f_B = f_{AB} \ .$$

Důkaz. Plyne ihned z asociativity násobení matic. Pro každý vektor $\mathbf{x} \in \mathbf{T}^p$ platí

$$f_A f_B(\mathbf{x}) = f_A(f_B(\mathbf{x})) = f_A(B\mathbf{x}) = A(B\mathbf{x}) = (AB)\mathbf{x} \ ,$$

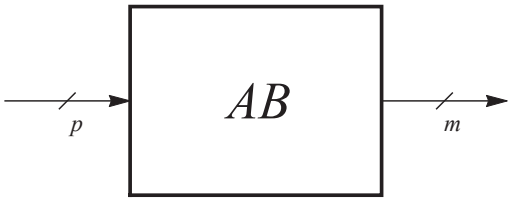
což dokazuje, že složené zobrazení $f_A f_B$ je určené součinem AB. □

Graficky můžeme složené zobrazení $f_A f_B$ znázornit jako



Obrázek 50. Diagram pro složení $f_A f_B$ zobrazení určených maticemi

Tvrzení 4.42 říká, že tento diagram můžeme nahradit jednodušším diagramem



Obrázek 51. Zobrazení f_{AB} určené součinem matic

Ukážeme si ještě, že pokud chceme, aby složení zobrazení určených maticemi A, B bylo určené nějakou maticí C, pak se C musí rovnat součinu matic AB.

Tvrzení 4.43. *Jsou-li A matice typu $m \times n$ a B matice typu $n \times p$ nad stejným tělesem $\mathbf{T}$, a C libovolná matice nad $\mathbf{T}$, pro kterou platí*

$$f_A f_B = f_C \ ,$$

pak platí $C = AB$.

Důkaz. Složené zobrazení $f_A f_B$ je definované na množině $\mathbf{T}^p$ a vede do množiny $\mathbf{T}^m$. Má-li pro matici C platit $f_C : \mathbf{T}^p \to \mathbf{T}^m$, musí být typu $m \times p$. Zapíšeme ji sloupcově $C = (\mathbf{c}_1|\mathbf{c}_2|\cdots|\mathbf{c}_p)$. Z předpokladu rovnosti $f_A f_B = f_C$ plyne, že pro každý vektor $\mathbf{e}_j$ kanonické báze v $\mathbf{T}^p$ platí

$$f_A f_B(\mathbf{e}_j) = f_C(\mathbf{e}_j) \ .$$

Na pravé straně dostáváme $f_C(\mathbf{e}_j) = \mathbf{c}_j$, zatímco vlevo vyjde

$$f_A f_B(\mathbf{e}_j) = f_A(B\mathbf{e}_j) = f_A(\mathbf{b}_j) = A\mathbf{b_j} \ ,$$

což je j-tý sloupec v součinu matic AB podle definice 4.12. Pro každé $j = 1, 2, \ldots, p$ se proto j-tý soupec součinu AB rovná j-tému sloupci $\mathbf{c}_j$ matice C. To dokazuje rovnost $C = AB$. □

4.6.4. *Další příklady.* Ukážeme si ještě nekolik příkladů, jejichž řešení je založené na tvrzení 4.42. Jako první dokážeme součtové vzorce pro funkce *sinus* a *cosinus*.

Příklad 4.44. Otočíme-li rovinu kolem počátku souřadnic o úhel β, je tato rotace podle příkladu 4.34 zobrazení $f_B : \mathbb{R}^2 \to \mathbb{R}^2$ určené maticí

$$B = \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix} \ .$$

Poté pootočíme rovinu kolem počátku ještě o úhel α v kladném směru. To je zobrazení $f_A : \mathbb{R}^2 \to \mathbb{R}^2$ určené maticí

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

Geometricky nahlédneme, že složením $f_A f_B$ těchto dvou rotací dostaneme rotaci kolem počátku o úhel $\alpha + \beta$ v kladném směru. Její matice je tedy

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

Matici složeného zobrazení $f_A f_B$ dostaneme rovněž jako součin matic

$$\begin{aligned} AB &= \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix} \\ &= \begin{pmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & -\cos\alpha\sin\beta - \sin\alpha\cos\beta \\ \sin\alpha\cos\beta + \cos\alpha\sin\beta & -\sin\alpha\sin\beta + \cos\alpha\cos\beta \end{pmatrix} \ . \end{aligned}$$

Protože matice zobrazení je určená jednoznačně podle tvrzení 4.40, plyne odtud rovnost matic

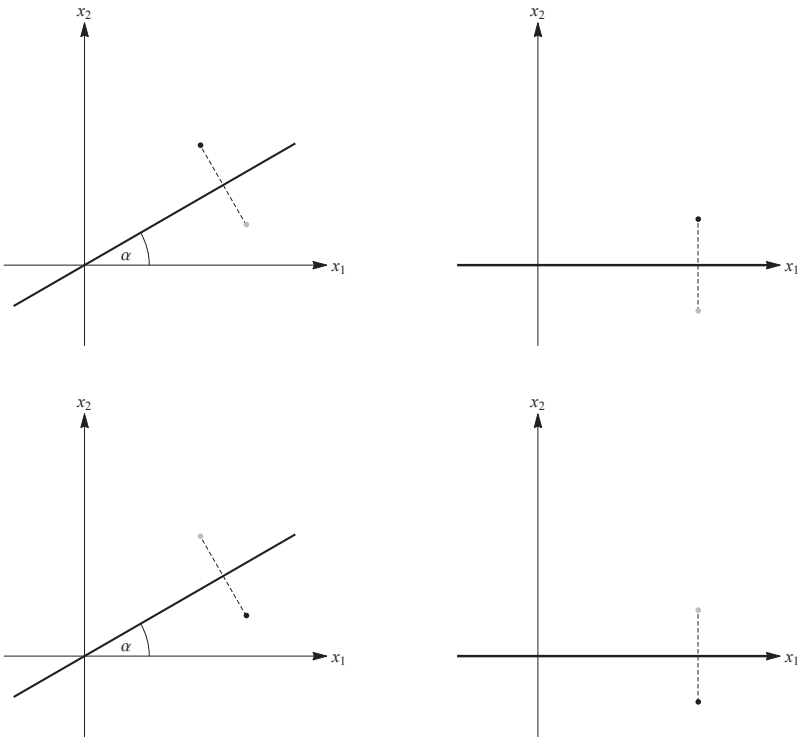
$$\begin{aligned} &\begin{pmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{pmatrix} \\ =&\begin{pmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & -\cos\alpha\sin\beta - \sin\alpha\cos\beta \\ \sin\alpha\cos\beta + \cos\alpha\sin\beta & -\sin\alpha\sin\beta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

Platí proto

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

pro libovolné dva úhly α, β.

Příklad 4.45. Odvodíme matici určující symetrie v rovině vzhledem k jakékoliv přímce procházející počátkem. Tato symetrie je složením tří zobrazení, jejichž matice už známe. Pokud osu symetrie dostaneme z první souřadné osy otočením o úhel α v kladném směru začneme tím, že osu symetrie otočíme do směru první souřadné osy po směru hodinových ručiček. Poté použijeme symetrii vzhledem k první souřadné ose a nakonec vše otočíme zpět.



Obrázek 52. Rozklad symetrie vzhledem k obecné přímce

Matici symetrie vzhledem k obecné přímce svírající úhel α s první souřadnou osou tak dostaneme jako součin matic

$$\begin{aligned}
&\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos(-\alpha) \end{pmatrix} \\
&= \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}\begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix} \\
&= \begin{pmatrix} \cos^2\alpha - \sin^2\alpha & 2\sin\alpha\cos\alpha \\ 2\sin\alpha\cos\alpha & \sin^2\alpha - \cos^2\alpha \end{pmatrix} = \begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix} .
\end{aligned}$$

Symetrie vzhledem k ose určené přímkou procházející počátkem souřadnic a bodem $(\cos\alpha, \sin\alpha)^T$ tak zobrazuje například bod o souřadnicích $(2,3)^T$ do bodu

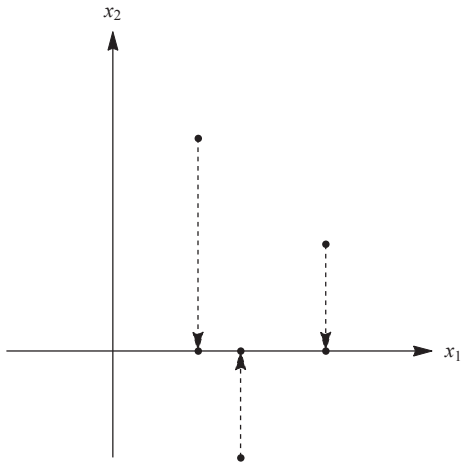
$$\begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix} \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 2\cos 2\alpha + 3\sin 2\alpha \\ 2\sin 2\alpha - 3\cos 2\alpha \end{pmatrix} .$$

Příklad 4.46. Jaké zobrazení dostaneme pokud uděláme rotaci kolem počátku o úhel α v kladném směru následovanou symetrií vzhledem k první souřadné ose? Toto složení je určené součinem matic

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ -\sin\alpha & -\cos\alpha \end{pmatrix} = \begin{pmatrix} \cos(-\alpha) & \sin(-\alpha) \\ \sin(-\alpha) & -\cos(-\alpha) \end{pmatrix} .$$

Na základě předchozího příkladu 4.45 tak můžeme odpovědět, že složené zobrazení je symetrie vzhledem k ose, kterou dostaneme z první souřadné osy otočením o úhel $\alpha/2$ v záporném směru, tj. po směru hodinových ručiček.

Příklad 4.47. Ortogonální projekce na první souřadnou osu v rovině zobrazuje každý bod $(x_1, x_2)^T$ do bodu $(x_1, 0)^T$ na první souřadné ose.



Obrázek 53. Projekce na první souřadnou osu

Odtud snadno dostaneme matici, která projekci na první souřadnou osu určuje. Platí totiž

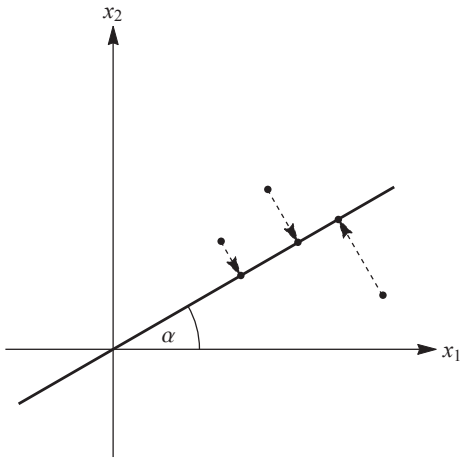
$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ 0 \end{pmatrix}$$

pro každý bod $(x_1, x_2)^T \in \mathbb{R}^2$.

Příklad 4.48. Podobně jako v příkladu 4.45 dostaneme matici určující ortogonální projekci na přímku procházející počátkem souřadnic a bodem $(\cos\alpha, \sin\alpha)^T$. Rovinu napřed otočíme o úhel $-\alpha$ tak, abychom přímku, na kterou projektujeme,

přesunuli do první souřadné osy. Poté uděláme projekci na první souřadnou osu, a nakonec otočíme rovinu o úhel α, abychom přímku, na kterou projektujeme, vrátili zpět do původního směru. Matici projekce pak dostaneme jako součin matic

$$\begin{aligned}
&\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos(-\alpha) \end{pmatrix} \\
&= \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} \cos\alpha & \sin\alpha \\ 0 & 0 \end{pmatrix} \\
&= \begin{pmatrix} \cos^2\alpha & \sin\alpha\cos\alpha \\ \sin\alpha\cos\alpha & \sin^2\alpha \end{pmatrix} .
\end{aligned}$$



Obrázek 54. Projekce na přímku

Příklad 4.49. Podíváme se ještě jednou na příklad 3.17 z konce kapitoly o tělesech. Tam jsme v $\mathbb{R}^3$ pomocí kvaternionů skládali rotaci kolem první souřadné osy o úhel $\pi/2$ s rotací kolem třetí souřadné osy o úhel $\pi/2$.

Matici B rotace kolem osy x_1 o úhel $\pi/2$ dostaneme tak, že do sloupců zapíšeme obrazy prvků $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ kanonické báze:

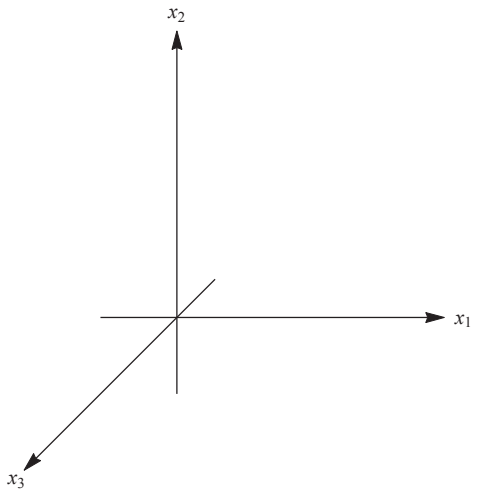
$$B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} .$$

Analogicky dostaneme matici A rotace kolem osy x_3 o úhel $\pi/2$:

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

Složením je zobrazení $f_A f_B = f_{AB}$ určené součinem matic

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



Obrázek 55. Kladně orientovaný souřadný systém v prostoru

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

$$f_{AB}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_3 \\ x_1 \\ x_2 \end{pmatrix} \ .$$

Odtud vidíme, že složené zobrazení $f_A f_B$ zobrazuje každý vektor $(x, x, x)^T$ opět do vektoru $(x, x, x)^T$. Osa výsledné rotace je tedy osou prvního oktantu. Není ale vidět, že jde o rotaci o úhel $2\pi/3$ v kladném směru, jak jsme zjistili výpočtem pomocí kvaternionů.

Příklad 4.50. Jednotková matice I_n řádu n nad tělesem $\mathbf{T}$ určuje zobrazení $f_{I_n} : \mathbf{T}^n \to \mathbf{T}^n$. Pro libovolný vektor $\mathbf{x} \in \mathbf{T}^n$ platí

$$f_{I_n}(\mathbf{x}) = I_n\mathbf{x} = \mathbf{x} \ ,$$

jednotková matice I_n tedy určuje identické zobrazení na množině $\mathbf{T}^n$ všech n-složkových aritmetických vektorů nad tělesem $\mathbf{T}$.

Identické zobrazení na množině $\mathbf{T}^n$ budeme v dalším textu označovat $\mathrm{id}_{\mathbf{T}^n}$.

4.6.5. *Elementární matice.* Tvrzení 4.22 naznačuje, že elementární řádkovou úpravu nějaké matice C lze provést také tak, že matici C vynásobíme zleva vhodnou čtvercovou maticí. Je tomu skutečně tak, jak ukazuje následující tvrzení.

Tvrzení 4.51. *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.*

$$E = \begin{matrix} \\ i \\ \\ j \\ \\ \end{matrix} \begin{matrix} \begin{matrix} & & & i & & j & & \end{matrix} \\ \begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \ddots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix} \end{matrix} .$$

(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.*

$$E = \begin{matrix} \\ i \\ \\ \end{matrix} \begin{matrix} \begin{matrix} & & & i & & & \end{matrix} \\ \begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & t & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix} \end{matrix} .$$

(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.*

$$E = \begin{matrix} \\ i \\ \\ \\ \\ \end{matrix} \begin{matrix} \begin{matrix} & & & i & & j & & \end{matrix} \\ \begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & \cdots & t & \cdots & 0 \\ \vdots & \vdots & & \vdots & \ddots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots & & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix} \end{matrix} .$$

Důkaz. Pozorování plyne z první části tvrzení 4.22. □

Definice 4.52. Maticím E z předchozího tvrzení říkáme *elementární matice.*

Elementární matice využijeme za chvilku při výpočtu inverzních matic a při dalším zkoumání průběhu Gaussovy eliminace.

4.7. **Regulární matice.** V další části této kapitoly se budeme zabývat otázkou, kdy ke čtvercové matici existuje inverzní matice.

4.7.1. *Algebraický a geometrický pohled.* Začneme algebraickou definicí.

Definice 4.53. 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}.

Geometricky si matici A představujeme jako zobrazení f_A určené maticí A. K zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^n$ existuje inverzní zobrazení právě když f_A je vzájemně jednoznačné zobrazení, tj. prosté a obor hodnot f_A se rovná $\mathbf{T}^n$. Místo vzájemně jednoznačné zobrazení se také používá termín *bijekce*.

Definice 4.54. Čtvercová matice A nad tělesem $\mathbf{T}$ řádu n se nazývá *regulární*, pokud je zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^n$ určené maticí A vzájemně jednoznačné (tj. bijekce).

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

Připomeňme, že zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^n$ je definované předpisem $f_A(\mathbf{x}) = A\mathbf{x}$ pro libovolný vektor $\mathbf{x} \in \mathbf{T}^n$. Vzájemná jednoznačnost zobrazení f_A znamená, že pro každý vektor $\mathbf{b} \in \mathbf{T}^n$ existuje právě jeden vektor $\mathbf{x} \in \mathbf{T}^n$, pro který platí $f_A(\mathbf{x}) = A\mathbf{x} = \mathbf{b}$. Platí proto následující pozorování.

Pozorování 4.55. *Matice A je regulární právě když soustava $A\mathbf{x} = \mathbf{b}$ má právě jedno řešení pro každou pravou stranu $\mathbf{b}$.*

Stejně snadno dokážeme také další tvrzení.

Tvrzení 4.56. *Každá invertovatelná matice je regulární.*

Důkaz. Je-li A invertovatelná, existuje matice X, pro kterou platí $AX = XA = I_n$. Podle tvrzení 4.42 platí pro zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^n$ a $f_X : \mathbf{T}^n \to \mathbf{T}^n$ rovnosti

$$f_A f_X = f_{I_n} = \mathrm{id}_{\mathbf{T}^n}, \quad f_X f_A = f_{I_n} = \mathrm{id}_{\mathbf{T}^n} \ .$$

Použili jsme fakt, že zobrazení f_{I_n} je identické zobrazení na množině $\mathbf{T}^n$, viz příklad 4.50. Zobrazení f_X určené maticí X je tedy inverzní k f_A, což dokazuje, že zobrazení f_A je vzájemně jednoznačné. □

Příklad 4.57. Z geometrického náhledu vidíme, že matice odpovídající rotaci kolem počátku a symetrii vzhledem k přímce procházející počátkem jsou regulární, protože tato zobrazení jsou vzájemně jednoznačná. Inverzní matice X k matici rotace o úhel α

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

musí určovat inverzní zobrazení k této rotaci, a geometricky vidíme, že inverzním zobrazením je rotace o úhel $-\alpha$. Zvolíme-li

$$X = \begin{pmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos -(\alpha) \end{pmatrix} = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} \ ,$$

snadno ověříme, že $AX = XA = I_2$.

Matice symetrie vzhledem k přímce procházející počátkem a bodem $(\cos\alpha, \sin\alpha)^T$ se rovná

$$B = \begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix} \ .$$

Výpočtem snadno ověříme, že $B^2 = I_2$, neboli že inverzní matice k B je opět B, což odpovídá geometrickému faktu, že symetrie vzhledem k přímce je inverzní k sobě samé.

Matice určující projekci na osu x_1 v $\mathbb{R}^2$ je singulární, protože projekce roviny na přímku není vzájemně jednoznačné zobrazení (dokonce není ani prosté ani na celý

prostor $\mathbb{R}^2$). Projekce je určená maticí

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

která proto nemůže být invertovatelná. O tom se snadno přesvědčíme, neboť pro každou čtvercovou matici X řádu 2 je druhý řádek součinu CX nulový, proto $CX \neq \mathbf{I}_2$. V součinu XC je vždy nulový druhý sloupec, proto také $XC \neq I_2$.

Stejně jako v případě inverzních prvků v tělese je také inverzní matice k matici A určená jednoznačně, pokud existuje. Protože násobení čtvercových matic stejného řádu není komutativní operace, můžeme jednoznačnost inverzní matice formulovat opatrněji.

Pozorování 4.58. *Jsou-li A, X, Y čtvercové matice stejného řádu n nad stejným tělesem $\mathbf{T}$, pro které platí $YA = I_n$ a $AX = I_n$, pak platí $Y = X$. Speciálně je inverzní matice k invertovatelné matici určená jednoznačně.*

Důkaz. Stačí využít asociativitu násobení matic:

$$Y = YI_n = Y(AX) = (YA)X = I_nX = X \ .$$

□

Neformálně budeme říkat, že platí-li pro nějaké dvě matice (nemusí být ani čtvercové) X, A rovnost $AX = I_n$, pak X je *inverzní zprava* k matici A a A je *inverzní zleva* k matici X. Poslední pozorování tedy říká, že v případě čtvercových matic se každá matice inverzní zleva k matici A rovná každé matici inverzní zprava k A.

Zdůrazněme ale ještě jednou, že pojmy invertovatelné a regulární matice se týkají **pouze čtvercových matic**.

Ukázali jsme už, že každá invertovatelná matice je regulární. Opačnou implikaci dokážeme tím, že popíšeme postup jak najít inverzní matici ke každé regulární matici.

4.7.2. *Hledání matice inverzní zprava.* K dané regulární matici A řádu n napřed najdeme matici X takovou, že $AX = I_n$. Budeme provádět obecnou diskuzi a zároveň ji ilustrovat na příkladu reálné matice

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

Především si všimneme, že sloupce jednotkové matice I_n jsou prvky $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$ kanonické báze v $\mathbf{T}^n$, tj. sloupcový zápis jednotkové matice I_n je $(\mathbf{e}_1|\mathbf{e}_2|\cdots|\mathbf{e}_n)$. Rovnost $AX = I_n$ pomocí definice součinu matic přepíšeme do tvaru

$$A(\mathbf{x}_1|\mathbf{x}_2|\cdots|\mathbf{x}_n) = (A\mathbf{x}_1|A\mathbf{x}_2|\cdots|A\mathbf{x}_n) = (\mathbf{e}_1|\mathbf{e}_2|\cdots|\mathbf{e}_n) \ .$$

Nalezení čtvercové matice $X = (\mathbf{x}_1|\mathbf{x}_2|\cdots|\mathbf{x}_n)$, pro kterou platí $AX = I_n$, se tak redukuje na řešení n soustav lineárních rovnic $A\mathbf{x}_i = \mathbf{e}_i$ pro $i = 1, 2, \ldots, n$.

Řešíme soustavy lineárních rovnic se stejnou maticí A a s různými pravými stranami. Protože A je regulární matice, každá soustava má jednoznačné řešení podle poznámky 4.55.

V našem konkrétním příkladě potřebujeme vyřešit soustavy

$$\begin{pmatrix} 1 & 3 \\ 2 & 9 \end{pmatrix} \begin{pmatrix} x_{11} \\ x_{12} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 3 \\ 2 & 9 \end{pmatrix} \begin{pmatrix} x_{21} \\ x_{22} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \ .$$

Tak je vyřešíme.

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

$$\left(\begin{array}{cc|c} 1 & 3 & 0 \\ 2 & 9 & 1 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 3 & 0 \\ 0 & 3 & 1 \end{array}\right), \quad \begin{pmatrix} x_{12} \\ x_{22} \end{pmatrix} = \begin{pmatrix} -1 \\ 1/3 \end{pmatrix}.$$

Matice inverzní zprava k matici $A = \begin{pmatrix} 1 & 3 \\ 2 & 9 \end{pmatrix}$ je tedy

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

Provedeme nyní dvě modifikace tohoto postupu.

Protože je matice všech n soustav stejná, totiž A, je možné všechny soustavy řešit stejnými řádkovými 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 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 uvědomíme, jak vypadá odstupňovaný tvar matice A po Gaussově eliminaci. Z předpokladu regularity matice A plyne, že rovnice $A\mathbf{x} = \mathbf{b}$ má právě jedno řešení pro každé $\mathbf{b}$. Při řešení soustav $A\mathbf{x}_i = \mathbf{e}_i$, tak nedostaneme žádné volné proměnné. Tím pádem musí pro odstupňovaný tvar matice A platit $r = n$ a $k_1 = 1, k_2 = 2, \ldots, k_n = n$, což znamená, že hodnost matice A je n a všechny její sloupce jsou bázové. Ještě jinými slovy, odstupňovaný tvar matice A je horní trojúhelníková matice s nenulovými prvky na hlavní diagonále.

Slíbená druhá modifikace. Po převedení soustav na odstupňovaný tvar budeme dále pokračovat v řádkových úpravách tak, abychom na levé straně dostali jednotkovou matici I_n. To lze provést díky tomu, že odstupňovaný tvar je horní trojúhelníková matice s nenulovými prvky na hlavní 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 hlavní diagonále, ze které umíme udělat jednotkovou vynásobením řádků vhodnými nenulovými prvky.

V našem případě máme

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

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

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

4.7.3. *Hledání matice inverzní zleva.* Ukázali jsme, že k regulární matici A existuje matice X inverzní zprava, tj. platí $AX = I_n$. K důkazu, že X je inverzní matice k A stačí dokázat, že také $XA = I_n$. Díky pozorování 4.58 nám stačí najít jakoukoliv matici Y řádu n, která je inverzní zleva k A.

Ve skutečnosti jsme ji už našli v průběhu elementárních řádkových úprav

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

vedoucích k matici X.

Podívejme se na tento postup pomocí elementárních matic. V tvrzení 4.51 jsme nahlédli, že každá elementární řádková úprava nějaké matice odpovídá násobení této matice nějakou elementární maticí zleva. Připomeňme, že všechny elementární matice jsou čtvercové, a tedy stejného řádu jako matice A. Úpravy lze zapsat jako

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

kde $E_1, E_2, \dots$ jsou elementární matice příslušných elementárních řádkových úprav.

Vezmeme-li v úvahu asociativitu násobení matic a pravidlo o násobení po blocích, můžeme postup zapsat ve tvaru

$$\begin{aligned}(A \mid I_n) \sim (E_1A \mid E_1I_n) = (E_1A \mid E_1) \sim (E_2E_1A \mid E_2E_1) \sim \cdots \sim \\ \sim (E_k \dots E_2E_1A \mid E_k \dots E_2E_1) = (I_n \mid X) \ .\end{aligned}$$

Srovnáním levých bloků v poslední rovnosti dostáváme, že pro matici $Y = E_k \dots E_2E_1$ platí $YA = I_n$, takže matice Y je inverzní zleva k matici A. Na základě pozorování 4.58 můžeme konstatovat, že $Y = X$. Tuto rovnost také získáme srovnáním pravých bloků v poslední rovnosti předchozího výpočtu.

Pro matici X nalezenou v části 4.7.2 tedy platí $XA = AX = I_n$, tj. X je inverzní matice k matici A. Současně jsme zjistili, že X můžeme vyjádřit jako součin elementárních matic.

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

Věta 4.59. *Pro čtvercovou matici A řádu n nad tělesem $\mathbf{T}$ jsou následující tvrzení ekvivalentní:*

(1) *matice A je regulární,*
(2) *zobrazení f_A je na $\mathbf{T}^n$,*
(3) *zobrazení f_A je prosté,*
(4) *homogenní 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 hlavní diagonále (ekvivalentně do odstupňovaného tvaru bez nulových řádků),*
(6) *matici A lze převést elementárními řádkovými úpravami do jednotkové matice I_n,*
(7) *matice A je invertovatelná,*
(8) *existuje čtvercová matice X řádu n taková, že $AX = I_n$,*
(9) *existuje čtvercová matice Y řádu n taková, že $YA = I_n$,*
(10) *matice 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.

(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 sloupce, 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 později v tvrzení 4.66.

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) ⇒ (3) se dokáže obdobně. □

Příklad 4.60. Najdeme matici inverzní k matici A nad tělesem $\mathbb{Z}_5$, pokud existuje.

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

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

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

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

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

Takže A je regulární a platí

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

Příklad 4.61. 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 $(A \mid I_n)$:

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

Odstupňovaný tvar matice A není horní trojúhelníková matice s nenulovými prvky na diagonále, takže A je singulární podle (1)⇔(5) z věty 4.59. 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 4.62. Někdy je výhodnější se trochu zamyslet než ihned začít počítat podle uvedeného algoritmu. Příkladem je výpočet inverzní matice k reálné matici

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

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 4.22. Druhý řádek matice A nám říká, že druhý řádek výsledné matice I_3, tj. řádek $(0, 1, 0)$, je $1/2$-násobek prvního řádku matice X. Z toho okamžitě vidíme, že první řádek matice X je $(0, 2, 0)$.

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

Z posledního řádku matice A vidíme, že třetí řádek výsledku I_3, tj. $(0, 0, 1)$, je roven 1-násobku prvního řádku matice X (o tom už víme, že se rovná $(0, 2, 0)$) plus $1/3$-násobku 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 4.63. Pokud A je regulární matice, pak každá soustava rovnic $A\mathbf{x} = \mathbf{b}$ má podle definice regulární matice 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

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

kde A^{-1} jsme spočítali v příkladu 4.60.

K numerickému řešení konkrétních rovnic se vzorec $\mathbf{x} = A^{-1}\mathbf{b}$ nehodí, protože Gaussova eliminace a zpětná substituce je rychlejší postup. Stejně jako v části 2.7 můžeme spočítat, že samotný výpočet inverzní matice převedením matice $(A|I_n)$ do matice $(I_n|A^{-1})$ pomocí elementárních řádkových úprav vyžaduje

$$n^3 \ \text{ násobení/dělení a } \ n^3 - 2n^2 + n \ \text{ sčítání/odčítání } .$$

K tomu je třeba ještě připočíst počet operací nutných k výpočtu součinu $A^{-1}\mathbf{b}$, který se rovná

$$n^2 \ \text{ násobení/dělení a } \ n^2 - n \ \text{ sčítání/odčítání } .$$

Celkem tedy řešení soustavy $A\mathbf{x} = \mathbf{b}$ s regulární maticí A pomocí vzorce $\mathbf{x} = A^{-1}\mathbf{b}$ vyžaduje

$$n^3 + n^2 \ \text{ násobení/dělení a } \ n^3 - n^2 \ \text{ sčítání/odčítání } .$$

Pro velká n je to zhruba třikrát více aritmetických operací než je třeba na Gaussovu eliminaci a zpětnou substituci.

Vzorec se spíš hodí pro teoretické úvahy, kdy potřebujeme zapsat řešení obecné soustavy lineárních rovnic s regulární maticí.

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

Tvrzení 4.64. *Každá elementární matice je regulární, navíc inverzní matice k elementární matici je opět elementární.*

Důkaz. K důkazu můžeme přímo najít matice inverzní, jsou jimi matice úprav, které ruší efekt příslušné elementární úpravy. Pak pouze využijeme ekvivalenci invertovatelnosti a regulárnosti z charakterizační věty 4.59. □

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

Tvrzení 4.65. *Jsou-li A, B regulární matice stejného řádu n nad stejným tělesem $\mathbf{T}$ 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 4.59.

Tvrzení 4.66. *Čtvercová matice A je regulární právě tehdy, když jde napsat jako součin elementárních matic.*

Důkaz. Každá elementární matice je regulární podle tvrzení 4.64, takže podle bodu (4) v předchozím tvrzení je libovolný součin elementárních matic regulární matice. To dokazuje implikaci zprava doleva.

Naopak, je-li A regulární, pak ji lze elementárními řádkovými úpravami převést na jednotkovou matici (podle bodu (6) charakterizační věty 4.59). Elementární řádkové úpravy se dají napsat jako násobení zleva elementární maticí, takže existují elementární matice $E_1, E_2, \ldots, E_k$ takové, že

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

kde n je řád A. Protože elementární matice jsou regulární (podle tvrzení 4.64), tedy i invertibilní, můžeme vztah upravit na

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

Teď jsme hotovi, protože inverzní matice k elementárním maticím jsou elementární (opět podle tvrzení 4.64). □

Příklad 4.67. Z důkazu také vidíme postup, jak rozklad na elementární matice nalézt. Najdeme rozklad matice

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

nad $\mathbb{Z}_5$. 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

$$\begin{aligned} A =& E_1^{-1}E_2^{-1}E_3^{-1}E_4^{-1}E_5^{-1} \\ =& \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 3 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix} . \end{aligned}$$

Nyní můžeme také rozhodnout, kdy lze jednu matici dostat z druhé posloupností elementárních řádkových úprav. Uvažujme dvě matice A, B stejného typu (nad stejným tělesem). Pokud B vznikla z A posloupností elementárních úprav, pak pro příslušné elementární matice $E_1, \dots, E_k$, které popisují provedené úpravy, platí

$$B = E_k \cdots E_2 E_1 A \ .$$

Podle tvrzení 4.66 je matice $R = E_k \cdots E_1$ regulární.

Naopak, pokud $B = RA$ pro nějakou regulární matici R, pak podle stejného tvrzení platí $R = E_k \cdots E_2 E_1$ pro nějaké elementární matice $E_1, \dots, E_k$. Z toho vyplývá, že B lze z A získat posloupností elementárních úprav. Dokázali jsme následující tvrzení.

Tvrzení 4.68. *Nechť A, B jsou matice typu $m \times n$ nad tělesem $\mathbf{T}$. Pak B lze z A získat posloupností elementárních řádkových úprav právě tehdy, když existuje regulární matice R řádu m nad $\mathbf{T}$ taková, že $B = RA$.*

4.8. **Maticový zápis Gaussovy eliminace, LU-rozklad.** Začneme podrobným rozborem jednoho příkladu.

Příklad 4.69. Máme vyřešit soustavu

$$\left(\begin{array}{ccc|c} 2 & 2 & 2 & 1 \\ 4 & 7 & 7 & 2 \\ 6 & 18 & 22 & 7 \end{array}\right) .$$

Gaussovo eliminací dostaneme

$$\left(\begin{array}{ccc|c} 2 & 2 & 2 & 1 \\ 4 & 7 & 7 & 2 \\ 6 & 18 & 22 & 7 \end{array}\right) \sim \left(\begin{array}{ccc|c} 2 & 2 & 2 & 1 \\ 0 & 3 & 3 & 0 \\ 0 & 12 & 16 & 4 \end{array}\right) \sim \left(\begin{array}{ccc|c} 2 & 2 & 2 & 1 \\ 0 & 3 & 3 & 0 \\ 0 & 0 & 4 & 4 \end{array}\right)$$

a po zpětné substituci vyjde řešení $(x_1, x_2, x_3)^T = (1/2, -1, 1)$.

Poté nám zadavatel úlohy řekne, že se spletl a dal nám pravou stranu v opačném pořadí, že vlastně potřebuje vyřešit soustavu

$$\left(\begin{array}{ccc|c} 2 & 2 & 2 & 7 \\ 4 & 7 & 7 & 2 \\ 6 & 18 & 22 & 1 \end{array}\right) .$$

Tak znovu Gaussova eliminace

$$\left(\begin{array}{ccc|c} 2 & 2 & 2 & 7 \\ 4 & 7 & 7 & 2 \\ 6 & 18 & 22 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|c} 2 & 2 & 2 & 7 \\ 0 & 3 & 3 & -12 \\ 0 & 12 & 16 & -20 \end{array}\right) \sim \left(\begin{array}{ccc|c} 2 & 2 & 2 & 7 \\ 0 & 3 & 3 & -12 \\ 0 & 0 & 4 & 28 \end{array}\right)$$

a po zpětné substituci odevzdáme nový výsledek $(x_1, x_2, x_3)^T = (15/2, -11, 7)$.

Zadavatel pohlédne na výsledek, chytne se za hlavu a prohlásí něco v tom smyslu, že nesjpíš tu pravou stranu špatně odečetl na přístrojích, a jestli bychom mu to nespočítali ještě jednou s pravou stranou rovnou $(6, 24, 70)^T$.

Dříve než mu ublížíme, se raději zamyslíme nad tím, že při řešení budeme znovu používat ty samé elementární řádkové úpravy jako poprvé, a možná bychom první řešení mohli nějak využít k urychlení dalších výpočtů.

Vzpomeneme si, že každé elementární řádkové úpravě odpovídá nějaká elementární matice, kterou soustavu násobíme zleva. V našem případě jsme násobili postupně elementárními maticemi

$$E_1 = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad E_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -3 & 0 & 1 \end{pmatrix}, \quad E_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -4 & 1 \end{pmatrix} .$$

Celý průběh Gaussovy eliminace tak zaznamenáme jako součin matic

$$\begin{aligned} R = E_3E_2E_1 &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -3 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 5 & -4 & 1 \end{pmatrix} . \end{aligned}$$

Protože jsme nemuseli prohazovat řádky, používali jsme pouze třetí elementární úpravu a navíc v podobě přičtení vhodného násobku nějakého řádku k řádku pod ním, což znamená, že jsme násobili pouze dolními trojúhelníkovými maticemi s jednotkami na hlavní diagonále. Jejich součin R je proto také dolní trojúhelníková matice s jednotkami na hlavní diagonále podle tvrzení 4.28.6.

Řešíme-li další soustavu $(A|\mathbf{b})$ se stejnou maticí soustavy A Gaussovo eliminací, násobíme ji opět zleva maticí $R = E_3E_2E_1$. Po Gaussově eliminaci tak dostaneme soustavu $R(A|\mathbf{b}) = (RA|R\mathbf{b})$. Součin matic $RA = E_3E_2E_1A$ navíc známe hned po první Gaussově eliminaci, neboť

$$RA = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 5 & -4 & 1 \end{pmatrix} \begin{pmatrix} 2 & 2 & 2 \\ 4 & 7 & 7 \\ 6 & 18 & 22 \end{pmatrix} = \begin{pmatrix} 2 & 2 & 2 \\ 0 & 3 & 3 \\ 0 & 0 & 4 \end{pmatrix} .$$

Při každém dalším pokusu uspokojit zadavatele tak potřebujeme vyřešit soustavu

$$U\mathbf{x} = RA\mathbf{x} = R\mathbf{b}$$

se známou horní trojúhelníkovou maticí $U = RA$. Tu můžeme vyřešit zpětnou substitucí, problém ale zůstává s pravou stranou, neboť ta vyžaduje provést všechny elementární řádkové úpravy použité při prvním výpočtu na nový vektor pravých stran.

Také výpočtu $R\mathbf{b}$ se lze vyhnout. Součin elementárních matic $R = E_3E_2E_1$ rozdělíme na dvě části $E_3(E_2E_1)$. Součin E_2E_1 odpovídá prvnímu cyklu Gaussovy eliminace – eliminaci prvního sloupce – a rovná se

$$E_2E_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -3 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ -3 & 0 & 1 \end{pmatrix} .$$

Součin E_2E_1 známe hned po první Gaussově eliminaci. Kromě jednotek na hlavní diagonále obsahuje v prvním sloupci koeficienty násobků prvního řádku, které přičítáme k řádkům pod ním během eliminace prvního sloupce. K druhému řádku jsme přičítali (-2)-násobek prvního řádku, ke třetímu (-3)-násobek. Můžeme tak říct, že součin E_2E_1 je záznamem prvního cyklu Gaussovy eliminace.

Podobně je matice

$$E_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -4 & 1 \end{pmatrix}$$

záznamem o eliminaci druhého sloupce matice A, tj. druhém cyklu Gaussovy elimkinace.

Obě matice E_2E_1 a E_3 mají tak jednoduchou strukturu, že můžeme přímo napsat matice k nim inverzní:

$$(E_2E_1)^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 3 & 0 & 1 \end{pmatrix}, \qquad E_3^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 4 & 1 \end{pmatrix} .$$

Můžeme proto také hned spočítat matici R^{-1} inverzní k součinu $R = E_3(E_2E_1)$:

$$R^{-1} = (E_2E_1)^{-1}E_3^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 3 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 3 & 4 & 1 \end{pmatrix} .$$

Matice R^{-1} je záznamem o celém průběhu Gaussovy eliminace při řešení první soustavy. Je to dolní trojúhelníková matice s jednotkami na hlavní diagonále a na místě (i, j) pod hlavní diagonálou je prvek opačný k číslu, kterým jsme násobili j-tý řádek při eliminaci prvku na místě (i, j).

Díky tomu, že matici R^{-1} známe hned po první Gaussově eliminaci, v tomto kontextu je vždy označována L, upravíme si soustavu $U\mathbf{x} = R\mathbf{b}$ do tvaru

$$R^{-1}U\mathbf{x} = LU\mathbf{x} = \mathbf{b} .$$

Protože $U = RA$, platí $LU = R^{-1}RA = A$. Matici A tak máme vyjádřenou jako součin dolní trojúhelníkové matice L s horní trojúhelníkovou maticí U. Podstatné je, že obě matice L a U známe poté, co jsme jednou použili Gaussovu eliminaci na matici A a *v jejím průběhu jsme nepoužili prohazování řádků.*

Řešení soustavy $LU\mathbf{x} = \mathbf{b}$ můžeme rozdělit na řešení dvou soustav. Napřed vyřešíme soustavu $L\mathbf{y} = \mathbf{b}$ s dolní trojúhelníkovou maticí a poté soustavu $U\mathbf{x} = \mathbf{y}$ s horní trojúhelníkovou maticí. Dá-li nám zadavatel novou pravou stranu $(6, 24, 70)^T$, nemrkneme okem a napřed vyřešíme *přímou substitucí* soustavu

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & 6 \\ 2 & 1 & 0 & 24 \\ 3 & 4 & 1 & 70 \end{array}\right) ,$$

dostaneme řešení $\mathbf{y} = (6, 12, 4)^T$. Poté použijeme zpětnou substituci na řešení soustavy

$$\left(\begin{array}{ccc|c} 2 & 2 & 2 & 6 \\ 0 & 3 & 3 & 12 \\ 0 & 0 & 4 & 4 \end{array}\right)$$

a dostaneme řešení $\mathbf{x} = (-1, 3, 1)^T$ soustavy $A\mathbf{x} = \mathbf{b}$.

Postup z předchozího příkladu můžeme použít při opakovaném řešení soustavy lineárních rovnic s regulární maticí A v případě, že během Gaussovy eliminace používáme pouze třetí krok, tj. nemusíme prohazovat řádky. V tom případě jsou všechny elementární matice odpovídající elementárním úpravám dolní trojúhelníkové s jednotkami na hlavní diagonále a jejich součin R je také dolní trojúhelníková matice s jednotkami na hlavní diagonále podle tvrzení 4.28.6. Ta je navíc regulární

coby součin elementárních matic, tvrzení 4.66. Inverzní matice R^{-1} proto existuje a podle následujícího tvrzení je rovněž dolní trojúhelníková s jednotkami na hlavní diagonále.

Tvrzení 4.70. *Pro regulární dolní (horní) trojúhelníkovou matici R řádu n platí, že inverzní matice R^{-1} je také dolní (horní) trojúhelníková. Má-li navíc matice R na hlavní diagonále všechny prvky rovné 1, pak i matice R^{-1} má samé jednotky na hlavní diagonále.*

Důkaz. Protože je R dolní trojúhelníková, je transponovaná matice R^T horní trojúhelníková. Protože je R regulární, je R^T také regulární podle tvrzení 4.65.2. Podle věty 4.59.5 Gaussova eliminace převede matici R^T do horní trojúhelníkové matice s nenulovými prvky na hlavní diagonále. Dokud jsou na hlavní diagonále matice R^T nenulové prvky, Gaussova eliminace nemusí prvky pod nimi eliminovat, protože už jsou nulové. První nulový prvek na hlavní diagonále matice R^T, například na místě (j, j), by ale znamenal, že v j-tém sloupci matice v odstupňovaném tvaru po Gaussově eliminaci nebude žádný pivot, proměnná x_j by byla volná, což by bylo ve sporu s podmínkou 5. z věty 4.59.

Matice R^T a tedy i matice R má na hlavní diagonále nenulové prvky. Při výpočtu inverzní matice R^{-1} převodem matice $(R|I_n)$ do $(I_n|R^{-1})$ pomocí elementárních řádkových úprav můžeme napřed změnit všechny prvky na hlavní diagonále na 1 pomocí vhodných násobků jednotlivých řádků a poté vynulujeme všechny prvky pod hlavní diagonálou pomocí přičítání vhodných násobků jednotlivých řádků k řádkům po ním. Všem řádkovým úpravám odpovídají dolní trojúhelníkové matice $E_1, E_2, \ldots, E_k$, platí proto $E_k \cdots E_2 E_1 R = I_n$ a matice $R^{-1} = E_k \cdots E_2 E_1$ je dolní trojúhelníková podle tvrzení 4.28.5.

Pokud má matice R hned na počátku na hlavní diagonále prvky 1, můžeme první fázi vynechat a použít pouze přičítání vhodných násobků jednoho řádku k řádkům pod ním. V tom případě používáme pouze dolní trojúhelníkové matice $E_1, E_2, \ldots, E_k$ s jednotkami na hlavní diagonále a jejich součin $R^{-1} = E_k \cdots E_2 E_1$ je proto rovněž dolní trojúhelníková matice s jednotkami na hlavní diagonále podle tvrzení 4.28.6.

Případy, kdy je matice R horní trojúhelníková plynou pomocí transponování z právě dokázaných vlastností inverze regulárních dolních trojúhelníkových matic. □

Vrátíme se k diskusi předcházející formulaci tvrzení 4.70. Pokud při Gaussově eliminaci použité na regulární matici A nepotřebujeme přehazovat řádky, existuje dolní trojúhelníková matice R s jednotkami na hlavní diagonále taková, že součin $RA = U$ je horní trojúhelníková matice s nenulovými prvky na hlavní diagonále. Podle tvrzení 4.70 je inverzní matice R^{-1} také dolní trojúhelníková s jednotkami na hlavní diagonále a platí pro ni $A = R^{-1}U$. Dokázali jsme tak existenční část následující věty o *LU-rozkladu.*

Věta 4.71 (O *LU*-rozkladu)**.** *Nechť A je regulární matice řádu n, u které při Gaussově eliminaci nemusíme prohazovat řádky. Pak existují regulární matice L, U řádu n, pro které platí*

- *$A = LU$,*
- *L je dolní trojúhelníková s jednotkami na hlavní diagonále,*
- *U je horní trojúhelníková s nenulovými prvky na hlavní diagonále.*

Matice L, U jsou těmito podmínkami určené jednoznačně.

Důkaz. Existenci jsme již dokázali, zbývá dokázat jednoznačnost. Předpokládejme tedy, že $A = L_1U_1 = L_2U_2$ jsou rozklady splňující podmínky věty. Chceme dokázat, že $L_1 = L_2$ a $U_1 = U_2$.

Vynásobením rovnosti $L_1U_1 = L_2U_2$ zleva maticí L_2^{-1} a poté zprava maticí U_1^{-1} získáme

$$L_2^{-1}L_1 = U_2U_1^{-1} \ .$$

Matice $L_2^{-1}L_1$ je dolní trojúhelníková s jednotkami na hlavní diagonále. Je rovná horní trojúhelníkové matici $U_2U_1^{-1}$. Z toho plyne, že obě strany jsou diagonální matice s jednotkami na hlavní diagonále, tj. jednotkové matice. Proto $L_2^{-1}L_1 = I_n$ a $U_2U_1^{-1} = I_n$, z čehož po úpravě dostáváme $L_1 = L_2$ a $U_1 = U_2$. □

V příkladu 4.69 jsme si na příkladu matice řádu 3 ukázali, jak efektivně nalézt LU-rozklad matice pomocí Gaussovy eliminace. Postup lze jednoduše zobecnit na regulární matici $A = (a_{ij})$ libovolného řádu n. Pokud nemusíme prohazovat řádky před eliminací prvního sloupce, je $a_{11} \neq 0$. Pro každé $i > 1$ pak přičteme $(-a_{i1}/a_{11})$-násobek prvního řádku k i-tému. Výsledek prvního cyklu Gaussovy eliminace dosáhneme vynásobením matice A zleva maticí

$$F_1 = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ -\ell_{21} & 1 & 0 & \cdots & 0 \\ -\ell_{31} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -\ell_{n1} & 0 & 0 & \cdots & 1 \end{pmatrix} = I_n - \begin{pmatrix} 0 \\ \ell_{21} \\ \ell_{31} \\ \vdots \\ \ell_{n1} \end{pmatrix} (1, 0, 0, \ldots, 0) \ ,$$

kde $\ell_{i1} = a_{i1}/a_{11}$ pro každé $i = 1, 2, \ldots, n$.

Výsledek druhého cyklu – eliminaci druhého sloupce – získáme tak, že matici F_1A vynásobíme zleva maticí

$$F_2 = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & -\ell_{32} & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & -\ell_{n2} & 0 & \cdots & 1 \end{pmatrix} = I_n - \begin{pmatrix} 0 \\ 0 \\ \ell_{31} \\ \vdots \\ \ell_{n1} \end{pmatrix} (0, 1, 0, \ldots, 0) \ ,$$

kde pro každé $i > 2$ je $-\ell_{i2}$ koeficient, kterým násobíme druhý řádek při eliminaci prvku na místě $(i, 2)$.

Obecně označíme pro každé $j = 1, 2, \ldots, n-1$ symbolem F_j matici

$$F_j = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & -\ell_{j+1,j} & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & -\ell_{n,j} & 0 & \cdots & 1 \end{pmatrix} = I_n - \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ \ell_{j+1,j} \\ \vdots \\ \ell_{n,j} \end{pmatrix} (0, 0, \ldots, 0, 1, \ldots, 0) \ ,$$

kde opět $-\ell_{i,j}$ je koeficient, kterým jsme násobili j-tý řádek při eliminaci prvku na místě (i, j) pro libovolné $i > j$. Výsledek Gaussovy eliminace je pak horní trojúhelníková matice s nenulovými prvky na hlavní diagonále

$$U = F_{n-1} \cdots F_2F_1A \ .$$

Všechny matice F_j jsou dolní trojúhelníkové matice s jednotkami na hlavní diagonále, proto i jejich součin $F_{n-1}\cdots F_2F_1$ a inverzní matice $(F_{n-1}\cdots F_2F_1)^{-1} = F_1^{-1}F_2^{-1}\cdots F_{n-1}^{-1}$ jsou dolní trojúhelníkové matice s jednotkami na hlavní diagonále podle tvrzení 4.28.6 a tvrzení 4.70.

Zbývá spočítat matici $F_1^{-1}F_2^{-1}\cdots F_{n-1}^{-1}$. K tomu se hodí označit sloupcové vektory použité při vyjádření matic F_j:

$$\mathbf{m}_j = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ \ell_{j+1,j} \\ \vdots \\ \ell_{n,j} \end{pmatrix} .$$

Pro každé $j = 1, 2, \ldots, n-1$ tak platí $F_j = I_n - \mathbf{m}_j\mathbf{e}_j^T$. Nyní snadno ověříme, že

$$F_j^{-1} = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & \ell_{j+1,j} & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \ell_{n,j} & 0 & \cdots & 1 \end{pmatrix} = I_n + \mathbf{m}_j\mathbf{e}_j^T \ .$$

Skutečně,

$$\begin{aligned} F_j(I_n + \mathbf{m}_j\mathbf{e}_j^T) &= (I_n - \mathbf{m}_j\mathbf{e}_j^T)(I_n + \mathbf{m}_j\mathbf{e}_j^T) \\ &= I_n^2 + \mathbf{m}_j\mathbf{e}_j^T I_n - I_n\mathbf{m}_j\mathbf{e}_j^T - \mathbf{m}_j\mathbf{e}_j^T\mathbf{m}_j\mathbf{e}_j^T \\ &= I_n + \mathbf{m}_j\mathbf{e}_j^T - \mathbf{m}_j\mathbf{e}_j^T + \mathbf{m}_j(\mathbf{e}_j^T\mathbf{m}_j)\mathbf{e}_j^T \\ &= I_n \ , \end{aligned}$$

neboť

$$\mathbf{e}_j^T\mathbf{m}_j = (0, 0, \ldots, 1, 0, \ldots, 0) \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ \ell_{j+1,j} \\ \vdots \\ \ell_{n,j} \end{pmatrix} = 0 \ .$$

Zbývá spočítat součin $F_1^{-1}F_2^{-1}\cdots F_{n-1}^{-1}$. Jako ukázku spočteme součin

$$\begin{aligned} F_1^{-1}F_2^{-1} &= (I_n + \mathbf{m}_1\mathbf{e}_1^T)(I_n + \mathbf{m}_2\mathbf{e}_2^T) \\ &= I_n + \mathbf{m}_1\mathbf{e}_1^T + \mathbf{m}_2\mathbf{e}_2^T + \mathbf{m}_1\mathbf{e}_1^T\mathbf{m}_2\mathbf{e}_2^T \\ &= I_n + \mathbf{m}_1\mathbf{e}_1^T + \mathbf{m}_2\mathbf{e}_2^T \ . \end{aligned}$$

Platí proto

$$F_1^{-1}F_2^{-1} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ \ell_{21} & 1 & 0 & \cdots & 0 \\ \ell_{31} & \ell_{32} & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \ell_{n1} & \ell_{n2} & 0 & \cdots & 1 \end{pmatrix} .$$

Naprosto stejně spočítáme

$$\begin{aligned} L = F_1^{-1}F_2^{-1}\cdots F_{n-1}^{-1} &= (I_n + \mathbf{m}_1\mathbf{e}_1^T)(I_n + \mathbf{m}_2\mathbf{e}_2^T)\cdots(I_n + \mathbf{m}_{n-1}\mathbf{e}_{n-1}^T) \\ &= I_n + \mathbf{m}_1\mathbf{e}_1^T + \mathbf{m}_2\mathbf{e}_2^T + \cdots + \mathbf{m}_{n-1}\mathbf{e}_{n-1}^T + \sum_{i<j} \mathbf{m}_i\mathbf{e}_i^T\mathbf{m}_j\mathbf{e}_j^T \\ &= I_n + \mathbf{m}_1\mathbf{e}_1^T + \mathbf{m}_2\mathbf{e}_2^T + \cdots + \mathbf{m}_{n-1}\mathbf{e}_{n-1}^T \\ &= \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ \ell_{21} & 1 & 0 & \cdots & 0 & 0 \\ \ell_{31} & \ell_{32} & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \ell_{n-1,1} & \ell_{n-1,2} & \ell_{n-1,3} & \cdots & 1 & 0 \\ \ell_{n1} & \ell_{n2} & \ell_{n3} & \cdots & \ell_{n,n-1} & 1 \end{pmatrix} . \end{aligned}$$

Obě matice v LU-rozkladu $A = LU$ tak známe bez dalších výpočtů ihned po dokončení Gaussovy eliminace matice A.

Příklad 4.72. Spočítáme LU-rozklad reálné matice

$$A = \begin{pmatrix} 2 & 1 & 1 \\ 4 & -6 & 0 \\ -2 & 7 & 2 \end{pmatrix} .$$

Gaussovo eliminací matici A upravíme do odstupňovaného tvaru

$$\begin{aligned} A = \begin{pmatrix} 2 & 1 & 1 \\ 4 & -6 & 0 \\ -2 & 7 & 2 \end{pmatrix} &\sim \begin{pmatrix} 2 & 1 & 1 \\ 0 & -8 & -2 \\ -2 & 7 & 2 \end{pmatrix} \\ \sim \begin{pmatrix} 2 & 1 & 1 \\ 0 & -8 & -2 \\ 0 & 8 & 3 \end{pmatrix} &\sim \begin{pmatrix} 2 & 1 & 1 \\ 0 & -8 & -2 \\ 0 & 0 & 1 \end{pmatrix} = U . \end{aligned}$$

Platí proto

$$\begin{pmatrix} 2 & 1 & 1 \\ 4 & -6 & 0 \\ -2 & 7 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 & 1 \\ 0 & -8 & -2 \\ 0 & 0 & 1 \end{pmatrix} .$$

4.8.1. *Využití LU-rozkladu.* LU-rozklad regulární matice $A = LU$ řádu n lze využít zejména při opakovaném řešení soustavy $A\mathbf{x} = \mathbf{b}$ s různými pravými stranami $\mathbf{b}$. Během prvního výpočtu si zaznamenáme výsledek Gaussovy eliminace v podobě rozkladu $A = LU$. Gaussova eliminace vyžaduje zhruba $2n^3/3$ aritmetických operací. Se znalostí LU-rozkladu matice A pak stačí nejprve přímou substitucí najít (jednoznačné) řešení $\mathbf{y}$ soustavy $L\mathbf{y} = \mathbf{b}$ a posléze zpětnou substitucí vyřešit soustavu $U\mathbf{x} = \mathbf{y}$. Nalezený vektor $\mathbf{x}$ splňuje $A\mathbf{x} = LU\mathbf{x} = L\mathbf{y} = \mathbf{b}$, takže řeší původní soustavu. Přímá a zpětná substituce vyžadují každá n^2 operací. Pro velká n první

řešení soustavy s maticí A tak vyžaduje přibližně stejně operací jako Gaussova eliminace následovaná zpětnou substitucí. Poté, co známe LU-rozklad matice A, je řešení každé další soustavy s maticí A řádově rychlejší. Matematické softwary proto při řešení soustav lineárních rovnic při prvním výpočtu spočtou LU-rozklad matice soustavy a poté už používají pouze přímou a zpětnou substituci.

4.8.2. *Když je nutné prohazovat řádky.* Ne každou regulární matici je možné převést do odstupňovaného tvaru Gaussovo eliminací bez prohazování řádků. Nejjednodušším příkladem je matice

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

I v případě, že lze provést Gaussovu eliminaci regulární matice bez prohazování řádků, může být vhodnější někdy pořadí řádků prohodit. Standardní metoda *částečné pivotace* zmíněná v části 2.6.1 požaduje, aby byl při řešení soustavy lineárních rovnic s reálnými koeficienty vždy z možných pivotů vybrán ten, který je v absolutní hodnotě největší. Takto použitá Gaussova eliminace má lepší numerickou stabilitu než jiné volby pivotů.

Pokud při Gaussově eliminaci používáme prohazování řádků, pak platí následující věta.

Věta 4.73 (O LU-rozkladu s částečnou pivotací)**.** *Je-li A regulární matice řádu n, pak existuje permutační matice P a regulární matice matice L, U, všechny řádu n, pro které platí*

- $PA = LU$,
- *L je dolní trojúhelníková matice s jednotkami na hlavní diagonále,*
- *U je horní trojúhelníková matice s nenulovými prvky na hlavní diagonále.*

Věta říká, že u matice A můžeme na začátku přeházet řádky pomocí nějaké permutační matice tak, aby matice PA měla LU-rozklad. Matice P není v tomto případě určená jednoznačně. Pokud ale nějakou takovou matici P zvolíme, pak LU-rozklad matice $PA = LU$ už jednoznačně učený je. Větu o LU-rozkladu s částečnou pivotací dokazovat nebudeme, na příkladu si ale ukážeme, jak matici P a příslušný LU-rozklad najít na základě jednoho průběhu Gaussovy eliminace.

Příklad 4.74. Předchozí věta platí pro libovolnou regulární matici A. Máme-li řešit soustavu rovnic $A\mathbf{x} = \mathbf{b}$ a známe=li rozklad $PA = LU$, stačí místo původní soustavy řešit ekvivalentní soustavu $PA\mathbf{x} = P\mathbf{b}$, kterou dostaneme vynásobením původní soustavy permutační maticí P zleva. Výpočet nového vektoru pravých stran $P\mathbf{b}$ nevyžaduje žádné další aritmetické operace, jde pouze o permutaci složek vektoru $\mathbf{b}$. Soustavu $PA\mathbf{x} = P\mathbf{b}$, tj. $LU\mathbf{x} = P\mathbf{b}$ pak už vyřešíme snadno pomocí přímé substituce následované zpětnou substitucí.

Příklad 4.75. Použijeme Gaussovu eliminaci s částečnou pivotaci na matici

$$A = \begin{pmatrix} 1 & 2 & -3 & 4 \\ 4 & 8 & 12 & -8 \\ 2 & 3 & 2 & 1 \\ -3 & -1 & 1 & -4 \end{pmatrix} .$$

K nalezení permutační matice P si k matici A přidáme sloupec $(1,2,3,4)^T$, do kterého budeme zaznamenávat prohazování řádků:

$$\left(\begin{array}{cccc||c} 1 & 2 & -3 & 4 & 1 \\ 4 & 8 & 12 & -8 & 2 \\ 2 & 3 & 2 & 1 & 3 \\ -3 & -1 & 1 & -4 & 4 \end{array}\right) .$$

Přidáváme dvě svislé čáry, abychom zdůraznili, že poslední sloupec není sloupec pravých stran nějaké soustavy lineárních rovnic, ale „počítadlo permutace“ řádků matice. Poslední sloupec měníme pouze v případě elementární úpravy matice A, která prohazuje řádky. V případě přičítání nějakého násobku jednoho řádku k řádku pod ním (v eliminační fázi cyklu Gaussovy eliminace) poslední sloupec matice neměníme.

$$\left(\begin{array}{cccc||c} 1 & 2 & -3 & 4 & 1 \\ 4 & 8 & 12 & -8 & 2 \\ 2 & 3 & 2 & 1 & 3 \\ -3 & -1 & 1 & -4 & 4 \end{array}\right) \sim \left(\begin{array}{cccc||c} 4 & 8 & 12 & -8 & 2 \\ 1 & 2 & -3 & 4 & 1 \\ 2 & 3 & 2 & 1 & 3 \\ -3 & -1 & 1 & -4 & 4 \end{array}\right)$$

$$\sim \left(\begin{array}{cccc||c} 4 & 8 & 12 & -8 & 2 \\ 0 & 0 & -6 & 6 & 1 \\ 0 & -1 & -4 & 5 & 3 \\ 0 & 5 & 10 & -10 & 4 \end{array}\right) \sim \left(\begin{array}{cccc||c} 4 & 8 & 12 & -8 & 2 \\ 0 & 5 & 10 & -10 & 4 \\ 0 & -1 & -4 & 5 & 3 \\ 0 & 0 & -6 & 6 & 1 \end{array}\right)$$

$$\sim \left(\begin{array}{cccc||c} 4 & 8 & 12 & -8 & 2 \\ 0 & 5 & 10 & -10 & 4 \\ 0 & 0 & -2 & 3 & 3 \\ 0 & 0 & -6 & 6 & 1 \end{array}\right) \sim \left(\begin{array}{cccc||c} 4 & 8 & 12 & -8 & 2 \\ 0 & 5 & 10 & -10 & 4 \\ 0 & 0 & -6 & 6 & 1 \\ 0 & 0 & -2 & 3 & 3 \end{array}\right)$$

$$\sim \left(\begin{array}{cccc||c} 4 & 8 & 12 & -8 & 2 \\ 0 & 5 & 10 & -10 & 4 \\ 0 & 0 & -6 & 6 & 1 \\ 0 & 0 & 0 & 1 & 3 \end{array}\right) .$$

Dostali jsme tak horní trojúhelníkovou matici s nenulovými prvky na hlavní diagonále

$$U = \left(\begin{array}{cccc} 4 & 8 & 12 & -8 \\ 0 & 5 & 10 & -10 \\ 0 & 0 & -6 & 6 \\ 0 & 0 & 0 & 1 \end{array}\right) ,$$

jak má v případě Gaussovy eliminace regulární matice vyjít podle věty 4.59.5. „Počítadlo permutace“ nám říká, že po celém výpočtu je na prvním řádku původně druhý řádek, na druhém řádku původně čtvrtý řádek, na třetím řádku je řádek, který byl v původní matici A jako první a na posledním čtvrtém řádku je původně třetí řádek. Stejného proházení řádků lze dosáhnout tím, že matici A na začátku vynásobíme zleva permutační maticí

$$P = \left(\begin{array}{cccc} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{array}\right) .$$

Věta o LU-rozkladu s částečnou pivotací říká, že matice PA už má LU-rozklad. Ten můžeme najít Gaussovo eliminací matice PA, ve skutečnosti jej ale už můžeme

přečíst z průběhu Gaussovy eliminace původní matice A. Jak to lze udělat nám objasní výpočet LU-rozkladu matice PA.

Převedeme matici PA do odstupňovaného tvaru pomocí Gaussovy eliminace bez prohazování řádků. Napřed spočteme matici PA:

$$PA = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 & -3 & 4 \\ 4 & 8 & 12 & -8 \\ 2 & 3 & 2 & 1 \\ -3 & -1 & 1 & -4 \end{pmatrix} = \begin{pmatrix} 4 & 8 & 12 & -8 \\ -3 & -1 & 1 & -4 \\ 1 & 2 & -3 & 4 \\ 2 & 3 & 2 & 1 \end{pmatrix} .$$

Nyní použijeme Gaussovu eliminaci bez prohazování řádků na matici PA:

$$\begin{pmatrix} 4 & 8 & 12 & -8 \\ -3 & -1 & 1 & -4 \\ 1 & 2 & -3 & 4 \\ 2 & 3 & 2 & 1 \end{pmatrix} \sim \begin{pmatrix} 4 & 8 & 12 & -8 \\ 0 & 5 & 10 & -10 \\ 0 & 0 & -6 & 6 \\ 0 & -1 & -4 & 5 \end{pmatrix}$$
$$\sim \begin{pmatrix} 4 & 8 & 12 & -8 \\ 0 & 5 & 10 & -10 \\ 0 & 0 & -6 & 6 \\ 0 & 0 & -2 & 3 \end{pmatrix} \sim \begin{pmatrix} 4 & 8 & 12 & -8 \\ 0 & 5 & 10 & -10 \\ 0 & 0 & -6 & 6 \\ 0 & 0 & 0 & 1 \end{pmatrix} .$$

Dostali jsme tak tutéž matici U jako při Gaussově eliminaci matice A s částečnou pivotací. A dále matici

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

Platí proto

$$PA = \begin{pmatrix} 4 & 8 & 12 & -8 \\ -3 & -1 & 1 & -4 \\ 1 & 2 & -3 & 4 \\ 2 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -3/4 & 1 & 0 & 0 \\ 1/4 & 0 & 1 & 0 \\ 1/2 & -1/5 & 1/3 & 1 \end{pmatrix} \begin{pmatrix} 4 & 8 & 12 & -8 \\ 0 & 5 & 10 & -10 \\ 0 & 0 & -6 & 6 \\ 0 & 0 & 0 & 1 \end{pmatrix} .$$

Pokud jde o matici L, všimněme si, že jsou v ní v jednotlivých sloupcích opět obsažené koeficienty, které jsme použili už při první Gaussově eliminaci původní matice A k vynulování prvků pod příslušným pivotem. Jsou pouze v jiném pořadí. Jejich správné pořadí v matici L zjistíme následujícím postupem. Během Gaussovy eliminace si na místo každého vynulovaného prvku zapíšeme místo výsledné 0 koeficient, který jsme k jeho vynulování použili.

Ukážeme si to na příkladu stejné matice. Abychom zdůraznili, že prvek na příslušném místě není výsledkem elementární řádkové úpravy, ale záznamem průběhu Gaussovy eliminace, budeme koeficienty psát do matice tučným písmem, zatímco ostatní prvky včetně prvků pod hlavní diagonálou, které na eliminaci ještě čekají, budeme psát nadále stejným typem písma jako dosud.

Zopakujeme původní Gaussovu eliminaci s touto modifikací:

$$\left(\begin{array}{cccc||c} 1 & 2 & -3 & 4 & 1 \\ 4 & 8 & 12 & -8 & 2 \\ 2 & 3 & 2 & 1 & 3 \\ -3 & -1 & 1 & -4 & 4 \end{array}\right) \sim \left(\begin{array}{cccc||c} 4 & 8 & 12 & -8 & 2 \\ 1 & 2 & -3 & 4 & 1 \\ 2 & 3 & 2 & 1 & 3 \\ -3 & -1 & 1 & -4 & 4 \end{array}\right)$$

$$\sim \left(\begin{array}{cccc||c} 4 & 8 & 12 & -8 & 2 \\ \mathbf{1/4} & 0 & -6 & 6 & 1 \\ \mathbf{1/2} & -1 & -4 & 5 & 3 \\ \mathbf{-3/4} & 5 & 10 & -10 & 4 \end{array}\right) \sim \left(\begin{array}{cccc||c} 4 & 8 & 12 & -8 & 2 \\ \mathbf{-3/4} & 5 & 10 & -10 & 4 \\ \mathbf{1/2} & -1 & -4 & 5 & 3 \\ \mathbf{1/4} & 0 & -6 & 6 & 1 \end{array}\right)$$

$$\sim \left(\begin{array}{cccc||c} 4 & 8 & 12 & -8 & 2 \\ \mathbf{-3/4} & 5 & 10 & -10 & 4 \\ \mathbf{1/2} & \mathbf{-1/5} & -2 & 3 & 3 \\ \mathbf{1/4} & \mathbf{0} & -6 & 6 & 1 \end{array}\right) \sim \left(\begin{array}{cccc||c} 4 & 8 & 12 & -8 & 2 \\ \mathbf{-3/4} & 5 & 10 & -10 & 4 \\ \mathbf{1/4} & \mathbf{0} & -6 & 6 & 1 \\ \mathbf{1/2} & \mathbf{-1/5} & -2 & 3 & 3 \end{array}\right)$$

$$\sim \left(\begin{array}{cccc||c} 4 & 8 & 12 & -8 & 2 \\ \mathbf{-3/4} & 5 & 10 & -10 & 4 \\ \mathbf{1/4} & \mathbf{0} & -6 & 6 & 1 \\ \mathbf{1/2} & \mathbf{-1/5} & \mathbf{1/3} & 1 & 3 \end{array}\right) .$$

Tímto postupem jsme během Gaussovy eliminace zjistili nejen permutační matici P a matici U (stačí nahradit tučné koeficienty nulami), ale také matici L. Tučně napsané koeficienty stačí doplnit jednotkami na hlavní diagonále a nulami nad hlavní diagonálou a dostaneme matici L.

Správnost uvedeného postupu, jak získat rozklad $PA = LU$ libovolné matice A během Gaussovy eliminace matice A, lze také dokázat obecně. Na tomto místě to ale dělat nebudeme, uvádíme jej pouze pro zajímavost.

4.9. **Jednostranné inverzy.**

4.9.1. *Matice inverzní zprava a zleva.* Pro zobrazení $f : X \to X$ na nekonečné množině X obecně neplatí, že f je vzájemně jednoznačné, pokud je f prosté. Také neplatí, že f je vzájemně jednoznačné, pokud je f na. To je rozdíl oproti situaci, kdy je množina X je konečná. Ve větě 4.59 jsme ukázali že zobrazení tvaru $f_A : \mathbf{T}^n \to \mathbf{T}^n$ (pro čtvercovou matici A) jsou „spořádaná“ v tom smyslu, že kdykoliv je f_A prosté nebo na, pak je f_A vzájemně jednoznačné. Dokázali jsme tam také, že pro čtvercovou matici A je zobrazení f_A prosté právě tehdy, když je na, a to nastane právě tehdy, když A má inverzní matici (zleva nebo zprava). Následující dvě tvrzení podávají podobné charakterizace pro obecné, ne nutně čtvercové, matice.

Tvrzení 4.76 (o matici inverzní zprava)**.** *Pro matici A typu $m \times n$ nad $\mathbf{T}$ je ekvivalentní:*

(i) *Existuje matice X typu $n \times m$ nad $\mathbf{T}$ taková, že $AX = I_m$.*
(ii) *Zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^m$ je na $\mathbf{T}^m$.*

Důkaz. Pokud $AX = I_m$, pak pro příslušná zobrazení f_A a f_X platí $f_{AX} = f_{I_m}$, tedy $f_A \circ f_X = \mathrm{id}_{T^m}$. Abychom ukázali, že f_A je zobrazení na celou množinu $\mathbf{T}^m$, zvolíme nějaký vektor $\mathbf{a} \in \mathbf{T}^m$. Pro tento vektor platí

$$f_A f_X(\mathbf{a}) = \mathrm{id}_{T^m}(\mathbf{a}) = \mathbf{a} \ ,$$

což znamená, že $f_A(X\mathbf{a}) = \mathbf{a}$ a tedy f_A je na celou množinu $\mathbf{T}^n$.

Naopak, předpokládejme, že f_A je na. Pro j-tý sloupec $\mathbf{e}_j$ jednotkové matice I_m najdeme nějaké řešení soustavy rovnic $A\mathbf{x}_j = \mathbf{e}_j$ (řešení existuje, protože f_A je na). Vektory $\mathbf{x}_j$ srovnáme do sloupců matice $X = (\mathbf{x}_1|\mathbf{x}_2|\dots|\mathbf{x}_m)$. Pak platí $AX = (A\mathbf{x}_1|\dots|A\mathbf{x}_m) = I_m$. □

Tvrzení 4.77 (o matici inverzní zleva)**.** *Pro matici A typu $m \times n$ nad $\mathbf{T}$ je ekvivalentní:*

(i) *Existuje matice X typu $n \times m$ nad $\mathbf{T}$ taková, že $XA = I_n$.*
(ii) *Zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^m$ je prosté.*

Důkaz. První část se dokáže obdobně jako u předchozího tvrzení. Z rovnosti $XA = I_n$ plyne $f_X \circ f_A = f_{XA} = f_{I_n} = \mathrm{id}_{T^n}$. Pokud pro vektory $\mathbf{a}, \mathbf{b} \in \mathbf{T}^n$ platí $f_A(\mathbf{a}) = f_A(\mathbf{b})$, platí rovněž $f_X \circ f_A(\mathbf{a}) = f_X \circ f_A(\mathbf{b})$ a tedy také

$$\mathbf{a} = \mathrm{id}_{T^n}(\mathbf{a}) = f_X \circ f_A(\mathbf{a}) = f_X \circ f_A(\mathbf{b}) = \mathrm{id}_{T^n}(\mathbf{b}) = \mathbf{b} \ ,$$

což dokazuje, že zobrazení f_A je prosté.

Je-li naopak zobrazení f_A prosté, má soustava $A\mathbf{x} = \mathbf{o}$ jediné řešení $\mathbf{x} = \mathbf{o}$. Všechny proměnné jsou bázové. Gaussova eliminace převede A do odstupňovaného tvaru C, kde prvních n řádků v C je nenulových a ostatní jsou nulové. Stejně jako v algoritmu pro hledání inverzní matice změníme pomocí elementárních úprav všechny pivoty na 1 a vynulujeme prvky nad nimi. Dostáváme

$$E_k \cdots E_1 A = \begin{pmatrix} I_n \\ 0_{(m-n)\times n} \end{pmatrix}$$

pro vhodné elementární matice $E_1, \dots, E_k$. Matici X definujeme jako prvních n řádků matice $E_k \cdots E_1$. □

4.10. **Různá použití matic.**

4.10.1. *Matice jako úložiště dat.* Mnohá data jsou přirozeně uspořádaná do matice.

Příklad 4.78. Ceny akcií v jednotlivých dnech můžeme uložit do matice $A = (a_{ij})$, kde a_{ij} je závěrečná cena i-té akcie v j-tém dni. Hospodářské přílohy novin nebo zpravodajských webů zveřejňují každý den nový sloupec matice.

Příklad 4.79. Fakulta organizuje přijímací řízení tak, že skupina tří porotců hodnotí každého uchazeče ve 12 kritériích. Hodnocení můžeme uložit do tří matic A, B, C, jedné pro každého porotce. V matici $A = (a_{ij})$ je prvek a_{ij} hodnocení i-tého studenta v j-tém kritériu porotcem A.

Příklad 4.80. Nějaká velká korporace vyrábí řadu produktů. K jejich výrobě potřebuje mnoho vstupů (materiál, součástky, pracovní síly, energie, voda, atd.). Materiálové náklady výroby lze zaznamenat do matice $A = (a_{ij})$, kde a_{ij} je počet jednotek vstupu j potřebných k výrobě produktu i. V i-tém řádku matice A jsou tak počty jednotek jednotlivých vstupů potřebných k výrobě i-tého produktu.

Označíme $\mathbf{x}$ vektor cen jednotlivých vstupů, jeho j-tá složka udává cenu jednotky j-tého vstupu. Spočítáme-li součin $A\mathbf{x}$, bude se jeho i-tá složka rovnat

$$a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n \ .$$

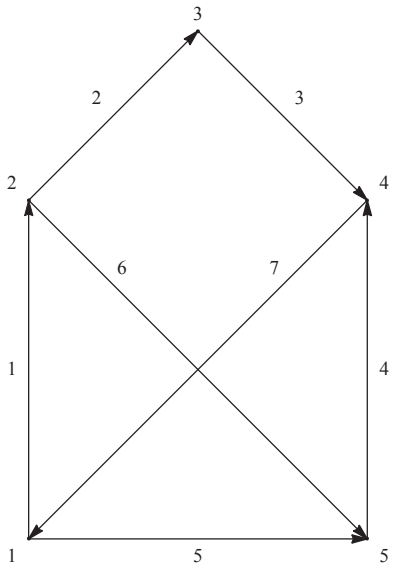
Jinak řečeno, i-tá složka vektoru $A\mathbf{x}$ se rovná výrobní ceně i-tého produktu.

- Může být v matici A nějaký prvek záporný?
- Který produkt má výrobní cenu nejcitlivější na cenu j-tého vstupu, např. elektrické energie ?

Příklad 4.81. Digitální fotoaparát zaznamenává pro každý pixel jeho barvu. Barvu se skládá ze tří základních složek - R,G,B. Intenzitu každé ze tří barev v daném pixelu zaznamenává v jednom bytu, neboli posloupností osmi nul a jedniček. Celkem je tedy možných $2^8 = 256$ odstínů každé ze tří barev. Ty jsou ukládány pro každou z barev do samostatné matice jako celá čísla mezi -127 a $+128$. Jedna fotka vyrobená fotoaparátem, který má 8 Mpixelů by tak vyžadovala paměť velikosti 24 MB. Na disk velikosti 1 GB bychom tak mohli uložit pouze 40 fotek. Fotky je proto nutné komprimovat, nejznámější komprimační formát je *jpeg*.

Příklad 4.82. Jiný typ dat, která lze uložit do matice, jsou grafy. Budeme uvažovat *orientované grafy*, ty mají nějakou množinu V *vrcholů* a nějakou množinu $E \subseteq V \times V$ *hran*. Je-li $e = (u, v)$ hrana grafu, pak u je *počáteční vrchol* hrany e a v je její *koncový vrchol*. Graf zapíšeme pomocí *matice incidence grafu* A. Je to čtvercová matice řádu $|V|$, prvky a sloupce budeme indexovat prvky množiny V. Prvek na místě (u, v) je

$$a_{uv} = \begin{cases} 1 & \text{pokud } (u,v) \in E, \\ 0 & \text{pokud } (u,v) \notin E. \end{cases}$$



Obrázek 56. Příklad grafu

Graf na obrázku popíšeme maticí řádu 5:

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

V úloze na zjišťování počtu leteckých spojení s daným počtem přestupů jsme použili právě matici incidence grafu spojů.

V posledních létech je intenzivně zkoumán *graf webu*. Jeho vrcholy odpovídají jednotlivým webovým stránkám a mezi vrcholy i a j vede orientovaná hrana (i, j) pokud stránka i odkazuje na stránku j. Matice incidence A grafu webu se nazývá *matice incidence webu*. Vyhledávač *Google* seřazuje webové stránky na základě jejich důležitosti pomocí umocňování matice A^T transponované k matici webu. Odhaduje se, že v současnosti existuje více než $4 \cdot 10^{10}$ webových stránek, což znamená, že matice webu má $16 \cdot 10^{20} \approx 2^4 \cdot 2^{70}$ prvků. Takovou matici samozřejmě nejde uložit do žádného počítače. Je ale hodně *řídká*, v průměru jedna stránka odkazuje na méně než 8 jiných stránek. Každý řádek obsahuje v průměru pouze osm prvků 1, jinak samé nuly. Lze ji proto výrazně komprimovat a s komprimovanými daty o propojení webu už počítat lze.

Příklad 4.83. Jiný typ matice grafu (V, E) je obdélníková matice, jejíž řádky odpovídají hranám grafu a sloupce jeho vrcholům. Prvky matice se rovnají 0, 1 nebo -1. V řádku určeném hranou (u, v) je

- prvek ve sloupci, který odpovídá počátečnímu vrcholu u, rovný -1,
- prvek ve sloupci, který odpovídá koncovému vrcholu v, rovný 1,
- všechny ostatní prvky se rovnají 0.

Graf na obrázku tak můžeme zapsat také následující maticí typu 7×5.

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

Příklad 4.84. Matice také můžeme použít při řešení nejrůznějších problémů v přírodovědných a technických oborech. Ukážeme si příklad úlohy stavebního inženýrství.

Na obrázku vlevo vidíme čtyři pružiny zavěšené pod sebou. Horní a dolní konec jsou pevné. Na obrázku vpravo vidíme situaci poté, co jsme do spojů mezi pružinami zavěsili závaží s hmotnostmi m_1, m_2 a m_3. Chceme vědět, o kolik se jednotlivé spoje posunou. Vektor neznámých posunutí si označíme $\mathbf{x} = (x_1, x_2, x_3)^T$. Horní a dolní konec jsou pevné, vlivem závaží se neposunou. Proto je velikost jejich posunutí $x_0 = x_4 = 0$.

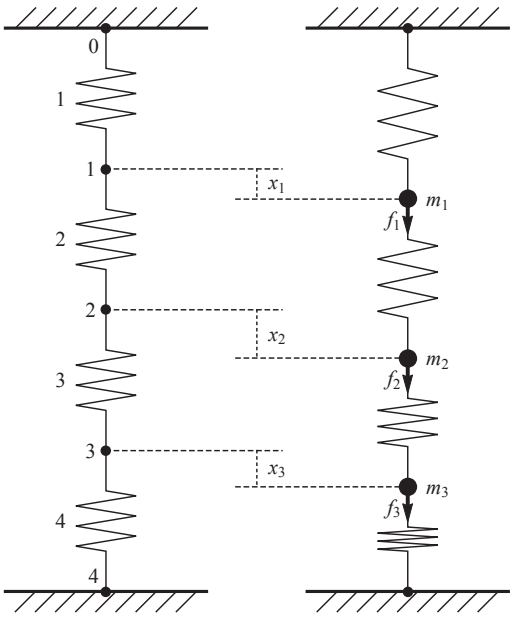
Posunutí koncových bodů pružin pod vlivem závaží způsobí natažení nebo zkrácení pružin. Ta si označíme d_1, d_2, d_3, d_4. Pro každé $i = 1, 2, 3, 4$ platí

$$d_i = x_i - x_{i-1} \ .$$

Hodnota d_i je kladná, pokud se i-tá pružina natáhne, a je záporná, pokud se zkrátí. Vztah mezi vektorem $\mathbf{d} = (d_1, d_2, d_3, d_4)^T$ a vektorem neznámých posunutí $\mathbf{x} = (x_1, x_2, x_3)^T$ je lineární a lze jej popsat rovností

$$\begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \ .$$

Označíme-li matici v poslední rovnosti A, dostáváme vztah $\mathbf{d} = A\mathbf{x}$.



Obrázek 57. Zavěšené pružiny

Prodloužení/zkrácení pružin v nich vyvolá vnitřní síly, jejichž velikost vyjadřuje *Hookeův zákon*. Označíme-li vnitřní síly v pružinách y_i, pak platí $y_i = k_i d_i$, kde $k_i > 0$ je konstanta udávající „pružnost“ i-té pružiny. Také vztah mezi vektorem vnitřních sil $\mathbf{y} = (y_1, y_2, y_3, y_4)^T$ a vektorem $\mathbf{d}$ lze popsat maticí:

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} k_1 & 0 & 0 & 0 \\ 0 & k_2 & 0 & 0 \\ 0 & 0 & k_3 & 0 \\ 0 & 0 & 0 & k_4 \end{pmatrix} \begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \end{pmatrix} ,$$

neboli $\mathbf{y} = C\mathbf{d}$, kde C označuje diagonální matici z poslední rovnosti. Je dobré si uvědomit, že pokud $d_i > 0$, tj. je-li i-tá pružina natažená, táhne vnitřní síla y_i dolní konec této pružiny vzhůru a horní konec dolů. V případě $d_i < 0$ je tomu přesně naopak. První pružina je vždy natažená, proto $y_1 > 0$, takže kladný směr vnitřních sil v pružinách je směrem vzhůru.

Na spoj i působí vnitřní síly pružin y_i a y_{i+1}, které se složí do síly $y_i - y_{i+1}$ působící na i-tý spoj. Vektor sil působících na jednotlivé spoje v důsledku vnitřních sil v pružinách spočteme opět pomocí matice, tentokrá platí

$$\begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} ,$$

matice v poslední rovnosti se rovná matici A^T transponované k A. Velikost vnitřních sil působících na jednotlivé spoje tak dostaneme jako součin

$$A^T C A \mathbf{x} \ .$$

V ustáleném rovnovážném stavu jsou vnitřní síly pružin v rovnováze s vnějšími gravitačními silami působícími na jednotlivé spoje. Vnější síla působící v i-tém spoji se rovná $f_i = m_i g$, kde g je gravitační konstanta. Vektor vnějších je tedy $\mathbf{f} = (f_1, f_2, f_3)^T$ a v rovnovážném stavu platí rovnost

$$A^T C A \mathbf{x} = \mathbf{f},$$

ze které můžeme hodnoty posunutí x_i vypočítat, známe-li hmotnosti závaží a koeficienty pružnosti jednotlivých pružin.

Matice soustavy ve tvaru $A^T C A$, kde C je diagonální matice s kladnými prvky na hlavní diagonále, se vyskytuje při řešení mnoha praktických problémů a v lineární algebře je těmto maticím věnována speciální pozornost. Setkáme se s nimi ještě několikrát.

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. Vypočítejte n-tou mocninu matice

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

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

10. 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.

11. Dokončete důkaz tvrzení 4.7.

12. Dokažte druhou distributivitu z tvrzení 4.18.

13. Dokažte tvrzení 4.20.

14. 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!)

15. Dokažte vzorec pro blokové násobení matic.

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

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

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

19. Spočítejte znovu příklad 4.62 alternativními postupy navržené v tomto příkladu.

20. Ke každé elementární matici najděte příslušnou matici inverzní, viz tvrzení 4.64.

21. 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).

22. Dokažte implikaci (2) $\Rightarrow$ (5) z věty 4.59.

23. Dokažte přímo implikaci (9) $\Rightarrow$ (3) z věty 4.59.

24. Dokažte tvrzení 4.65 a vysvětlete geometrický význam.

25. Dokažte, že n-tá mocnina diagonální matice je diagonální a na diagonále jsou n-té mocniny původních prvků.

Shrnutí čtvrté kapitoly

(1) *Matice typu $m \times n$ nad tělesem* $\mathbf{T}$ je obdélníkové schéma prvků tělesa $\mathbf{T}$ s m řádky a n sloupci. Matice typu $m \times m$ se nazývá *čtvercová matice řádu* m.

(2) *sloupcový aritmetický vektor* s m složkami nad $\mathbf{T}$ je matice typu $m \times 1$, *řádkový aritmetický vektor* s m složkami nad $\mathbf{T}$ je matice typu $1 \times m$.

(3) Dvě matice $A = (a_{ij})$ a $B = (b_{ij})$ se rovnají, pokud mají stejný typ $m \times n$, jsou nad stejným tělesem $\mathbf{T}$, a také mají stejné prvky na odpovídajících pozicích. Formálněji, pro každé $i \in \{1, 2, \ldots, m\}$ a každé $j \in \{1, 2, \ldots, n\}$ platí $a_{ij} = b_{ij}$. Rovnost mezi dvěma maticemi tak znamená mn rovností mezi jejich prvky na stejných místech.

(4) Pro matice $A = (a_{ij})$ a $B = (b_{ij})$ stejného typu $m \times n$ nad stejným tělesem definujeme
- *součet matic A a B* jako matici $A + B = (a_{ij} + b_{ij})_{m\times n}$,
- *matici opačnou k A* jako matici $-A = (-a_{ij})_{m\times n}$,
- dále definujeme *nulovou matici* typu $m\times n$ jako matici $0_{m\times n} = (0)_{m\times n}$.

(5) Jsou-li A, B, C matice stejného typu $m \times n$ nad stejným tělesem $\mathbf{T}$, pak platí
(a) $(A + B) + C = A + (B + C)$,
(b) $A + 0_{m\times n} = A$,
(c) $A + (-A) = 0_{m\times n}$,
(d) $A + B = B + A$.

(6) Pro matici $A = (a_{ij})$ typu $m \times n$ nad tělesem $\mathbf{T}$ a $t \in \mathbf{T}$ definujeme
- *t-násobek matice A* jako matici $t \cdot A = tA = (ta_{ij})_{m\times n}$.

(7) Pro matice $A = (a_{ij})$ a $B = (b_{ij})$ téhož typu $m \times n$ nad stejným tělesem $\mathbf{T}$ a pro libovolné dva prvky $s, t \in \mathbf{T}$ platí
(a) $s(tA) = (st)A$,
(b) $1A = A$,
(c) $-A = (-1)A$,
(d) $(s + t)A = sA + tA$,
(e) $s(A + B) = sA + sB$.

(8) *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 $i \in \{1, 2, \ldots, m\}$ a $j \in \{1, 2, \ldots, n\}$.

(9) Pro matice $A = (a_{ij})$ a $B = (b_{ij})$ téhož typu $m \times n$ nad stejným tělesem $\mathbf{T}$ a pro libovolný prvek $s \in \mathbf{T}$ platí
(a) $\left(A^T\right)^T = A$,
(b) $(A + B)^T = A^T + B^T$,
(c) $(sA)^T = s\, A^T$.

(10) Matici $A = (a_{ij})_{m\times n}$ nad tělesem $\mathbf{T}$ můžeme také zapsat po sloupcích. *Sloupcový zápis* matice A je

$$A = (\mathbf{a}_1|\mathbf{a}_2|\ldots|\mathbf{a}_n) \ ,$$

kde pro každé $j = 1, 2, \ldots, n$ vektor $\mathbf{a}_j = (a_{1j}, a_{2j}, \ldots, a_{mj})^T$ je m-složkový sloupcový aritmetický vektor nad $\mathbf{T}$.

(11) Sloupcový zápis matice A^T je

$$A^T = (\tilde{\mathbf{a}}_1|\tilde{\mathbf{a}}_2|\cdots|\tilde{\mathbf{a}}_m) \ ,$$

kde pro každé $i = 1, 2, \ldots, m$ vektor $\tilde{\mathbf{a}}_i = (a_{i1}, a_{i2}, \ldots, a_{in})^T$ je i-tý sloupcový vektor transponované matice A^T.

Řádkový zápis matice A je

$$A = \begin{pmatrix} \tilde{\mathbf{a}}_1^T \\ \tilde{\mathbf{a}}_2^T \\ \vdots \\ \tilde{\mathbf{a}}_m^T \end{pmatrix} ,$$

kde $\tilde{\mathbf{a}}_i^T = (a_{i1}, a_{i2}, \dots, a_{in})$ je i-tý řádkový vektor matice A.

(12) Je-li $A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ matice typu $m \times n$ nad tělesem $\mathbf{T}$ a $\mathbf{b} = (b_1, b_2, \dots, b_n)^T$ (sloupcový) aritmetický vektor s n-složkami z tělesa $\mathbf{T}$, pak definujeme *součin matice A s vektorem* $\mathbf{b}$ jako

$$A\mathbf{b} = b_1\mathbf{a}_1 + b_2\mathbf{a}_2 + \cdots + b_n\mathbf{a}_n \ .$$

(13) Soustavu m lineárních rovnic o n neznámých $x_1, x_2, \dots, x_n$ s maticí soustavy $A = (a_{ij})_{m\times n}$ a vektorem pravých stran $\mathbf{b} \in \mathbf{T}^m$ můžeme zapsat jako součin

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

kde $\mathbf{x} = (x_1, x_2, \dots, x_n)^T$ je *vektor neznámých*.

(14) Je-li A matice typu $m \times n$ a $B = (\mathbf{b}_1|\mathbf{b}_2|\cdots|\mathbf{b}_p)$ matice typu $n \times p$, obě nad stejným tělesem $\mathbf{T}$, pak *součinem matic* A a B rozumíme matici

$$AB = (A\mathbf{b_1}|A\mathbf{b}_2|\cdots|A\mathbf{b}_p) \ ,$$

tj. j-tý sloupec součinu matic AB se rovná součinu matice A s j-tým sloupcem matice B. Součin AB má tedy typ $m \times p$.

(15) Součin matic $A = (a_{ij})_{m\times n}$ a $B = (b_{jk})_{n\times p}$ můžeme také spočítat po prvcích, neboť prvek na místě (i, k) v součinu AB se rovná

$$a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj} = \sum_{j=1}^{n} a_{ij}b_{jk} = \tilde{\mathbf{a}}_i^T\mathbf{b}_k \ .$$

Také se říká „výpočet součinu matic podle pravidla *řádek* × *sloupec*“.

(16) Jsou-li $A = (a_{ij})$ a $B = (b_{ij})$ matice téhož typu $m \times n$, $C = (c_{jk})$ matice typu $n \times p$, a $D = (d_{kl})$, $E = (e_{kl})$ matice téhož typu $p \times q$, všechny nad stejným tělesem $\mathbf{T}$, a $s \in \mathbf{T}$, pak platí
   (a) $B(CD) = (BC)D$,
   (b) $(A + B)C = AC + BC$,
   (c) $C(D + E) = CD + CE$,
   (d) $(BC)^T = C^T B^T$,
   (e) $s(BC) = (sB)C = B(SC)$.

(17) **Násobení matic není komutativní**.

(18) Součin matice $A = (a_{ij})_{m\times n}$ s maticí $B = (b_{jk})_{n\times p}$ můžeme také spočítat *po řádcích*, neboť pro každé $i = 1, 2, \dots, m$ se i-tý řádek v součinu AB rovná součinu i-tého řádku $\tilde{\mathbf{a}}_i^T$ matice A s maticí B, tj. $\tilde{\mathbf{a}}_i^T B$.

(19) *Jednotková matice řádu n nad tělesem* $\mathbf{T}$ je čtvercová matice $I_n = (a_{ij})_{n\times n}$, kde pro každé $i, j \in \{1, 2, \dots, n\}$ platí

$$a_{ij} = \begin{cases} 1 & \text{pokud } \ i = j, \\ 0 & \text{pokud } \ i \neq j, \end{cases}$$

tj.

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

Jednotkovou matici také zapisujeme jako $I_n = \delta_{ij}$, kde δ_{ij} je tzv. *Kroneckerovo delta* rovnající se 1, pokud $i = j$, a 0 pokud $i \neq j$.

(20) Pro každou matici A typu $m \times n$ platí

$$I_m A = A = A I_n \ .$$

(21) Matice $A = (a_{ij})_{m\times n}$ a $B = (b_{jk})_{n\times p}$ můžeme také vynásobit *po blocích*

$$\left(\begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{21} & A_{22} \end{array}\right)\left(\begin{array}{c|c} B_{11} & B_{12} \\ \hline B_{21} & B_{22} \end{array}\right) = \left(\begin{array}{c|c} A_{11}B_{11} + A_{12}B_{21} & A_{11}B_{12} + A_{12}B_{22} \\ \hline A_{21}B_{11} + A_{22}B_{21} & A_{21}B_{12} + A_{22}B_{22} \end{array}\right) ,$$

pokud jsou všechny součiny bloků vpravo definované, tj. pokud jsou rozklady matic A, B do bloků *kompatibilní*. Matice můžeme kompatibilně rozdělit do více bloků a pak je vynásobit po blocích.

(22) U libovolné matice $A = (a_{ij})$ říkáme, že prvky a_{ii} tvoří *hlavní diagonálu*.

(23) Čtvercovou matici $A = (a_{ij})$ nazýváme
- *diagonální*, pokud $a_{ij} = 0$ kdykoliv $i \neq j$,
- *permutační*, má-li v každém řádku a každém sloupci právě jeden prvek 1 a ostatní 0,
- *horní trojúhelníková*, pokud $a_{ij} = 0$ kdykoliv $i > j$,
- *dolní trojúhelníková*, pokud $a_{ij} = 0$ kdykoliv $i < j$.

(24) Právě definované speciální typy matic jsou uzavřené na násobení, neboť pro čtvercové libovolné matice $A = (a_{ij})$ a $B = (b_{jk})$ téhož řádu n platí, že jejich součin AB je
  (a) diagonální, jsou-li obě matice A, B diagonální,
  (b) permutační matice, jsou-li obě matice A, B permutační,
  (c) horní trojúhelníková matice, jsou-li obě matice A, B horní trojúhelníkové matice,
  (d) horní trojúhelníková s prvky 1 na hlavní diagonále, jsou-li obě matice A, B horní trojúhelníkové s prvky 1 na hlavní diagonále,
  (e) dolní trojúhelníková matice, jsou-li obě matice A, B dolní trojúhelníkové matice,
  (f) dolní trojúhelníková s prvky 1 na hlavní diagonále, jsou-li obě matice A, B dolní trojúhelníkové s prvky 1 na hlavní diagonále.

(25) Soustava $A\mathbf{x} = \mathbf{o}$ s nulovou pravou stranou se nazývá *homogenní soustava lineárních rovnic*.

(26) Množina všech řešení homogenní soustavy lineárních rovnic $A\mathbf{x} = \mathbf{o}$ se nazývá *jádro matice* A nebo také *nulový prostor matice* A. Označujeme ji $\operatorname{Ker} A$.

(27) Je-li $\mathbf{u}$ jedno pevně zvolené partikulární řešení soustavy lineárních rovnic $A\mathbf{x} = \mathbf{b}$ nad tělesem $\mathbf{T}$, pak se množina všech řešení této soustavy rovná

$$\{\mathbf{u} + \mathbf{v} : \mathbf{v} \in \operatorname{Ker} A\} \;=\; \mathbf{u} + \operatorname{Ker} A \;.$$

(28) Je-li A matice typu $m \times n$ nad tělesem $\mathbf{T}$, pak definujeme *zobrazení* $f_A : \mathbf{T}^n \to \mathbf{T}^m$ *určené maticí* A předpisem

$$f_A(\mathbf{x}) = A\mathbf{x}$$

pro každý aritmetický vektor $\mathbf{x} \in \mathbf{T}^n$.

(29) Rotace kolem počátku souřadnic v tovině o úhel α proti směru hodinových ručiček je určená maticí

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

(30) Symetrie v rovině vzhledem k první souřadné ose je určená maticí

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

(31) Je-li $\mathbf{T}$ nějaké těleso a $n \in \mathbb{N}$, pak pro každé $j = 1, 2, \ldots, n$ označujeme $\mathbf{e}_j = (0, \ldots, 0, 1, 0, \ldots, 0)^T \in \mathbf{T}^n$ vektor, který má j-tou složku rovnou 1 a všechny ostatní složky rovné 0. Vektory $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$ nazýváme *prvky kanonické báze* v $\mathbf{T}^n$.

(32) Pro každou matici $A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ a každé $j = 1, 2, \ldots, n$ platí rovnost $f_A(\mathbf{e}_j) = \mathbf{a}_i$. Matice A určující zobrazení f_A je určená jenoznačně.

(33) Je-li A matice typu $m \times n$ nad tělesem $\mathbf{T}$, pak pro každé dva aritmetické vektory $\mathbf{x}, \mathbf{y} \in \mathbf{T}^n$ a každý prvek $s \in \mathbf{T}$ platí
- $f_A(s\mathbf{x}) = A(s\mathbf{x}) = s\,A\mathbf{x} = s\,f_A(\mathbf{x})$,
- $f_A(\mathbf{x} + \mathbf{y}) = A(\mathbf{x} + \mathbf{y}) = A\mathbf{x} + A\mathbf{y} = f_A(\mathbf{x}) + f_A(\mathbf{y})$.

(34) Jsou-li A matice typu $m \times n$ a B matice typu $n \times p$ nad stejným tělesem $\mathbf{T}$, pak zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^m$ a $f_B : \mathbf{T}^p \to \mathbf{T}^n$ můžeme složit v pořadí $f_A f_B$ a pro složené zobrazení $f_A f_B : \mathbf{T}^p \to \mathbf{T}^m$ platí

$$f_A f_B = f_{AB} \;,$$

protože pro každý vektor $\mathbf{x} \in \mathbf{T}^{\mathbf{n}}$ platí $f_A f_B(\mathbf{x}) = f_A(B\mathbf{x}) = A(B\mathbf{x}) = (AB)\mathbf{x} = f_{AB}(\mathbf{x})$.

(35) Symetrie v rovině vzhledem k přímce, kterou dostaneme z první souřadné osy otočením kolem počátku o úhel α v kladném směru, je určená maticí

$$\begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix} .$$

(36) Ortogonální projekce v rovině na první souřadnou osu je určená maticí

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

(37) Jednotková matice I_n nad tělesem $\mathbf{T}$ určuje identické zobrazení na množině $\mathbf{T}^n$.

(38) *Elementární matice* řádu m je libovolná matice, kterou dostaneme z identické matice I_m jednou elementární řádkovou úpravou.

(39) Je-li E elementární matice řádu m a A libovolná matice typu $m \times n$, pak matici EA dostaneme z matice A tou samou elementární řádkovou úpravou, kterou jsme dostali matici E z jednotkové matice I_m.

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

(41) Čtvercová matice A nad tělesem $\mathbf{T}$ řádu n se nazývá *regulární*, pokud je zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^n$ určené maticí A vzájemně jednoznačné (tj. bijekce). Čtvercová matice, která není regulární, se nazývá *singulární*.

(42) **10 ekvivalentních formulací, co znamená být regulární maticí**. Pro čtvercovou matici A řádu n nad tělesem $\mathbf{T}$ jsou následující tvrzení ekvivalentní:
   (a) matice A je regulární,
   (b) zobrazení f_A je na $\mathbf{T}^n$,
   (c) zobrazení f_A je prosté,
   (d) homogenní soustava $A\mathbf{x} = \mathbf{o}$ má jediné řešení $\mathbf{x} = \mathbf{o}$,
   (e) Gaussova eliminace převede matici A do horního trojúhelníkového tvaru s nenulovými prvky na hlavní diagonále (ekvivalentně do odstupňovaného tvaru bez nulových řádků),
   (f) matici A lze převést elementárními řádkovými úpravami do jednotkové matice I_n,
   (g) matice A je invertovatelná,
   (h) existuje čtvercová matice X řádu n taková, že $AX = I_n$,
   (i) existuje čtvercová matice Y řádu n taková, že $YA = I_n$,
   (j) matice A je součinem elementárních matic.

(43) Speciálně, čtvercová matice A je invertovatelná právě když je regulární.

(44) Inverzní matici k regulární matici A najdeme tak, že matici $(A|I_n)$ převedeme elementárními řádkovými úpravami do matice $(I_n|X)$. Matice X se pak rovná inverzní matici A^{-1}.

(45) Je-li $A\mathbf{x} = \mathbf{b}$ soustava lineárních rovnic s regulární maticí A, pak jednoznačně určené řešení této soustavy lze zapsat jako $\mathbf{x} = A^{-1}\mathbf{b}$. Soustavy lineárních rovnic takto neřešit! Je to třikrát pomalejší než Gaussova eliminace se zpětnou substitucí.

(46) Každá elementární matice je regulární, navíc inverzní matice k elementární matici je opět elementární matice.

(47) Jsou-li A, B regulární matice stejného řádu n nad stejným tělesem $\mathbf{T}$ a $t \in T$ nenulový prvek, pak platí
   (a) A^{-1} je regulární a platí $(A^{-1})^{-1} = A$,
   (b) A^T je regulární a platí $(A^T)^{-1} = (A^{-1})^T$,
   (c) $(tA)^T$ je regulární a platí $(tA)^{-1} = t^{-1}A^{-1}$,
   (d) AB je regulární a platí $(AB)^{-1} = B^{-1}A^{-1}$.

(48) Jsou-li A, B matice téhož typu $m \times n$ nad tělesem $\mathbf{T}$, pak B lze z A získat posloupností elementárních řádkových úprav právě tehdy, když existuje regulární matice R řádu m nad $\mathbf{T}$ taková, že $B = RA$.

(49) Pro regulární dolní (horní) trojúhelníkovou matici R řádu n platí, že inverzní matice R^{-1} je také dolní (horní) trojúhelníková. Má-li navíc matice R na hlavní diagonále všechny prvky rovné 1, pak i matice R^{-1} má samé jednotky na hlavní diagonále.

(50) **Věta o LU-rozkladu**. Je-li A regulární matice řádu n, u které při Gaussově eliminaci nemusíme prohazovat řádky, pak existují regulární matice L, U řádu n, pro které platí

- $A = LU$,
- L je dolní trojúhelníková s jednotkami na hlavní diagonále,
- U je horní trojúhelníková s nenulovými prvky na hlavní diagonále.

Matice L, U jsou těmito podmínkami určené jednoznačně.

(51) Horní trojúhelníkovou matici U dostaneme jako výsledek Gaussovy eliminace bez prohazování řádků použité na matici A. Dolní trojúhelníkovou matici $L = (\ell)_{i\times j}$ dostaneme tak, že na místo (i, j) pod hlavní diagonálou napíšeme koeficient ℓ_{ij}, kterým jsme násobili j-tý řádek a pak jej odečetli od i-tého při nulování prvku na místě (i, j). To znamená, že LU-rozklad regulární matice A najdeme Gaussovo eliminací matice A.

(52) Známe-li LU-rozklad $A = LU$ matice A, můžeme soustavu lineárních rovnic $A\mathbf{x} = \mathbf{b}$ převést na tvar $LU\mathbf{x} = \mathbf{b}$ a vyřešit ji ve dvou krocích. Napřed *přímou substitucí* najdeme řešení soustavy $L\mathbf{y} = \mathbf{b}$ a potom *zpětnou substitucí* vyřešíme soustavu $U\mathbf{x} = \mathbf{y}$. Celý postup je řádově rychlejší než opětovná Gaussova eliminace následovaná zpětnou substitucí.

(53) **Věta o LU-rozkladu s částečnou pivotací**. Je-li A regulární matice řádu n, pak existuje permutační matice P a regulární matice matice L, U, všechny řádu n, pro které platí

- $PA = LU$,
- L je dolní trojúhelníková matice s jednotkami na hlavní diagonále,
- U je horní trojúhelníková matice s nenulovými prvky na hlavní diagonále.

(54) Pro matici A typu $m \times n$ nad $\mathbf{T}$ je ekvivalentní

- existuje matice X typu $n \times m$ nad $\mathbf{T}$ taková, že $AX = I_m$,
- zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^m$ je na $\mathbf{T}^m$.

(55) Pro matici A typu $m \times n$ nad $\mathbf{T}$ je ekvivalentní

- existuje matice X typu $n \times m$ nad $\mathbf{T}$ taková, že $XA = I_n$,
- zobrazení $f_A : \mathbf{T}^n \to \mathbf{T}^m$ je prosté.

Klíčové znalosti ze čtvrté kapitoly nezbytné pro průběžné sledování přednášek s pochopením

(1) Operace s maticemi (sčítání, násobení číslem, transponování, součin, inverzní matice) a jejich algebraické vlastnosti (distributivita, asociativita násobení, atd.).
(2) Jednotkové a elementární matice, vyjádření elementární řádkové úpravy matice násobením elementární maticí zleva.
(3) Blokové násobení matic.
(4) Speciální typy matic, jejich součiny a inverzní matice k nim.
(5) Homogenní soustava rovnic a jádro matice.
(6) Vyjádření množiny všech řešení soustavy $A\mathbf{x} = \mathbf{b}$ ve tvaru $\{\mathbf{u} + \operatorname{Ker} A\}$.
(7) Zobrazení určené maticí a jeho jednoduché vlastnosti.
(8) Matice jednoduchých geometrických zobrazení.
(9) Matice složeného zobrazení $f_A f_B$.
(10) Regulární matice a různé podmínky ekvivalentní s regularitou.
(11) Metoda výpočtu inverzní matice.
(12) Vztah invertování a ostatních operací.

(13) Kdy lze jednu matici dostat z druhé posloupností elementárních řádkových úprav.
(14) Věta o LU-rozkladu.

5. Lineární prostory

Cíl. *Podobně jako jsme běžné vlastnosti počítání s reálnými čísly zobecnili do pojmu tělesa, zobecníme vlastnosti počítání s aritmetickými vektory do pojmu lineárního prostoru. Ukážeme si některé základní vlastnosti lineárních prostorů.*

5.1. **Definice, příklady a základní vlastnosti.** V kapitole o tělesech jsme se zabývali tím, jaké vlastnosti čísel využíváme při řešení lineárních rovnic, a reálná čísla jsme zobecnili na tělesa. Odměnou za větší abstraktnost je větší použitelnost. Stejná tvrzení a algoritmy, například pro řešení soustav rovnic nebo invertování matic, můžeme použít nejen pro reálná nebo komplexní čísla, ale také pro tělesa $\mathbb{Z}_p$, a jakákoliv jiná tělesa.

Aritmetické n-složkové vektory nad tělesem $\mathbf{T}$ můžeme sčítat a násobit prvky tělesa $\mathbf{T}$. Výsledkem je opět aritmetický n-složkový vektor nad tělesem $\mathbf{T}$. Řadu vlastností těchto dvou operací s aritmetickými vektory jsme dokázali v předchozí kapitole jako speciální případ vlastností počítání s maticemi nad tělesem $\mathbf{T}$. Všechny bezprostředně vyplývaly z axiomů tělesa $\mathbf{T}$.

V této kapitole zobecníme vlastnosti uvedených dvou operací s aritmetickými vektory nad tělesem $\mathbf{T}$ do abstraktního pojmu lineárního prostoru nad tělesem $\mathbf{T}$. Prvky lineárního prostoru mohou být nejen aritmetické vektory, ale například také nekonečné posloupnosti čísel, reálné funkce reálné proměnné, polynomy, apod.

Pojem lineárního prostoru umožňuje používat geometrickou intuici získanou z geometrie bodů a vektorů v rovině a prostoru ke studiu objektů, které na první pohled nemají s vektory nic společného. I při studiu reálných funkcí můžeme používat obrázky jako 30 nebo 31. Díky tomu, že reálné funkce reálné proměnné můžeme také sčítat a násobit reálným číslem a že tyto operace mají stejné základní vlastnosti jako počítání s reálnými aritmetickými vektory, dovoluje nám abstraktní pojem lineárního prostoru přenášet úvahy o vektorech na funkce na základě analogie.

Definice 5.1. Nechť $\mathbf{T}$ je těleso. *Lineárním 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 prvků množiny V prvky tělesa $\mathbf{T}$ (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 $a \cdot (\mathbf{u} + \mathbf{v}) = a \cdot \mathbf{u} + a \cdot \mathbf{v}$.

Při studiu lineárních prostorů budeme prvkům tělesa $\mathbf{T}$ říkat *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. Podobně jako při počítání v tělesech má $\cdot$ 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 prvků $\mathbf{u}, \mathbf{v} \in V$ a násobení skalárem $a\mathbf{v}$ je definováno pro každé $a \in T$ a $\mathbf{v} \in V$. Z definice rovněž vyplývá, že množina V je neprázdná, protože musí obsahovat podle (vS2) alespoň nulový prvek.

Axiomy (vS1), (vS2), (vS3), (vS4) jsou stejné jako axiomy pro sčítání v tělese. Stejně jako v tělese proto platí, že nulový prvek a opačné prvky jsou určené jednoznačně. Máme teď dvě různé nuly, 0 v tělese $\mathbf{T}$ a $\mathbf{o}$ v lineárním prostoru $\mathbf{V}$. Abychom je odlišili i jazykově, budeme v případě $0 \in \mathbf{T}$ mluvit o *nulovém skaláru* a výraz *nulový prvek* budeme nadále používat pouze pro prvek $\mathbf{o} \in \mathbf{V}$. 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 lineárního prostoru je množina všech uspořádaných 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 · (definovanými jako v definici 2.3). Označujeme jej $\mathbf{T}^n$.

To, že aritmetický vektorový prostor $\mathbf{T}^n$ je skutečně lineárním prostorem, jsme dokázali obecně pro matice v tvrzení 4.4 a tvrzení 4.7.

Aritmetické vektorové prostory jsou velmi konkrétní, zároveň ale v jistém smyslu „jediné“, příklady lineárních prostorů konečné dimenze. Uvidíme, že v každém lineárním prostoru konečné dimenze lze zvolit soustavu souřadnic (říkáme jí báze), a místo prvků prostoru 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 to, že lineární prostor (hlavně nad $\mathbb{R}$) si představujeme jako množinu šipek. Z tohoto prostoru se stává aritmetický vektorový prostor až po volbě nějaké soustavy souřadnic, kdežto operace s prvky lineárního prostoru na této volbě nezávisí. Žádná volba souřadnic nemusí být přirozená a v různých situacích mohou být užitečné různé soustavy souřadnic. 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 lineárních prostorů není ihned patrné, že se v podstatě jedná jen o uspořádané n-tice prvků nějakého 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.

Uvedeme několik dalších příkladů lineárních prostorů.

Příklad 5.3. 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 lineární prostor je „v podstatě“ aritmetický vektorový prostor $\mathbb{R}^{174}$, protože na polynom $a_0 + a_1x + \cdots + a_{173}x^{173}$ se můžeme dívat jako na uspořádanou 174-ici koeficientů $(a_0, a_1, \ldots, a_{173})^T$ a operace jsou při tomto pohledu stejné jako v $\mathbb{R}^{174}$.

Příklad 5.4. Množina všech matic typu 7×15 nad tělesem $\mathbb{Z}_3$ s běžnými operacemi + a · (nebo matic jiného daného typu nad jiným tělesem). Vzhledem k operacím

+ a · se tato množina chová stejně jako množina uspořádaných 105-tic, takže tento lineární prostor je „v podstatě“ aritmetický vektorový prostor $\mathbb{Z}_3^{105}$. To, že množina matic daného typu nad daným tělesem je lineární prostor jsme dokázali v tvrzení 4.4 a tvrzení 4.7. Když matice daného typu sčítáme a násobíme skalárem, můžeme se na ně dívat jako na k-tice prvků tělesa, ale tento pohled není výhodný například když matice interpretujeme jako zobrazení, násobíme je nebo invertujeme.

Lineární prostor matic typu $m \times n$ nad tělesem $\mathbf{T}$ s běžnými operacemi sčítání a násobení skalárem z $\mathbf{T}$ budeme označovat $\mathbf{T}^{m\times n}$. Aritmetický vektorový prostor $\mathbf{T}^n$ lze také chápat jako $\mathbf{T}^{n\times 1}$.

Následují další příklady lineárních prostorů.

Příklad 5.5. Množina všech podmnožin množiny $X = \{1, 2, \dots, 11\}$ (nebo jiné dané množiny X) spolu s operací symetrické diference, tj. $A+B = (A\setminus B)\cup(B\setminus A)$, a násobení skalárem $0 \cdot A = \emptyset, 1 \cdot A = A$ pro libovolné $A \subseteq X$, je lineární prostor nad $\mathbb{Z}_2$. Jako cvičení dokažte, že toto je skutečně lineární prostor, a vysvětlete proč je tento prostor „v podstatě“ $\mathbb{Z}_2^{11}$.

Příklad 5.6. Množina komplexních čísel je vektorovým prostorem nad $\mathbb{R}$ (s běžnými operacemi). Vzhledem ke sčítání a násobení reálným číslem se komplexní číslo $a + ib$ 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.

Příklad 5.7. Těleso $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ s běžnými operacemi sčítání a násobení racionálním číslem je lineární 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 prvku tělesa $\mathbb{Q}(\sqrt{2})$, důkaz je přenechán jako cvičení.

Vlastnosti podobných lineárních prostorů, jako například dimenze, jsou důležité například v již zmíněných problémech kvadratury kruhu, trisekce úhlu, zdvojení krychle a „neřešitelnosti“ rovnic pátého stupně.

Příklad 5.8. Množina všech funkcí z $\mathbb{R}$ do $\mathbb{R}$ tvoří spolu s přirozenými operacemi sčítání funkcí a násobení funkce reálným číslem lineární 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 $[0, 1]$.

Prostory funkcí jsou důležité příklady lineárních prostorů, kterými se budete v dalším studiu zabývat hlavně v jiných předmětech, například ve funkcionální analýze. My se soustředíme hlavně na lineární prostory konečné dimenze.

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

Tvrzení 5.9. *V každém lineárním prostoru* $\mathbf{V}$ *nad tělesem* $\mathbf{T}$ *platí*

(1) *nulový prvek* $\mathbf{o}$ *je určený jednoznačně,*
(2) *rovnice* $\mathbf{u} + \mathbf{x} = \mathbf{v}$ *má pro pevná* $\mathbf{u}, \mathbf{v} \in V$ *právě jedno řešení, speciálně, opačný prvek* $-\mathbf{v}$ *je vektorem* $\mathbf{v}$ *určen jednoznačně,*
(3) $0\mathbf{v} = \mathbf{o}$ *pro libovolný prvek* $\mathbf{v} \in V$*,*
(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 prvek* $\mathbf{v} \in V$*, speciálně* $-(-\mathbf{v}) = \mathbf{v}$*.*

Axiomy lineárního prostoru stejně jako právě uvedené jednoduché důsledky těchto axiomů 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 lineární prostory studovat, je *podprostor*.

Definice 5.10. Je-li $\mathbf{V}$ lineární prostor nad $\mathbf{T}$, pak lineární prostor $\mathbf{U}$ nad tělesem $\mathbf{T}$ 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 spolu s příslušnými operacemi tvoří podprostor.

Tvrzení 5.11. *Je-li* $\mathbf{V}$ *vektorový prostor nad tělesem* $\mathbf{T}$*, pak neprázdná podmnožina* U *množiny* V *je podprostorem* $\mathbf{V}$ *právě tehdy, když současně*

- *(„uzavřenost na sčítání“) pro libovolné* $\mathbf{u}, \mathbf{v} \in U$ *platí* $\mathbf{u} + \mathbf{v} \in U$*,*
- *(„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 množina U musí být uzavřená na sčítání a násobení skalárem, neboť spolu s těmito operacemi tvoří lineární prostor.

Předpokládejme, že U je neprázdná množina uzavřená na sčítání a násobení skalárem. Pak opačný prvek k $\mathbf{u} \in U$ je v U, protože $-\mathbf{u}$ lze napsat jako $(-1) \cdot \mathbf{u}$. Rovněž nulový prvek lineárního 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 $\mathbf{V}$. □

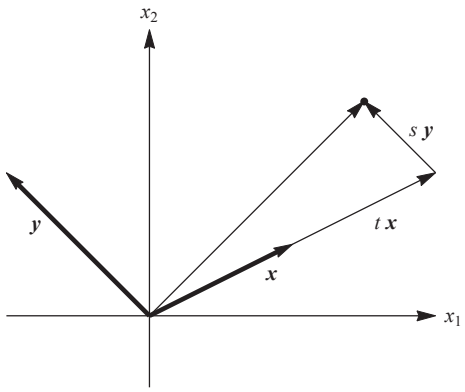
Množina $\{\mathbf{o}\}$ tvořená pouze nulovým prvkem $\mathbf{o}$ je vždy podprostorem $\mathbf{V}$, rovněž celý prostor $\mathbf{V}$ je podprostorem $\mathbf{V}$. Těmto podprostorům říkáme *triviální*, ostatní podprostory nazýváme *netriviální* nebo *vlastní*. Zdůrazněme pozorování z důkazu předchozího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

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 $\mathbf{o}$. 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 skalární násobky $\{s\mathbf{y} : s \in \mathbb{R}\}$, 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 $\{s\mathbf{y} : s \in \mathbb{R}\}$.

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 $\{\mathbf{o}\}$ 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 $U \leq \mathbb{R}^3$. 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 $\mathbf{y}$,



Obrázek 58. Podprostor $\mathbb{R}^2$ obsahující přímku a vektor mimo ni

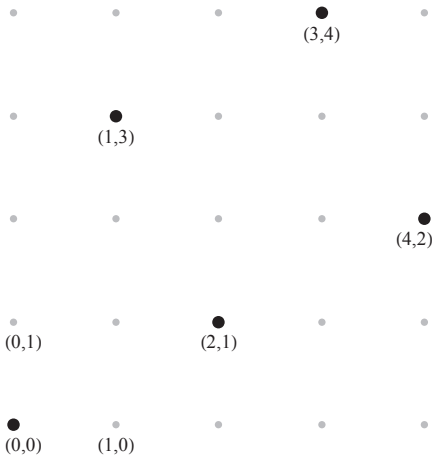
pak $\{s\mathbf{y} : s \in \mathbb{R}\} \subseteq U$ a U pak obsahuje celou rovinu určenou body $\mathbf{x}, \mathbf{y}$ a počátkem $\mathbf{o}$, což je rovina s parametrickým vyjádřením

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

Obsahuje-li U ještě nějaký jiný vektor mimo tuto rovinu, 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 $\mathbf{o} \neq \mathbf{x} \in T^2$.



Obrázek 59. Přímka $\{t(2,1)^T : t \in \mathbb{Z}_5\}$ v prostoru $\mathbb{Z}_5^2$

S podprostory $\mathbf{T}^n$ jsme se již setkali už v předchozí kapitole při řešení homogenních soustav lineárních rovnic. Zde je třeba si připomenout definici 4.32 jádra matice A jako množinu všech řešení homogenní soustavy $A\mathbf{x} = \mathbf{o}$.

Tvrzení 5.12. *Pro libovolnou matici A typu $m \times n$ nad $\mathbf{T}$ platí, že* $\operatorname{Ker} A$ *je podprostor* $\mathbf{T}^n$*, neboli* $\operatorname{Ker} A \leq \mathbf{T}^n$*.*

Důkaz. Podle tvrzení 5.11 stačí ověřit, že množina $\operatorname{Ker} A$ je neprázdná a uzavřená na sčítání a násobení skalárem.

Protože $A\mathbf{o} = \mathbf{o}$, množina $\operatorname{Ker} A$ obsahuje nulový prvek $\mathbf{o} \in \mathbf{T}^n$, 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 $s \in T$, pak $A(s\mathbf{u}) = s(A\mathbf{u}) = s\mathbf{o} = \mathbf{o}$, tedy $s\mathbf{u} \in \operatorname{Ker} A$. □

Geometricky je $\operatorname{Ker} A$ vzorem nulového vektoru při zobrazení f_A, tj. $\operatorname{Ker} A = f_A^{-1}(\mathbf{o})$. Vzor $f_A^{-1}(\mathbf{b})$ nenulového vektoru $\mathbf{b} \in \mathbf{T}^m$ (neboli množina všech řešení soustavy $A\mathbf{x} = \mathbf{b}$ **není** podprostor $\mathbf{T}^n$, viz cvičení. Tato množina je sice „rovný útvar“, ale neobsahuje nulový prvek $\mathbf{o} \in \mathbf{T}^n$. Množinám tvaru $f_A^{-1}(\mathbf{b})$ budeme později říkat afinní podprostory $\mathbf{T}^n$. Každý podprostor $\mathbf{T}^n$ je tedy také afinní podprostor $\mathbf{T}^n$, ale pouze afinní podprostory $\mathbf{T}^n$ obsahující $\mathbf{o} \in \mathbf{T}^n$ jsou současně podprostory lineárního prostoru $\mathbf{T}^n$.

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

5.2.4. *Lineární kombinace, podprostor generovaný množinou, množina generátorů.* Už několikrát jsme se setkali s množinami typu $\{t\mathbf{u} + s\mathbf{v} + r\mathbf{w} : r, s, t \in \mathbb{R}$, kde $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w}$ jsou nějaké reálné aritmetické vektory. Naposledy při popisu podprostorů $\mathbb{R}^3$. Takovým výrazům říkáme lineární kombinace vektorů $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w}$. Lineární kombinace můžeme definovat v každém lineárním prostoru.

Definice 5.13. Jsou-li $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ prvky lineárního prostoru $\mathbf{V}$ nad $\mathbf{T}$ a $t_1, t_2, \ldots, t_k \in \mathbf{T}$ skaláry, tj. prvky tělesa $\mathbf{T}$, pak prvek

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

se nazývá *lineární kombinace prvků* $\mathbf{v}_1$, $\mathbf{v}_2$, …, $\mathbf{v}_k \in \mathbf{V}$. 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 prvků prostoru $\mathbf{V}$. Součet nekonečně mnoha prvků v lineárním prostoru není definován.

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 5.14. Nechť $\mathbf{V}$ je lineární 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. Poznamenejme, že množina X může být i nekonečná. Je také dobré si všimnout, že zatímco v množině X je každý prvek pouze jednou, v součtu určujícím lineární kombinaci prvků množiny X se může jeden a ten samý prvek vyskytnout vícekrát.

Příklad 5.15. $\langle \emptyset \rangle = \{\mathbf{o}\}$ – lineární obal prázdné množiny je triviální prostor tvořený nulovým vektorem.

Příklad 5.16. 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 v předcházejícím příkladu obvykle vynecháváme pro přehlednost závorky $\{\ldots\}$ označující množinu. Někdy říkáme „lineární obal vektorů $\ldots$“, místo formálně přesného „lineární obal množiny vektorů $\{\ldots\}$“.

Tvrzení 5.17. *Pro libovolný lineární 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 prvků prázdné podmnožiny X, tj. vektor $\mathbf{o}$.

Součet lineární kombinace $s_1\mathbf{v}_1 + s_2\mathbf{v}_2 + \cdots + s_k\mathbf{v}_k$ vektorů $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k \in X$ s koeficienty s_1, s_2, …, $s_k \in T$ a lineární kombinace $t_1\mathbf{w}_1 + t_2\mathbf{w}_2 + \cdots + t_l\mathbf{w}_l$ vektorů $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_l \in X$ s koeficienty t_1, t_2, …, t_l se rovná

$$s_1\mathbf{v}_1 + s_2\mathbf{v}_2 + \cdots + s_k\mathbf{v}_k + t_1\mathbf{w}_1 + t_2\mathbf{w}_2 + \cdots + t_l\mathbf{w}_l \ ,$$

což je lineární kombinace vektorů $\mathbf{v}_1, \ldots, \mathbf{v}_k, \mathbf{w}_1, \ldots, \mathbf{w}_l \in X$ s koeficienty s_1, …, s_k, t_1, …, t_l.

Konečně, r-násobkem lineární kombinace $s_1\mathbf{v}_1 + s_2\mathbf{v}_2 + \cdots + s_k\mathbf{v}_k$ vektorů $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k \in X$ s koeficienty $s_1, s_2, \ldots, s_k$ je lineární kombinace

$$r(s_1\mathbf{v}_1 + s_2\mathbf{v}_2 + \cdots + s_k\mathbf{v}_k) = (rs_1)\mathbf{v}_1 + (rs_2)\mathbf{v}_2 + \cdots + (rs_k)\mathbf{v}_k$$

stejných vektorů s koeficienty rs_1, rs_2, …, rs_k. □

Obsahuje-li podprostor $U \leq \mathbf{V}$ množinu X, pak díky uzavřenosti na sčítání a násobení skalárem obsahuje také 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 5.18. Je-li $\mathbf{V}$ lineární prostor nad $\mathbf{T}$ a $X \subseteq V$. Pokud $\langle X \rangle = V$, pak říkáme, že X je *množina generátorů prostoru* $\mathbf{V}$, nebo také že X *generuje* $\mathbf{V}$.

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

Příklad 5.19.

- 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 vyjádřit 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 podmnožina $\mathbf{T}^2$ obsahující vektory $(1,0)^T$ a $(0,1)^T$ je množinou generátorů $\mathbf{T}^2$.
- 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 množinou generátorů prostoru všech reálných polynomů stupně nejvýše 2.

Příklad 5.20. 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 5.21. Definujeme $\mathbb{R}^\omega$ jako prostor všech posloupností reálných čísel s operacemi prováděnými po složkách, podobně jako s aritmetickými vektory. Množina

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

negeneruje prostor $\mathbb{R}^\omega$. Snadno lze ověřit, že $\langle X \rangle$ se rovná množině všech posloupností reálných čísel, které obsahují pouze konečně mnoho nenulových prvků.

Také množina všech posloupností reálných čísel konvergujících k 0 je podprostor $\mathbb{R}^\omega$ a obsahuje $\langle X \rangle$.

Jiným zajímavým podprostorem $\mathbb{R}^\omega$ je 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.

Následující tvrzení budeme mlčky používat při práci s lineárním obalem konečné množiny nebo posloupnosti prvků.

Tvrzení 5.22. *Je-li $(\mathbf{v}_1, \dots, \mathbf{v}_l)$ konečná posloupnost prvků lineárního prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$, pak*

$$\langle \mathbf{v}_1, \dots, \mathbf{v}_l \rangle = \{ t_1\mathbf{v}_1 + \cdots + t_l\mathbf{v}_l : t_1, \dots, t_l \in T \} \ .$$

Důkaz. Inkluze „$\supseteq$“ plyne triviálně z definice lineárního obalu.

Naopak, je-li $\mathbf{u} \in \langle \mathbf{v}_1, \dots, \mathbf{v}_l \rangle$, pak $\mathbf{u} = s_1\mathbf{u}_1 + \cdots + s_k\mathbf{u}_k$, kde každý z vektorů $\mathbf{u}_i$ leží v množině $\{\mathbf{v}_1, \dots, \mathbf{v}_l\}$. V součtu $s_1\mathbf{u}_1 + \cdots + s_k\mathbf{u}_k$ seskupíme sčítance podle vektorů $\mathbf{v}_1, \dots, \mathbf{v}_l$ a užitím (vD1) nahradíme jediným sčítancem tvaru $t_j\mathbf{v}_j$. Nakonec pro chybějící $\mathbf{v}_j$ přidáme sčítanec $0\mathbf{v}_j$. Tím získáme vyjádření $\mathbf{u} = t_1\mathbf{v}_1 + t_2\mathbf{v}_2 + \cdots + t_l\mathbf{v}_l$. □

5.2.5. *Sloupcový a řádkový prostor matice.* Každá matice přirozeně definuje dvě množiny aritmetických vektorů – množinu řádkových vektorů a množinu sloupcových vektorů. Prostorům, které tyto množiny generují, říkáme řádkový a sloupcový prostor.

Definice 5.23. Je-li A matice typu $m \times n$ nad $\mathbf{T}$, pak *sloupcovým prostorem matice* A rozumíme podprostor $\mathbf{T}^m$ generovaný množinou sloupcových vektorů matice A a značíme jej $\operatorname{Im} A$.

$$\operatorname{Im} A = \langle \mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n \rangle \leq \mathbf{T}^m$$

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

$$\operatorname{Im} A^T = \langle \tilde{\mathbf{a}}_1, \tilde{\mathbf{a}}_2, \dots, \tilde{\mathbf{a}}_m \rangle \leq \mathbf{T}^n$$

Příklad 5.24. 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 nějakého 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 5.25. 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 5.19 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 určené maticí 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 regulární maticí 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 určeným maticí A je jádro $\operatorname{Ker} A$. Ten se řádkovými úpravami (neboli násobením zleva regulární maticí) rovněž nemění. To již vlastně víme, neboť $\operatorname{Ker} A$ je množina všech řešení soustavy $A\mathbf{x} = \mathbf{o}$ a ta se nemění provedením elementární úpravy. Maticově, $\operatorname{Ker}(EA) = \operatorname{Ker} A$ pro každou elementární matici E. Protože každá regulární matice R je součinem elementárních matic, máme $\operatorname{Ker}(RA) = \operatorname{Ker} A$. V důkazu následujícího tvrzení zvolíme rychlejší postup.

Tvrzení 5.26. *Nechť $A = (\mathbf{a}_1|\dots|\mathbf{a}_n)$ je matice typu $m \times n$ nad $\mathbf{T}$ a R je regulární matice řádu m. Pak*

$$\operatorname{Im}(RA) = \langle R\mathbf{a}_1, R\mathbf{a}_2, \dots, R\mathbf{a}_n \rangle, \quad \operatorname{Ker} A = \operatorname{Ker}(RA), \quad \operatorname{Im} A^T = \operatorname{Im}(RA)^T \ .$$

Důkaz. První část je důsledkem definice součinu matic 4.12.

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 $\mathbf{x} \in \operatorname{Ker}(RA)$. Tím jsme dokázali $\operatorname{Ker} A \subseteq \operatorname{Ker}(RA)$ pro každou matici A a regulární matici R.

Je-li naopak $\mathbf{x} \in \operatorname{Ker}(RA)$, pak $RA\mathbf{x} = \mathbf{o}$. Protože R je regulární, je také R^{-1} regulární podle tvrzení 4.65.1. Podle předcházejícího odstavce pak platí $\operatorname{Ker}(RA) \subseteq$

$\operatorname{Ker}(R^{-1}RA) = \operatorname{Ker}(A)$. Tím je dokázána opačná inkluze nutná k ověření druhé rovnosti $\operatorname{Ker} A = \operatorname{Ker}(RA)$.

Zbývá dokázat třetí rovnost. Opět si uvědomíme, že násobení v matici RA je každý řádek lineárních kombinací řádků matice A podle tvrzení 4.22. To znamená, že každý řádek matice RA leží v lineárním obalu řádků matice A, tj. v řádkovém prostoru $\operatorname{Im} A^T$, tj. $\operatorname{Im}(RA)^T \subseteq \operatorname{Im} A^T$. Stejnou úvahou jako v předchozím odstavci získáme opačnou inkluzi $\operatorname{Im}(A^T) = \operatorname{Im}(R^{-1}RA)^T \subseteq \operatorname{Im}(RA)^T$. □

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 třetí rovnosti předchozího tvrzení na matici A^T místo A a R^T místo R dostaneme $\operatorname{Im}(A^T)^T = \operatorname{Im}(R^TA^T)^T$, což je po úpravě za použití rovností $(A^T)^T = A$ a $(R^TA^T)^T = AR$ dokazuje rovnost $\operatorname{Im} A = \operatorname{Im}(AR)$.

Důsledek 5.27. *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 5.16. Důvod je ten, že třetí vektor $(9,12,15)^T$ lze napsat jako lineární kombinaci zbývajících dvou vektorů. Množinám prvků libovolného lineárního prostoru, ve kterých žádný z prvků není lineární kombinací ostatních, říkáme *lineárně nezávislé*. Z formulačních důvodů definujeme lineární (ne)závislost pro posloupnosti prvků lineárního prostoru, nikoliv pro množiny.

Definice 5.28. Nechť $\mathbf{V}$ je lineární prostor nad tělesem $\mathbf{T}$. Posloupnost prvků $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k)$ prostoru $\mathbf{V}$ se nazývá *lineárně závislá*, pokud některý z prvků $\mathbf{v}_i$ je lineární kombinací zbývajících prvků $\mathbf{v}_1$, $\mathbf{v}_2$, …, $\mathbf{v}_{i-1}$, $\mathbf{v}_{i+1}$, …, $\mathbf{v}_k$.

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

Později si ukážeme, jak lineární (ne)závislost definovat i pro nekonečné soubory vektorů.

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

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

ekvivalentně

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

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.

Někdy se používá nepřesná formulace typu „vektory … jsou lineárně nezávislé“, apod. Uvědomte si, že lineární (ne)závislost není vlastnost vektorů ale jejich posloupností. Takže takovou formulaci je potřeba vždy přeložit jako „posloupnost vektorů … je lineárně nezávislá“.

Příklad 5.29. 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 prvků $(\mathbf{u}, \mathbf{v}, \mathbf{u}+\mathbf{v})$ v libovolném lineárním prostoru je vždy lineárně závislá.

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 prvek, tak je lineárně závislá, protože nulový prvek je lineární kombinací ostatních prvků posloupnosti. To platí i v případě, že posloupnost obsahuje jediný prvek $\mathbf{o}$ díky tomu, že nulový prvek je lineární kombinací prvků prázdné množiny.
- Jednočlenná posloupnost $(\mathbf{v})$ je lineárně nezávislá právě tehdy, když $\mathbf{v} \neq \mathbf{o}$.
- Kdykoliv posloupnost obsahuje dva stejné prvky, je lineárně závislá. Obecněji, pokud je některý z prvků 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 aritmetických 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 řečeno, pokud je podposloupnost prvků lineárně závislá, tak 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 prvků $\mathbf{v}_1, \ldots, \mathbf{v}_k$ ukázat, že jej nelze vyjádřit jako lineární kombinaci ostatních. Snazší je použít bod (2) nebo (3) z následujícího pozorování, které dává elegantnější charakterizaci lineární nezávislosti.

Tvrzení 5.30. *Nechť $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ je posloupnost prvků lineárního prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$. Následující tvrzení jsou ekvivalentní.*

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

(2) *Žádný z prvků $\mathbf{v}_i$ $(1 \leq i \leq k)$ nelze vyjádřit jako lineární kombinaci předchozích prvků $\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}$.*

(3) *Nulový prvek $\mathbf{o}$ lze vyjádřit jako lineární kombinaci prvků $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ 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 z rovnosti

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

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

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

Důkaz. (1) $\Rightarrow$ (2) je zřejmé.

(2) $\Rightarrow$ (3). Pokud platí

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

a jedno z čísel $a_1, a_2, \ldots, a_k$ je nenulové, zvolíme největší takové i, pro které $a_i \neq 0$. Pak můžeme upravit

$$a_i\mathbf{v}_i = -a_1\mathbf{v}_1 - \ldots - a_{i-1}\mathbf{v}_{i-1}$$

a

$$\mathbf{v}_i = -a_i^{-1}a_1\mathbf{v}_1 - \ldots - a_i^{-1}a_{i-1}\mathbf{v}_i \ ,$$

z čehož vidíme, že podmínka (2) není splněna.

(3) $\Rightarrow$ (4). Pokud máme dvě vyjádření prvku $\mathbf{u}$

$$\mathbf{u} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k = b_1\mathbf{v}_1 + b_2\mathbf{v}_2 + \cdots + b_k\mathbf{v}_k \ ,$$

jejich odečtením 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 (3) dostáváme, že $a_i - b_i = 0$ pro každé i, neboli $a_i = b_i$ a tedy obě vyjádření vektoru $\mathbf{u}$ jsou stejná.

(4) $\Rightarrow$ (3) je triviální.

(3) $\Rightarrow$ (1). Pokud je posloupnost prvků $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ lineárně závislá, pak pro nějaké i je prvek $\mathbf{v}_i$ lineární kombinací ostatních, tedy

$$\mathbf{v}_i = b_1\mathbf{v}_1 + b_2\mathbf{v}_2 + \cdots + b_{i-1}\mathbf{v}_{i-1} + b_{i+1}\mathbf{v}_{i+1} + \cdots + b_k\mathbf{v}_k \ .$$

Poslední rovnost přepíšeme do tvaru

$$\mathbf{o} = b_1\mathbf{v}_1 + b_2\mathbf{v}_2 + \cdots + b_{i-1}\mathbf{v}_{i-1} + (-1)\mathbf{v}_i + b_{i+1}\mathbf{v}_{i+1} + \cdots + b_k\mathbf{v}_k \ ,$$

takže dostáváme netriviální lineární kombinaci prvků $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ s koeficienty $a_i = -1$ a $a_j = b_j$ pro $j \neq i$, která se rovná nulovému prvku. □

Bod (3) lze formulovat také tak, že posloupnost prvků lineárního prostoru je lineárně závislá právě tehdy, když existuje její *netriviální* lineární kombinace, která se rovná nulovému vektoru. Netriviální znamená, že alespoň jeden koeficient je nenulový (skalár). Ještě jedna ekvivalentní formulace je ve cvičeních: posloupnost prvků $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ je lineárně nezávislá právě tehdy, když žádný z jejích prvků není v lineárním obalu předchozích (tj. pro každé i platí $\mathbf{v}_i \notin \langle \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{i-1} \rangle$).

Připomeňme, že prvky $\mathbf{v}_1, \ldots, \mathbf{v}_k$ generují lineární prostor $\mathbf{V}$, pokud se každý vektor dá napsat jako lineární kombinace těchto prvků alespoň jedním způsobem. Bod (4) ukazuje, že lineární nezávislost je jakýmsi opakem.

Příklad 5.31. Zjistíme, zda je posloupnost aritmetických vektorů

$$((1,1,1,1)^T, (1,2,1,1)^T, (0,1,0,1)^T)$$

je lineárně nezávislá v prostoru $\mathbb{Z}_3^4$. Pokusíme se vyjádřit nulový vektor jako lineární kombinaci vektorů 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 aritmetických vektorů, která se rovná nulovému vektoru má všeschny koeficienty nulové, tj. je triviální. Podle bodu (3) z předchozího tvrzení je daná posloupnost aritmetických vektorů lineárně nezávislá.

Tento příklad nám dává návod jak zjistit, je-li daná posloupnost aritmetických vektorů lineárně (ne)závislá. Formulujeme učiněné pozorování jako tvrzení.

Tvrzení 5.32. *Posloupnost sloupcových vektorů matice $A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ typu $m \times n$ nad tělesem $\mathbf{T}$ tvoří lineárně nezávislou posloupnost v $\mathbf{T}^m$ právě tehdy, když $\operatorname{Ker} A = \{\mathbf{o}\}$, tj. právě když má soustava $A\mathbf{x} = \mathbf{o}$ pouze triviální řešení $\mathbf{x} = \mathbf{o}$.*

Důkaz. Je-li $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, pak podle definice 4.10 součinu matice s aritmetickým vektorem platí $A\mathbf{x} = x_1\mathbf{a}_1 + x_2\mathbf{a}_2 + \cdots + x_n\mathbf{a}_n$. Z definice 4.32 jádra matice plyne, že $\operatorname{Ker} A = \{\mathbf{o}\}$ právě když je nulový vektor $\mathbf{o} \in \mathbf{T}^n$ jediným řešení soustavy $A\mathbf{x} = \mathbf{o}$. To platí právě když z rovnosti

$$x_1\mathbf{a}_1 + x_2\mathbf{a}_2 + \cdots + x_n\mathbf{a}_n = \mathbf{o}$$

plyne $x_1 = x_2 = \cdots = x_n = 0$, což je podmínka (3) z tvrzení 5.30 ekvivalentní lineární nezávislosti posloupnosti sloupcových vektorů matice A. □

Příklad 5.33. Posloupnost $(3i+5, 2, 3), (5, 2+i, 1), (4, 2, 12), (\pi, e^\pi, 4)$ v prostoru $\mathbb{C}^3$ je lineárně závislá.

K důkazu můžeme využít předchozí tvrzení. Dané aritmetické vektory si napíšeme do sloupců matice A typu 3×4. Při řešení soustavy $A\mathbf{x} = \mathbf{o}$ máme díky typu matice A aspoň jednu volnou proměnnou, protože proměnné jsou 4 a pivotů může být nejvýše tolik, kolik je řádků v matici A. Z toho plyne, že soustava má netriviální řešení. Stačí za jednu volnou proměnnou dosadit například 1, za ostatní volné proměnné, pokud jsou, skalár 0, a dopočítat volné proměnné zpětnou substitucí.

Na tomto místě si znovu uvědomme, že aritmetické vektorové prostory tvoří jen jeden z mnoha možných typů lineárních 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 prvky $\cos(2x), \sin x + e^x, x^3$ lineárního prostoru spojitých reálných funkcí jedné reálné proměnné?

Příklad 5.34. Posloupnost $(1, \sqrt{2})$ je lineárně nezávislá v lineárním prostoru $\mathbb{R}$ nad tělesem $\mathbb{Q}$, protože $\sqrt{2}$ je iracionální číslo. Stejná posloupnost je lineárně závislá v lineárním prostoru $\mathbb{R}$ nad tělesem $\mathbb{R}$, protože např. $\sqrt{2}$ je $\sqrt{2}$-násobkem vektoru 1. Protože je druhý lineární prostor nad tělesem reálných čísel, můžeme použít číslo $\sqrt{2} \in \mathbb{R}$ jako koeficient lineární kombinace.

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 hodit o něco později.

Rovnou si také všimneme, že řádkové úpravy nemění ani lineární (ne)závislost sloupců. Tvrzení nejprve formulujeme pro sloupce. Řádkovou verzi dostaneme transponováním.

Tvrzení 5.35. *Nechť $A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ je matice typu $m \times n$ nad tělesem $\mathbf{T}$, R je regulární matice řádu m a Q je regulární matice řádu n. Pak platí*

(1) *posloupnost $(\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n)$ sloupcových vektorů matice A je lineárně nezávislá právě tehdy, když je lineárně nezávislá posloupnost sloupcových vektorů matice AQ,*
(2) *posloupnost $(\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n)$ sloupcových vektorů matice A je lineárně nezávislá právě tehdy, když je lineárně nezávislá posloupnost sloupcových vektorů matice RA.*

Důkaz. Použijeme pozorování formulované jako tvrzení 5.32, které říká, že posloupnost sloupcových vektorů matice B je lineárně nezávislá právě tehdy, když soustava $B\mathbf{x} = \mathbf{o}$ má pouze triviální řešení.

Předpokládejme, že posloupnost $(\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n)$ sloupcových vektorů matice A je lineárně nezávislá a že $\mathbf{x}$ je řešením soustavy $AQ\mathbf{x} = \mathbf{o}$. Potom $Q\mathbf{x}$ je řešením soustavy $A(Q\mathbf{x}) = \mathbf{o}$ a protože posloupnost $(\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n)$ je lineárně nezávislá, platí $Q\mathbf{x} = \mathbf{o}$. Odtud plyne, že $\mathbf{x} = \mathbf{o}$ (použijeme například bod (4) charakterizace regulárních matic z věty 4.59, nebo bod (7) a vynásobíme rovnost $Q\mathbf{x} = \mathbf{o}$ zleva maticí Q^{-1}). Ukázali jsme, že soustava $AQ\mathbf{x} = \mathbf{o}$ má pouze triviální řešení, takže posloupnost sloupcových vektorů matice AQ je lineárně nezávislá.

Opačná implikace se dá dokázat užitím právě dokázané implikace, nahradíme-li matici A maticí AQ a matici Q maticí Q^{-1}.

Druhou ekvivalenci jsme již vlastně dokázali v tvrzení 5.26. Platí rovnost $\operatorname{Ker}(RA) = \operatorname{Ker} A$, takže soustava $A\mathbf{x} = \mathbf{o}$ má netriviální řešení právě tehdy, když má soustava $RA\mathbf{x} = \mathbf{o}$ netriviální řešení. □

Z rovnosti $\operatorname{Ker}(RA) = \operatorname{Ker} A$ plyne dokonce více než druhá ekvivalence v předchozím tvrzení. Pro posloupnost sloupcových vektorů matice $A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ platí

$$x_1\mathbf{a}_1 + x_2\mathbf{a}_2 + \cdots + x_n\mathbf{a}_n = \mathbf{o}$$

právě když $\mathbf{x} \in \operatorname{Ker} A = \operatorname{Ker}(RA)$, což platí právě když

$$x_1R\mathbf{a}_1 + x_2R\mathbf{a}_2 + \cdots + x_nR\mathbf{a}_n = \mathbf{o}\ ,$$

neboť $RA = (R\mathbf{a}_1|R\mathbf{a}_2|\cdots|R\mathbf{a}_n)$ podle definice součinu matic. Neformálně můžeme říct, že mezi sloupcovými vektory matice A platí stejné lineární závislosti jako

mezi sloupcovými vektory matice RA. Například pokud $2\mathbf{a}_1 + 3\mathbf{a}_2 - 4\mathbf{a}_3 = \mathbf{o}$, pak pro matici $RA = (\mathbf{b}_1|\mathbf{b}_2|\mathbf{b}_3)$ platí $2\mathbf{b}_1 + 3\mathbf{b}_2 - 4\mathbf{b}_3 = \mathbf{o}$, a naopak. Slovy, součet 2-násobku prvního sloupce, 3-násobku druhého sloupce a (-4)-násobku třetího sloupce v matici A je nulový vektor právě tehdy, když součet 2-násobku prvního sloupce, 3-násobku druhého sloupce a (-4)-násobku třetího sloupce v matici RA je nulový vektor.

Důsledek 5.36. *Elementární řádkové úpravy nemění lineární (ne)závislost posloupnosti sloupcových vektorů ani posloupnosti řádkových vektorů matice.*

Elementární sloupcové úpravy nemění lineární (ne)závislost posloupnosti sloupcových vektorů ani posloupnosti řádkových vektorů matice.

Důkaz. Zvolíme-li v předchozím tvrzení za regulární matice R nebo Q elementární matice stejného řádu, dostaneme obě tvrzení pro případ posloupnosti sloupcových vektorů maticde. Protože posloupnost řádkových vektorů matice A se rovná posloupnosti sloupcových vektorů transponované matice A^T, plynou řádkové verze z právě dokázaných sloupcových verzí. □

Zbývá nahlédnout, kdy je lineárně nezávislá posloupnost řádkových vektorů matice v řádkově odstupňovaném tvaru. Z předchozího tvrzení a tvrzení 5.32 vidíme, kdy je posloupnost sloupcových vektorů matice v odstupňovaném tvaru lineárně nezávislá. Je to právě tehdy, když příslušná homogenní soustava nemá žádné volné proměnné.

Je zřejmé, že je-li v matici nulový řádek, pak je posloupnost jejích řádkových vektorů lineárně závislá.

Tvrzení 5.37. *Posloupnost řádkových vektorů matice v odstupňovaném tvaru je lineárně nezávislá právě tehdy, když matice neobsahuje nulový řádek.*

Důkaz. Implikace zleva doprava je zřejmá.

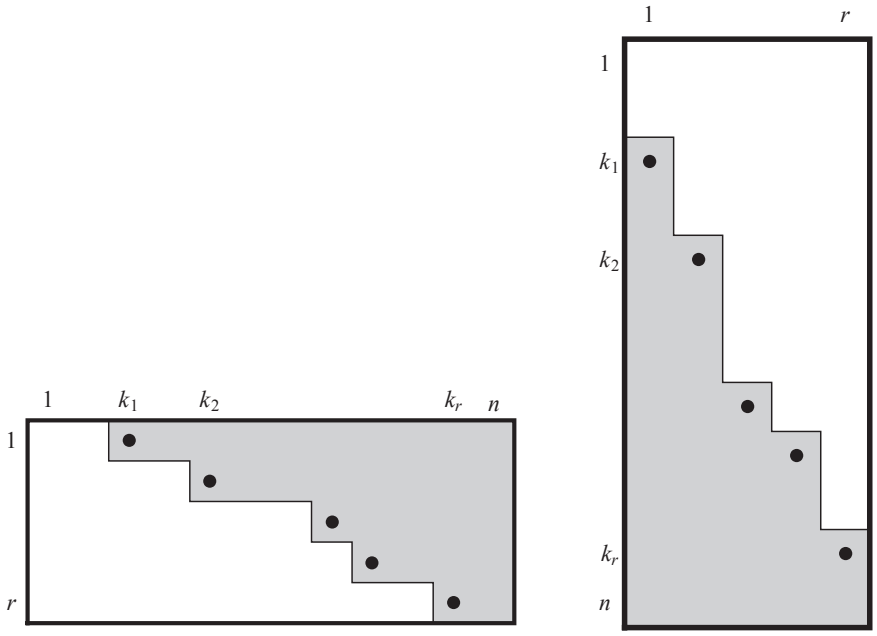
Předpokládejme, že matice A typu $m \times n$ bez nulového řádku je v odstupňovaném tvaru a vezmeme parametry $r, k_1, \ldots, k_r$ z definice odstupňovaného tvaru. Protože A nemá nulový řádek je $r = m$. K důkazu lineární nezávislosti posloupnosti řádkových vektorů matice A stačí dokázat lineární nezávislost posloupnosti sloupcových vektorů matice A^T, tj. dokázat, že homogenní soustava $A^T\mathbf{x} = \mathbf{o}$ má pouze triviální řešení (viz opět tvrzení 5.32). Ze soustavy $A^T\mathbf{x} = \mathbf{o}$ vybereme pouze rovnice s pořadovými čísly k_1, k_2, …, k_r. Tato vybraná soustava má dolní trojúhelníkovou matici s nenulovými prvky na hlavní diagonále a ta má pouze triviální nulové řešení.

□

Myšlenku důkazu můžeme zobecnit na užitečné pozorování. Máme-li posloupnost n-složkových aritmetických vektorů $(\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_p)$ nad tělesem $\mathbf{T}$, zapíšeme je do sloupců matice $A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_p)$ nad $\mathbf{T}$. Ta je maticí homogenní soustavy lineárních rovnic $A\mathbf{x} = \mathbf{o}$. Pokud z této soustavy vybereme nějakých $m \leq n$ rovnic takových, že už tyto rovnice mají pouze triviální nulové řešení, pak také celá soustava $A\mathbf{x} = \mathbf{o}$ má pouze triviální nulové řešení. To znamená, že i původní posloupnost $(\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_p)$ lineárně nezávislá.

Příklad 5.38. Chceme zjistit, je-li posloupnost aritmetických vektorů

$$((1, 37, 3, 45, 1)^T, (0, -e, 1, \pi^e, 4)^T, (0, -12, 0, 33, 2)^T)$$



Obrázek 60. Matice A a matice A^T

v prostoru $\mathbb{R}^5$ lineárně závislá nebo nezávislá. Z homogenní soustavy s maticí

$$\begin{pmatrix} 1 & 0 & 0 \\ 37 & -e & -12 \\ 3 & 1 & 0 \\ 45 & \pi^e & 33 \\ 1 & 4 & 2 \end{pmatrix}$$

vybereme první, třetí a pátou rovnici a dostaneme homogenní soustavu s maticí

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

která má zjevně pouze triviální nulové řešení. Proto je původní posloupnost vektorů lineárně nezávislá.

Všimněme si, že k rozhodnutí o lineární nezávislosti původní posloiupnosti nám stačilo vybrat pouze první, třetí a pátou složku těchto vektorů.

Příklad 5.39. Podíváme se znovu na příklad 5.31, 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 5.36 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 5.40. 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 posloupnost řádkových vektorů vzniklé matice, a tedy i původní matice, je lineárně závislá.

Shrneme poznatky o důsledcích řádkových úprav. Řádkové úpravy nemění lineární nezávislost posloupnosti řádkových vektorů ani posloupnosti sloupcových vektorů. Dále nemění sloupcový prostor $\operatorname{Im} A^T$ transponované matice, tj. lineární obal řádků matice A, a jádro $\operatorname{Ker} A$ matice A. Obecně mění lineární obal $\operatorname{Im} A$ sloupců matice A a jádro $\operatorname{Ker} A^T$ transponované matice A.

5.4. **Báze.**

5.4.1. *Definice.* Dostali jsme se ke stěžejnímu pojmu *báze* lineárního prostoru. Jako u lineární nezávislosti množin se budeme zabývat především konečnými bázemi a obecnou definici odložíme na později.

Definice 5.41. Posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ prvků lineárního prostoru $\mathbf{V}$ nad $\mathbf{T}$ se nazývá *báze*, pokud je lineárně nezávislá a $\langle \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n \rangle = \mathbf{V}$.

Druhou podmínku můžeme také vyjádřit tak, že množina $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ generuje prostor $\mathbf{V}$.

Intuitivně, báze je uspořádaná konečná množina prvků $\mathbf{V}$, která je „dost velká“ na to, aby šel každý prvek prostoru $\mathbf{V}$ vyjádřit jako lineární kombinace jejích prvků, a současně „dost malá“, aby takové vyjádření bylo nejvýše jedno.

Formálně, daná posloupnost prvků $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ generuje prostor $\mathbf{V}$ právě tehdy, když lze každý prvek zapsat jako jejich lineární kombinaci alespoň jedním způsobem. Podle tvrzení 5.30 je posloupnost lineárně nezávislá právě tehdy, když lze každý prvek vyjádřit jako lineární kombinaci $\mathbf{v}_1$, $\mathbf{v}_2$, …, $\mathbf{v}_n$ nejvýše jedním způsobem. Dohromady dostáváme následující důležité pozorování.

Pozorování 5.42. *Posloupnost prvků $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ tvoří bázi lineárního prostoru $\mathbf{V}$ právě tehdy, když lze každý prvek $\mathbf{b} \in V$ vyjádřit právě jedním způsobem jako lineární kombinaci prvků $\mathbf{v}_1$, $\mathbf{v}_2$, …, $\mathbf{v}_n$.*

Příklad 5.43. Posloupnost sloupcových vektorů jednotkové matice I_n nad tělesem $\mathbf{T}$, tj. n-tice aritmetických vektorů $((1,0,0,\ldots,0)^T, (0,1,0,\ldots,0)^T, \ldots, (0,0,\ldots,0,1)^T)$, je bází aritmetického vektorového prostoru $\mathbf{T}^n$.

Tato posloupnost je totiž lineárně nezávislá, například podle tvrzení 5.37, a generuje $\mathbf{T}^n$, protože každý vektor $(x_1, \dots, x_n)^T$ jde vyjádřit jako lineární kombinaci

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix} = x_1 \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \cdots + x_n \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} .$$

Obě podmínky (lineární nezávislost i generování) lze nahlédnout najednou z toho, že každý vektor $(x_1, x_2, \dots, x_n)^T \in \mathbf{T}^n$ lze jednoznačně vyjádřit jako právě uvedenou lineární kombinaci

Báze z posledního příkladu jsou význačné báze aritmetických prostorů, proto mají svoje pojmenování a značení.

Definice 5.44. *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 5.45. Posloupnost $((1,1)^T, (3,2)^T)$ je bází prostoru $\mathbb{R}^2$. Můžeme to odůvodnit například tím, že matice

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

je regulární podle charakterizační věty 4.59 (např. podmínka 5). Zobrazení $f_A : \mathbb{R}^2 \to \mathbb{R}^2$ je proto vzájemně jenoznačné, což znamená, že soustava $A\mathbf{x} = \mathbf{b}$ má právě jedno řešení pro každý vektor pravých stran $\mathbf{b}$. 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 5.42 právě tehdy, když posloupnost sloupcových vektorů matice A je báze $\mathbb{R}^2$.

Obecněji lze z věty 4.59 charakterizující 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 5.46.

- 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 5.29. 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 5.25. Posloupnost $((1,2,3)^T,\ (4,5,6)^T)$ je bází $\mathbf{V}$, protože generuje $\mathbf{V}$ (viz opět 5.29) a je lineárně nezávislá, jak se snadno přesvědčíme.

Příklad 5.47. 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 5.27). Vektory tedy napíšeme do řádků a převedeme řádkovými úpravami na odstupňovaný tvar. Nenulové řádky generují stejný prostor a navíc jsou podle tvrzení 5.37 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 5.48. Uvažujme prostor $\mathbf{V}$ nekonečných posloupností $p = (a_1,\ a_2,\ \dots)$ splňujících rovnost $a_n = a_{n-1} + a_{n-2}$ pro každé $n \geq 3$, s běžnými operacemi sčítání a násobení skalárem. Prostor $\mathbf{V}$ je podprostorem $\mathbb{R}^\omega$ mezi jehož prvky patří také Fibonacciho posloupnost, viz příklad 5.21.

Teď nás osvítí záblesk geniality a zkusíme najít v prostoru $\mathbf{V}$ nějakou nenulovou geometrickou posloupnost $(q, q^2, q^3, \dots)$ pro vhodné $q \in \mathbb{R}$. Geometrická posloupnost leží v prostoru $\mathbf{V}$ právě když platí $q^n = q^{n-1} + q^{n-2}$ pro každé $n \geq 3$, což platí právě když

$$q^2 - q - 1 = 0 \ .$$

Tato kvadratická rovnice má kořeny

$$\varphi = \frac{1+\sqrt{5}}{2}, \qquad \text{a} \qquad \frac{1-\sqrt{5}}{2} = 1 - \varphi \ .$$

Našli jsme tedy dvě geometrické posloupnosti v prostoru $\mathbf{V}$ a to

$$p_1 = (\varphi, \varphi^2, \varphi^3, \dots), \quad p_2 = ((1-\varphi), (1-\varphi)^2, (1-\varphi)^3, \dots) \ ,$$

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

Ukážeme, že uspořádaná dvojice posloupností (p_1, p_2) je báze ve $\mathbf{V}$. Použijeme podmínku 3. z tvrzení 5.30. Platí-li pro nějaká dvě čísla $s, t \in \mathbb{R}$ rovnost

$$sp_1 + tp_2 = (0, 0, 0, \dots) \ ,$$

porovnáme první dva prvky v posloupnostech na obou stranách. Musí platit rovnosti

$$s\varphi + t(1-\varphi) = 0$$
$$s\varphi^2 + (1-\varphi)^2 = 0 \ .$$

Čísla s, t jsou tedy řešením homogenní soustavy lineárních rovnic s maticí

$$\begin{pmatrix} \varphi & 1-\varphi \\ \varphi^2 & 1-2\varphi+\varphi^2 \end{pmatrix} \sim \begin{pmatrix} \varphi & 1-\varphi \\ 0 & 1-3\varphi+2\varphi^2 \end{pmatrix} .$$

Protože $1-3\varphi+2\varphi^2 = (1-\varphi)(1-2\varphi) \neq 0 \neq \varphi$, je matice soustavy regulární a jediným řešením soustavy jsou čísla $s = t = 0$. Podle tvrzení 5.30 je posloupnost (p_1, p_2) lineárně nezávislá ve $\mathbf{V}$.

Dokážeme, že také $\langle p_1, p_2\rangle = \mathbf{V}$. Je-li $a = (a_1, a_2, a_3, \dots) \in \mathbf{V}$, pak soustava

$$s\varphi + t(1-\varphi) = a_1$$
$$s\varphi^2 + (1-\varphi)^2 = a_2$$

má regulární matici a tudíž právě jedno řešení $(s, t)^T$. Protože je posloupnost a určená stejně jako každý jiný prvek prostoru $\mathbf{V}$ svými dvěma prvky, musí platit rovnost $sp_1 + tp_2 = a$. Formálně to dokážeme indukcí podle n. Pro tato dvě reálná čísla s, t platí rovnost prvních dvou složek. Indukcí předpokládáme, že pro nějaké $n \geq 2$ platí rovnost $i \leq n-1$ platí $s\varphi^i + t(1-\varphi)^i = a_i$. Potom

$$\begin{aligned} a_n = a_{n-1} + a_{n-2} &= s\varphi^{n-1} + t(1-\varphi)^{n-1} + s\varphi^{n-2} + t(1-\varphi)^{n-2} \\ &= s(\varphi^{n-1} + \varphi^{n-2}) + t((1-\varphi)^{n-1}(1-\varphi)^{n-2}) = s\varphi^n + t(1-\varphi)^n \ , \end{aligned}$$

což dokazuje rovnost $sp_1 + tp_2 = a$ a tedy $a \in \langle p_1, p_2\rangle$.

Pro vyjádření Fibonacciho posloupnosti $a = (1, 1, 2, \dots) \in \mathbf{V}$ jako lineární kombinace posloupností p_1 a p_2 stačí najít koeficienty s, t jako řešení soustavy

$$s\varphi + t(1-\varphi) = 1$$
$$s\varphi^2 + (1-\varphi)^2 = 1 \ .$$

Ta má řešení $t = 1/(1-2\varphi) = -1/\sqrt{5}$ a $s = 1/\sqrt{5}$. Pro n-tý člen Fibonacciho posloupnosti tak dostáváme vyjádření

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

které jsme bez důkazu uvedli už v příkladu 4.3.2.

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 $\mathbb{R}^2$ 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 lineární 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 5.49. Lineární prostor se nazývá *konečně generovaný*, pokud má nějakou konečnou množinu generátorů.

Jedna možnost, jak se můžeme pokusit hledat bázi lineárho prostoru je vzít nějakou posloupnost generátorů a vynechávat prvky z posloupnosti tak dlouho, dokud vzniklé posloupnosti stále generují daný prostor. Pokud již nemůžeme pokračovat, máme minimální posloupnost generátorů. Minimální zde znamená, že vynecháním libovolného prvku vznikne posloupnost, která už prostor negeneruje. Následující tvrzení říká, že v tomto případě již máme bázi.

Tvrzení 5.50. *Minimální posloupnost generátorů* $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$ *lineárního prostoru* $\mathbf{V}$ *je báze* $\mathbf{V}$.

Důkaz. Podle poznámek za definicí 5.28 je posloupnost lineárně závislá právě tehdy, když

$$\langle \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n \rangle = \langle \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{i-1}, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_n \rangle$$

pro nějaké $i \in \{1, 2, \ldots, n\}$. To se ale nestane, protože předpokládáme, že máme minimální posloupnost generátorů. Posloupnost je tedy lineárně nezávislá, takže je to báze. □

Důsledek 5.51. *Z každé konečné množiny generátorů lineárního prostoru lze vybrat bázi.*

Důkaz. Postupně vynecháváme prvky 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 5.52. *Každý konečně generovaný lineární prostor má bázi.*

Příklad 5.53. 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 5.29). 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 5.50, 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 5.54 (Steinitzova věta o výměně)**.** *Nechť $N = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$ je lineárně nezávislá posloupnost prvků lineárního prostoru $\mathbf{V}$ nad $\mathbf{T}$ a nechť $G = (\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_l)$ generuje $\mathbf{V}$. Pak $k \leq l$ a při vhodném uspořádání $G' = (\mathbf{w}'_1, \mathbf{w}'_2, \ldots, \mathbf{w}'_l)$ posloupnosti G platí, že $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k, \mathbf{w}'_{k+1}, \mathbf{w}'_{k+2}, \ldots, \mathbf{w}'_l)$ 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 $G'' = (\mathbf{w}''_1, \mathbf{w}''_2, \ldots, \mathbf{w}''_l)$ takové, že

$$P = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{k-1}, \mathbf{w}''_k, \mathbf{w}''_{k+1}, \ldots, \mathbf{w}''_l)$$

generuje $\mathbf{V}$. Zbývá do P umístit prvek $\mathbf{v}_k$ výměnou za některý z prvků $\mathbf{w}''_k$, $\mathbf{w}''_{k+1}$, ...

Protože P generuje $\mathbf{V}$, prvek $\mathbf{v}_k$ jde napsat jako lineární kombinace prvků 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 prvků $\mathbf{v}_1, \ldots, \mathbf{v}_{k-1}$. To znamená, že platí $k \leq l$ a navíc alespoň jeden z prvků $a_k, a_{k+1}, \ldots, a_l$ 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

$$Z = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k, \mathbf{w}''_{k+1}, \mathbf{w}''_{k+2}, \ldots, \mathbf{w}''_l)$$

generuje $\mathbf{V}$. Prvek $\mathbf{w}''_k$ jde napsat jako lineární kombinace prvků $\mathbf{v}_1$, …, $\mathbf{v}_k$, $\mathbf{w}''_{k+1}$, …, $\mathbf{w}''_l$, což lze nahlédnout z rovnosti výše (z rovnosti vyjádříme $a_k\mathbf{w}''_k$ a vynásobíme a_k^{-1}). Takže lineární obal Z obsahuje prvek $\mathbf{w}''_k$ 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 prvků. To umožňuje dát přesný význam slovu dimenze.

Důsledek 5.55. *Každé dvě báze konečně generovaného lineárního 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 lineárního 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 5.56. *Dimenzí* konečně generovaného lineárního prostoru $\mathbf{V}$ nad $\mathbf{T}$ rozumíme počet prvků jeho libovolné báze. Dimenzi prostoru $\mathbf{V}$ značíme $\dim(V)$.

Příklad 5.57. 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 5.47 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 lineárního prostoru nad $\mathbb{R}$ je 2.

V důsledku 5.51 jsme viděli, že z každé konečné množiny generátorů lze vybrat bázi. Při hledání báze můžeme postupovat i opačně – k lineárně nezávislé množině doplnit další prvky tak, aby vznikla báze. Následující důsledek říká, že to jde, navíc můžeme doplňovat pouze prvky z libovolně zvolené množiny generátorů. Důsledek formulujeme pro konečné množiny, obecněji necháme důkaz do cvičení.

Důsledek 5.58. *Nechť G je konečná množina generátorů lineárního prostoru $\mathbf{V}$. Potom každou lineárně nezávislou posloupnost 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 5.51 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 5.51 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 5.59. *Maximální lineárně nezávislá posloupnost v konečně generovaném prostoru je bází.*

Obecněji, maximální lineárně nezávislá posloupnost prvků konečné množiny generátorů je bází.

Příklad 5.60. V příkladu 5.47 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 5.51 plyne, že to jde. Předchozí důsledek 5.58 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 $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_5\}$ (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 5.61. *V každém lineárním prostoru $\mathbf{V}$ dimenze n platí:*

(1) *Každá množina generátorů $\mathbf{V}$ obsahuje alespoň n prvků.*
(2) *Každá n-prvková posloupnost generátorů je bází $\mathbf{V}$.*
(3) *Každá lineárně nezávislá posloupnost ve $\mathbf{V}$ obsahuje nejvýše n prvků.*
(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 prvků. Z toho plynou první dva body.

Každou lineárně nezávislou množinu lze doplnit na n-prvkovou bázi. Z toho plynou zbylé dva body. □

Příklad 5.62. V příkladu 5.33 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 5.63. *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 prvek $\mathbf{w}_1 \in W$. Protože $\{\mathbf{w}_1\}$ negeneruje W_2, existuje prvek $\mathbf{w}_2 \in W$ takový, že $\mathbf{w}_2 \notin \langle \mathbf{w}_1 \rangle$, atd.: Indukcí najdeme pro libovolné i prvek $\mathbf{w}_i \in W$, který neleží v lineárním obalu předchozích prvků $\mathbf{w}_1, \ldots, \mathbf{w}_{i-1}$. Podle poznámky za tvrzením 5.30 (cvičení **??**) je pro každé i posloupnost $(\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_i)$ 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 5.52. 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 $\mathbf{V}$ podle (4), z čehož vyplývá, že $V = W$. (Naopak z $V = W$ triviálně plyne $\dim(V) = \dim(W)$.) □

Příklad 5.64. 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 5.42, které říká, že máme-li bázi $B = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ prostoru $\mathbf{V}$, pak každý prvek $\mathbf{v}$ ve $\mathbf{V}$ lze jednoznačným způsobem vyjádřit jako lineární kombinaci prvků $\mathbf{v}_1, \ldots, \mathbf{v}_n$. Koeficientům této lineární kombinace říkáme souřadnice $\mathbf{v}$ vzhledem k B.

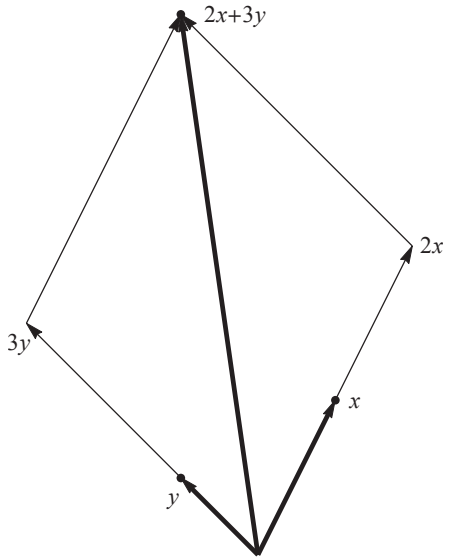
Definice 5.65. Nechť $B = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ je báze lineárního prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$ a $\mathbf{w} \in \mathbf{V}$. *Souřadnicemi* (též *vyjádřením*) *prvku* $\mathbf{w}$ *vzhledem k* B rozumíme (jednoznačně určený) aritmetický vektor $(a_1, a_2, \ldots, a_n)^T \in \mathbf{T}^n$ 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.

$$[\mathbf{w}]_B = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} .$$

Příklad 5.66. Lineární kombinace prvků $\mathbf{u}, \mathbf{v}$ prostoru $\mathbf{V}$ nad $\mathbf{R}$ s koeficienty 2, 3, tj. prvek $2\mathbf{u} + 3\mathbf{v}$, je vlastně „prvek o souřadnicích $(2, 3)$ vzhledem k soustavě souřadnic $\mathbf{u}, \mathbf{v}$“.



Obrázek 61. Lineární kombinace $2\mathbf{x} + 3\mathbf{y}$ (k příkladu 5.66)

Souřadnice závisí na pořadí prvků v bázi. Z tohoto důvodu jsme bázi definovali jako posloupnost prvků lineárního prostoru, nikoliv množinu.

Zvolíme-li v prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$ dimenze n bázi B, pak předchozí definice jednoznačně přiřazuje každému prvku $\mathbf{v} \in V$ 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) prvek $\mathbf{v} \in V$. Zobrazení přiřazující $[\mathbf{v}]_B$ prvku $\mathbf{v}$ je tedy bijekcí mezi V a T^n.

Příklad 5.67. V příkladu 5.43 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 5.46. 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. Souřadnicemi polynomu $a+bx+cx^2$ vzhledem k této bázi je aritmetický vektor

$$[a + bx + cx^2]_B = (b, c, a)^T \ .$$

Příklad 5.68. 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 5.45. 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 prvky lineárního prostoru a jejich souřadnicemi ve zvolené bázi je ještě těsnější, zachovává totiž operace lineárního prostoru. Konkrétně, souřadnice součtu prvků ve $\mathbf{V}$ (vzhledem k B) jsou rovny součtu jejich souřadnic (vzhledem k B) v prostoru $\mathbf{T}^n$. Podobně pro násobení skalárem.

Tvrzení 5.69. *Nechť $B = (\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$ je báze lineární 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 5.70. 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 lineární prostory jsou v podstatě $\mathbf{T}^n$“. Zvolíme-li v prostoru bázi B, můžeme místo původních prvků 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 za okamžik.

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 5.71. *Nechť B je báze lineárního 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 $\mathbf{T}^n$.*

5.4.4. *Přechod mezi bázemi.* Často je potřeba umět rychle přecházet mezi bázemi, tj. počítat souřadnice nějakého prvku vzhledem k jedné bázi, známe-li jeho souřadnice vzhledem k jiné bázi.

Tento přechod je možné popsat maticí. Rozmyslíme si nejprve jednoduchý případ aritmetického vektorového prostoru $\mathbf{T}^3$ s bází $B = (\mathbf{v}_1,\mathbf{v}_2,\mathbf{v}_3)$. Najdeme vzoreček jak najít vektor $\mathbf{x} = (x_1,x_2,x_3)^T$, známe-li jeho vyjádření $[\mathbf{x}]_B = (y_1,y_2,y_3)^T$ vzhledem k bázi B. Podle definice je

$$\mathbf{x} = y_1\mathbf{v}_1 + y_2\mathbf{v}_2 + y_3\mathbf{v}_3 \ ,$$

což můžeme maticově zapsat

$$\mathbf{x} = (\mathbf{v}_1|\mathbf{v}_2|\mathbf{v}_3)[\mathbf{x}]_B \ .$$

Vektor $\mathbf{x}$ je roven svému vyjádření vzhledem ke kanonické bázi $K = (\mathbf{e}_1,\mathbf{e}_2,\mathbf{e}_3)$. Matice $(\mathbf{v}_1|\mathbf{v}_2|\mathbf{v}_3)$ se nazývá matice přechodu od B ke K a značí se $[\mathrm{id}]_K^B$. Umožňuje nám “přecházet” od báze B k bázi K pomocí vzorce

$$[\mathbf{x}]_K = [\mathrm{id}]_K^B[\mathbf{x}]_B \ .$$

Podobnou formulku můžeme nalézt pro přechod mezi libovolnými dvěma bázemi libovolného konečně generovaného lineárního prostoru.

Definice 5.72. Nechť $B = (\mathbf{v}_1,\dots,\mathbf{v}_n)$ a C jsou báze lineárního prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$. *Maticí přechodu od báze B k bázi C* rozumíme matici

$$[\mathrm{id}]_C^B = ([\mathbf{v}_1]_C|[\mathbf{v}_2]_C|\dots|[\mathbf{v}_n]_C) \ .$$

Slovy, matice přechodu od B k C má ve sloupcích vyjádření prvků báze B vzhledem k bázi C.

Tvrzení 5.73. *Nechť* $\mathbf{V}$ *je lineární prostor* $\mathbf{V}$ *nad tělesem* $\mathbf{T}$ *dimenze* n *a* B, C *jsou báze* $\mathbf{V}$*. Pak pro libovolný prvek* $\mathbf{x} \in \mathbf{V}$ *platí*

$$[\mathbf{x}]_C = [\mathrm{id}]_C^B [\mathbf{x}]_B \ .$$

Navíc je matice $[\mathrm{id}]_C^B$ *tímto vztahem určena jednoznačně.*

Důkaz. Označme $B = (\mathbf{v}_1, \dots, \mathbf{v}_n)$.

Vezmeme libovolný prvek $\mathbf{x} \in \mathbf{V}$ a označme $[\mathbf{x}]_B = (a_1, \dots, a_n)$, tj. podle definice $\mathbf{x} = a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n$. Podle tvrzení 5.69 platí

$$\begin{aligned}[\mathbf{x}]_C &= [a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n]_C = [a_1\mathbf{v}_1]_C + \cdots + [a_n\mathbf{v}_n]_C \\ &= a_1[\mathbf{v}_1]_C + \cdots + a_n[\mathbf{v}_n] = ([\mathbf{v}_1]_C | \dots | [\mathbf{v}_n]_C)(a_1, \dots, a_n)^T \\ &= [\mathrm{id}]_C^B [\mathbf{x}]_B \ .\end{aligned}$$

K důkazu jednoznačnosti uvažujme matici A, která splňuje pro libovolný prvek $\mathbf{x} \in \mathbf{V}$ vztah

$$[\mathbf{x}]_C = A[\mathbf{x}]_B \ .$$

Dosazením $\mathbf{x} = \mathbf{v}_i$ dostaneme

$$[\mathbf{v}_i]_C = A[\mathbf{v}_i]_B = A\mathbf{e}_i \ ,$$

takže i-tý sloupec matice A je roven $[\mathbf{v}_i]_C$ a tím pádem $A = [\mathrm{id}]_C^B$. □

Příklad 5.74. Matice přechodu od báze $B = ((1,2)^T, (5,6)^T)$ ke kanonické bázi K prostoru $\mathbb{R}^2$ je

$$[\mathrm{id}]_K^B = \begin{pmatrix} 1 & 5 \\ 2 & 6 \end{pmatrix} \ .$$

Pro libovolný prvek $\mathbf{x} \in \mathbb{R}^2$ platí

$$\mathbf{x} = [\mathbf{x}]_K = \begin{pmatrix} 1 & 5 \\ 2 & 6 \end{pmatrix} [\mathbf{x}]_B \ .$$

Pokud chceme naopak vyjadřovat vzhledem k bázi B, známe-li vyjádření vzhledem ke kanonické bázi, upravíme tento vztah na

$$[\mathbf{x}]_B = \begin{pmatrix} 1 & 5 \\ 2 & 6 \end{pmatrix}^{-1} \mathbf{x} = \frac{1}{4} \begin{pmatrix} -6 & 5 \\ 2 & -1 \end{pmatrix} \mathbf{x} \ .$$

(Využili jsme toho, že $[\mathrm{id}]_K^B$ je regulární matice. Obecně, každá matice přechodu je regulární a platí $[\mathrm{id}]_B^C = ([\mathrm{id}]_C^B)^{-1}$. Dokažte!)

Příklad 5.75. Najdeme matici přechodu od báze B k bázi C prostoru $\mathbf{V} \leq \mathbb{R}^3$, kde

$$\mathbf{V} = \left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right\rangle, \ B = \left(\begin{pmatrix} 2 \\ 4 \\ 4 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix} \right), \ C = \left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right) \ .$$

(Ověřte, že B a C jsou skutečně báze prostoru $\mathbf{V}$!) Potřebujeme najít vyjádření vektorů báze B vzhledem k bázi C. To vede na dvě soustavy rovnic se stejnou

maticí, které vyřešíme současně.

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

Vychází $[(2,4,4)^T]_C = (-2,4)^T$ a $[(1,-1,-1)^T]_C = (2,-1)^T$, takže matice přechodu od B k C je

$$[\mathrm{id}]_C^B = \begin{pmatrix} -2 & 2 \\ 4 & -1 \end{pmatrix} .$$

5.5. **Dimenze podprostorů určených maticí, soustavy rovnic potřetí.**

K matici A nad tělesem $\mathbf{T}$ typu $m \times n$ máme přiřazeny řádkový a sloupcový prostor $\mathrm{Im}\, A^T \leq \mathbf{T}^n$ a $\mathrm{Im}\, A \leq T^m$. Ukážeme, že mají stejnou dimenzi. Dále dáme do souvislosti dimenzi prostoru $\mathrm{Ker}\, A \leq \mathbf{T}^n$ a $\mathrm{Im}\, A$, 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 5.80). Výsledek samozřejmě formulujeme v jazyku matic.

Definice 5.76. Nechť $A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ je matice nad $\mathbf{T}$. Říkáme, že i-tý sloupec matice A je *bázový*, pokud není lineární kombinací předchozích sloupců, tj. pokud platí

$$\mathbf{a}_i \notin \langle \mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{i-1} \rangle \ .$$

Pojmenování ospravedlňuje skutečnost, že bázové sloupce tvoří bázi sloupcového prostoru matice. To si rozmyslete jako cvičení.

Pozorování 5.77. *Pro libovolnou matici A tvoří bázové sloupce bázi sloupcového prostoru. Speciálně, dimenze* $\mathrm{Im}\, A$ *je rovna počtu bázových sloupců.*

Příklad 5.78. V matici

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

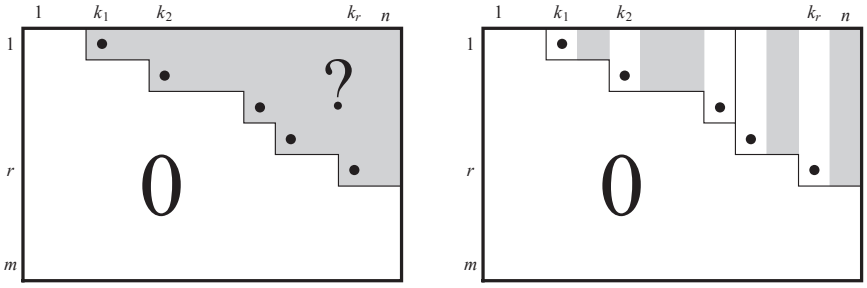
je bázový druhý a čtvrtý sloupec. První, třetí ani pátý sloupec není bázový. Je to vidět u prvního a třetího sloupce, pátý je součtem druhého a čtvrtého, takže také není bázový.

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 5.79. *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 2.12 odstupňovaného tvaru.*

Důkaz. Označme $A = (\mathbf{a}_1|\ldots|\mathbf{a}_n)$. Pro $j = 1, 2, \ldots, n$ označme W_j lineární obal prvních j sloupců, tj. $W_j = \langle \mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_j \rangle$. Dále nechť $\mathbf{V}_j$ je následující podprostor $\mathbf{T}^m$:

$$V_j = \{(x_1, x_2, \ldots, x_j, 0, 0, \ldots, 0) : x_1, x_2, \ldots, x_j \in T\} \ .$$



Obrázek 62. Matice po Gussově eliminaci a následné zpětné substituci

Pro libovolné i je W_{k_i-1} podprostorem prostoru $\mathbf{V}_{i-1}$. Sloupec $\mathbf{a}_{k_i}$ 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 $(\mathbf{a}_{k_1}, \mathbf{a}_{k_2}, \dots, \mathbf{a}_{k_i})$ je lineárně nezávislá posloupnost (žádný z vektorů v posloupnosti není lineární kombinací předchozích, takže posloupnost je lineárně nezávislá podle tvrzení 5.30), 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 5.63.

Nyní již důkaz dokončíme snadno. Sloupce $\mathbf{a}_1, \dots, \mathbf{a}_{k_1-1}$ jsou celé nulové, takže nejsou bázové. Sloupce $\mathbf{a}_{k_1+1}, \mathbf{a}_{k_1+2}, \dots, \mathbf{a}_{k_2-1}$ nejsou bázové, protože patří do V_2, tedy i do W_{k_1}, atd. □

Tvrzení 5.80. *Nechť A je matice nad tělesem $\mathbf{T}$ typu $m \times n$ a R je regulární matice řádu m. Pak pro libovolné $i \in \{1, 2, \dots, n\}$ 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 5.63). Obšírněji, i-tý sloupec matice A je bázový právě tehdy, když není lineární kombinací předchozích sloupců, tj. právě tehdy, když $A(a_1, \dots, a_{i-1}, 1, 0, 0, \dots, 0)^T = \mathbf{o}$ pro nějaké prvky $a_1, \dots, a_{i-1} \in T$. To nastane právě tehdy, když $RA(a_1, \dots, a_{i-1}, 1, 0, 0, \dots, 0)^T = \mathbf{o}$. (Připomeňme, že implikaci zprava doleva v této ekvivalenci lze dokázat například vynásobením zleva maticí R^{-1}.) □

Příklad 5.81. 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 5.82. *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 A 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 5.77), tyto dimenze jsou stejné (viz tvrzení 5.80) a rovnají se počtu nenulových řádků matice RA (viz tvrzení 5.79).

Dimenze řádkového prostoru matice RA je také rovna počtu nenulových řádků, protože nenulové řádky tvoří lineárně nezávislou posloupnost (viz tvrzení 5.37), která zřejmě generuje řádkový prostor. Ale násobení regulární maticí zleva nemění lineární obal řádků (viz tvrzení 5.26), speciálně, dimenze řádkového prostoru matice RA je stejná jako dimenze řádkového prostoru matice A. □

Definice 5.83. *Hodností* matice A rozumíme dimenzi řádkového (sloupcového) prostoru matice A. Značíme $\operatorname{rank}(A)$.

Shrneme některé důležité triviální důsledky do pozorování.

Pozorování 5.84. *Pro libovolnou matici A typu $m\times n$ platí* $\operatorname{rank}(A) = \operatorname{rank}(A^T) \leq m, n$. *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 5.85. 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 5.86. *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 **??** 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 5.63 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 5.87. *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 4.59. 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 5.63 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 5.88. *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 5.61.

Příklad 5.89. 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 5.86 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. *Skeletní rozklad, Gaussova-Jordanova eliminace.* Uvažujme matici A typu $m \times n$ hodnosti r nad tělesem $\mathbf{T}$. Napíšeme nějakou bázi $\operatorname{Im} A$ do sloupců matice B. Každý sloupec $\mathbf{a}_i$ matice A je lineární kombinací sloupců matice B, takže platí $\mathbf{a}_i = B\mathbf{c}_i$ pro nějaký vektor $\mathbf{c}_i \in \mathbf{T}^r$. Označíme-li tedy $C = (\mathbf{c}_1 | \ldots | \mathbf{c}_n)$, máme rozklad $A = BC$, kde B je typu $m \times r$ a C je typu $r \times n$. Takovému rozkladu říkáme *skeletní rozklad*.

Rozklad se hodí pro ukládání matic nízkých hodností a počítání s nimi. Je-li například A čtvercová matice řádu 1000 hodnosti 100, pak na uložení matice A potřebujeme 10^6 skalárů, kdežto na uložení matic B, C pouze $2 \cdot 10^5$ skalárů. Na výpočet součinu $A\mathbf{x}$ pro nějaký vektor $\mathbf{x} \in \mathbf{T}^{1000}$ přímočarým způsobem potřebujeme 10^6 násobení, na výpočet postupem $B(C(\mathbf{x}))$ opět pouze $2 \cdot 10^5$ násobení.

Za sloupce matice B můžeme vzít bázové sloupce matice A. Ve tvrzení 5.91 ukážeme, že v tomto případě je matice C tzv. redukovaný odstupňovaný tvar matice A.

Definice 5.90. Matice je v *redukovaném (řádkově) odstupňovaném tvaru*, pokud je v řádkově odstupňovaném tvaru a každý bázový sloupec má jedinou nenulovou složku rovnou 1.

Každou matici A lze převést do redukovaného odstupňovaného tvaru takto:

(1) Matici Gaussovo eliminací převedeme do odstupňovaného tvaru.
(2) Vynásobíme nenulové řádky tak, aby byl každý pivot roven 1.
(3) Postupně vynulujeme zbylé prvky v každém bázovém sloupci.

Tomuto procesu se říká Gaussova-Jordanova eliminace. Vzniklé matici říkáme *redukovaný odstupňovaný tvar* matice A. (Jako cvičení dokažte, že tento tvar je dokonce maticí určen jednoznačně, tj. pro každou matici A existuje právě jedna matice J

v redukovaném odstupňovaném tvaru taková, že J lze získat z A elementárními řádkovými úpravami.)

Přejdeme ke slíbenému tvrzení o skeletním rozkladu.

Tvrzení 5.91. *Libovolná matice A typu $m \times n$ nad $\mathbf{T}$ s hodností r je rovná součinu $A = BC$, kde B je matice typu $m \times r$ tvořená bázovými sloupci matice A (v pořadí v jakém se vyskytují v A) a C je matice typu $r \times n$ tvořená nenulovými řádky v redukovaném odstupňovaném tvaru D matice A.*

Důkaz. Označme $k_1, \dots, k_r$ indexy bázových sloupců matice $A = (\mathbf{a}_1 | \dots | \mathbf{a}_n)$. Matice $D = (\mathbf{d}_1 | \dots | \mathbf{d}_n)$ vznikla z A posloupností řádkových elementárních úprav, takže $D = RA$ pro nějakou regulární matici R řádu m. Matice C je v odstupňovaném tvaru, čísla $k_1, \dots, k_r$ se shodují s definicí 2.12, $B = (\mathbf{a}_{k_1} | \dots | \mathbf{a}_{k_r})$ a navíc platí $\mathbf{d}_{k_i} = \mathbf{e}_i$ pro každé $1 \leq i \leq r$, tedy také $\mathbf{c}_{k_i} = \mathbf{e}_i$ (v tomto výrazu má $\mathbf{e}_i$ jiný počet složek než v přechozím).

Dokážeme, že matice A a BC mají stejné sloupce s pořadovým číslem j. Triviálně to je splněné pro $j < k_1$ (na obou stranách jsou nulové sloupce). Jinak označme i největší takové číslo, že $j \geq k_i$. Sloupec j matice A je lineární kombinací bázových sloupců $\mathbf{a}_{k_1}, \dots, \mathbf{a}_{k_i}$, tedy pro nějaké prvky $t_1, \dots, t_i \in T$ platí

$$\mathbf{a}_j = t_1 \mathbf{a}_{k_1} + t_2 \mathbf{a}_{k_2} + \dots + t_i \mathbf{a}_{k_i} \ .$$

Vynásobením maticí R zleva a úpravou užitím $D = RA$ získáme

$$\mathbf{d}_j = R\mathbf{a}_j = t_1 R\mathbf{a}_{k_1} + \dots + t_i R\mathbf{a}_{k_i} = t_1 \mathbf{d}_{k_1} + \dots + t_i \mathbf{d}_{k_i} = t_1 \mathbf{e}_1 + \dots + t_i \mathbf{e}_i = (t_1, \dots, t_i, 0, \dots, 0)^T \ ,$$

tím pádem také

$$\mathbf{c}_j = (t_1, \dots, t_i, 0, \dots, 0)^T \ ,$$

kde vektor má tentokrát r složek. Sloupec j matice BC je proto

$$B\mathbf{c}_j = B(t_1, \dots, t_i, 0, \dots, 0) = t_1 \mathbf{a}_{k_1} + \dots + t_i \mathbf{a}_{k_i} = \mathbf{a}_j \ .$$

□

5.5.4. *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 2.17), přesto některé důkazy stručně zopakujeme, aby vynikla elegance a užitečnost pojmů zavedených v této kapitole. (Navíc věta 2.17 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 5.92 (Frobeniova věta)**.** *Soustava $A\mathbf{x} = \mathbf{b}$ má řešení právě tehdy, když* $\operatorname{rank}(A) = \operatorname{rank}(A \,|\, \mathbf{b})$.

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 5.63). □

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 5.93. *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 2.17).

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 2.17). □

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 $\mathbf{x} = (x_1, \ldots, x_n) \in \operatorname{Ker} A$ (neboli každé řešení homogenní soustavy $A\mathbf{x} = \mathbf{o}$) je jednoznačně určen vektorem $(x_{j_1}, x_{j_2}, \ldots, x_{j_{n-r}}) \in T^{n-r}$ (a naopak, libovolný vektor v T^{n-r} určuje jedno řešení). Toto jsme nahlédli v pozorování 2.16 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 2.17 jsme použili kanonickou bázi) a dopočítáním zbylých složek (prakticky provedeme z odstupňovaného tvaru; ve větě 2.17 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 5.94 (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 5.95. Vrátíme se k soustavě z části 2.3.5.

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

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 $5 - 2 = 3$. Partikulární řešení získáme dopočítáním z libovolné volby volných proměnných. V 2.3.5 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 2.3.5 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 5.96. *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 5.11). 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 5.97. 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 5.98 (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 5.63). 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 5.52). 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 5.58). Podobně doplníme B na bázi $D = (\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k, \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m)$ 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 $c_1, \ c_2, \ \ldots, \ c_m$ 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 5.99. 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 5.100. 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 5.63 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 5.101. 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 5.102. *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 $\mathbf{V}_1, \mathbf{V}_2, \ldots, \mathbf{V}_k$, 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 5.28 a 5.41)**.** 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 $I = \{1, 2, \dots, n\}$.

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 $\mathbf{e}_i = (0, 0, \dots, 1, 0, 0, \dots)$ 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 5.30 charakterizující lineární nezávislost.
- Pozorování 5.42, 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 5.69 o souřadnicích a operacích i obdoba pozorování 5.71 o zachovávání důležitých vlastností jako lineární nezávislost platí.
- Minimální soubor generátorů je vždy báze (obdoba tvrzení 5.50). Obdoba důsledku 5.51, 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 5.52). Poznamenejme, že důkaz vyžaduje axiom výběru.
- Všechny báze mají stejnou mohutnost (obdoba důsledku 5.55), takže má smysl zavést dimenzi jako mohutnost libovolné báze. Rovněž platí obdoba důsledku 5.58, že libovolný lineárně nezávislý soubor lze doplnit do báze vektory z libovolné množiny generátorů. Z toho plyne obdoba důsledku 5.59, že maximální lineárně nezávislý soubor je báze.
- Obdoba tvrzení 5.63 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 $0, 1, \dots, 9$ 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 nějakě 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 5.103. *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, není 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 5.104. 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 5.105. 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 5.106.

- 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 5.107. *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 $a_1 a_2 \cdots a_{n-1}$, existuje právě jedno $a_n \in \{0, 1\}$ takové, že slovo $\mathbf{a} = a_1 a_2 \cdots a_{n-1} a_n \in S$. 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 $a_1 a_2 \cdots a_{n-1}$. 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 5.108. 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 5.109. *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 5.110. 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 5.111. 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 5.112. *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 $A = (\mathbf{a}_1|\dots|\mathbf{a}_n)$ 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

$$x_1\mathbf{a}_1 + x_2\mathbf{a}_2 + \cdots x_n\mathbf{a}_n = \mathbf{o}^T.$$

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

$$x_{j_1}\mathbf{a}_{j_1} + x_{j_2}\mathbf{a}_{j_2} + \cdots x_{j_l}\mathbf{a}_{j_l} = \mathbf{o}^T,$$

l-prvková podposloupnost sloupcových vektorů $\mathbf{a}_{j_1}, \dots, \mathbf{a}_{j_l}$ je tedy lineárně závislá.

Jestliže naopak existuje lineárně závislá podposloupnost $\mathbf{a}_{i_1}, \mathbf{a}_{i_2}, \dots, \mathbf{a}_{i_m}$ sloupcových vektorů matice A, existují prvky $x_{i_j} \in \mathbb{Z}_2$, ne všechny nulové, takové, že

$$x_{i_1}\mathbf{a}_{i_1} + x_{i_2}\mathbf{a}_{i_2} + \cdots + x_{i_m}\mathbf{a}_{i_m} = \mathbf{o}^T.$$

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 5.109 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 5.113. Kontrolní matice A kódu C z Příkladu 5.110 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 5.114. 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 5.115. *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 5.116. 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 5.117. 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 $\mathbf{y} = y_1y_2 \cdots y_7$ je ten poškozený. Označme $A\mathbf{y}^T = (s_1s_2s_3)^T$.

Protože matice A obsahuje všechny nenulové vektory $\mathbb{Z}_2^3$ jako sloupce, existuje jednoznačně určený sloupec $\mathbf{a}_j = (s_1s_2s_3)^T$. Platí $\mathbf{a}_j = A\mathbf{e}_j^T$ 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

$$A(\mathbf{y}^T + \mathbf{e}_j^T) = A\mathbf{y}^T + A\mathbf{e}_j^T = (s_1s_2s_3)^T + \mathbf{a}_j = (s_1s_2s_3)^T + (s_1s_2s_3)^T = \mathbf{o}^T.$$

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 5.118. 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 5.119. *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 5.120. *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. Množina všech podmnožin množiny $\{1,2,3,\dots,n\}$ (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“ $\mathbb{Z}_2^n$.

5. Dokažte tvrzení 5.9 a formulujte a dokažte obdoby vlastností (8) a (9) z tvrzení 3.3.

6. Dokažte, že $\mathbf{T}$ jako vektorový prostor nad $\mathbf{T}$ má pouze triviální podprostory.

7. Dokažte, že jedinými netriviálními podprostory prostoru $\mathbf{T}^2$ jsou množinu tvaru $\{t\mathbf{x} : t \in T\}$, kde $\mathbf{o} \neq \mathbf{x} \in \mathbf{T}^2$.

8. 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 $\mathbf{b} = \mathbf{o}$.

9. Zjistěte lineární obal množiny X z příkladu 5.21 a dokažte, že množina Y tvoří podprostor.

10. Dokažte, že posloupnost vektorů $(\mathbf{v}_1, \dots, \mathbf{v}_k)$ 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 $\mathbf{v}_i \notin \langle \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_{i-1} \rangle$).

11. Dokažte, že sloupce matice v řádkově odstupňovaném tvaru jsou lineárně nezávislé právě tehdy, když příslušná homogenní soustava nemá žádné volné proměnné.

12. Dokončete příklad 5.48 o Fibonacciho posloupnostech.

13. Dokažte, že sloupce (řádky) čtvercové matice A nad $\mathbf{T}$ řádu n tvoří bázi $\mathbf{T}^n$ právě tehdy, když A je regulární.

14. 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.

15. 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 $a_1 = 3$, $a_2 = 7$.

16. Dokažte, že z každé množiny generátorů konečně generovaného prostoru lze vybrat bázi.

17. Dokažte, že důsledek 5.58 platí bez předpokladu konečnosti G. Předpoklad tedy změníme na „G je množina generátorů konečně generovaného prostoru $\mathbf{V}$“.

18. Spočítejte počet všech různých bází $\mathbf{V}$ vybraných z vektorů $\mathbf{v}_1, \dots, \mathbf{v}_5$ z příkladu 5.60.

19. Dokažte druhou část tvrzení 5.69.

20. Dokažte, že bázové sloupce tvoří bázi sloupcového prostoru matice.

21. 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 $(x_1, x_2, \dots, x_n)$.

22. Jednoznacnost redukovaneho tvaru

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 5.120.

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

$$2^r(\binom{n}{0} + \binom{n}{1} + \cdots \binom{n}{d}) \leq 2^n.$$

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 $\{1, 2, \ldots, 7\}$ 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.

Shrnutí páté kapitoly

(1) Je-li $\mathbf{T}$ těleso, pak *lineárním 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 prvků množiny V prvky tělesa $\mathbf{T}$ (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 $a\cdot(\mathbf{u}+\mathbf{v})=a\cdot\mathbf{u}+a\cdot\mathbf{v}$.

(2) Pro libovolné těleso $\mathbf{T}$ a přirozené číslo n *aritmetický vektorový prostor dimenze* n *nad* $\mathbf{T}$ je množina všech n-složkových aritmetických (sloupcových) vektorů T^n spolu s přirozenými operacemi $+$ a $\cdot$ (definovanými jako v definici 2.3), označujeme jej $\mathbf{T}^n$.

(3) Další příklady lineárních prostorů: prostory polynomů s reálnými koeficienty, prostor $\mathbf{T}^{m\times n}$ matic typu $m\times n$ nad tělesem $\mathbf{T}$, prostor $\mathbb{R}^\infty$ všech posloupností reálných čísel, prostor $R^{(\infty)}$ posloupností reálných čísel s konečně mnoha nenulovými prvky, prostor všech konvergentních posloupností reálných čísel, prostor všech posloupností reálných čísel konvergujících k 0, prostory reálných funkcí reálné proměnné, atd. Všechny s přirozenými operacemi sčítání a násobení skalárem.

(4) V každém lineárním prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$ platí
   (a) nulový prvek $\mathbf{o}$ je určený jednoznačně,
   (b) rovnice $\mathbf{u}+\mathbf{x}=\mathbf{v}$ má pro pevná $\mathbf{u},\mathbf{v}\in V$ právě jedno řešení, speciálně, opačný prvek $-\mathbf{v}$ je vektorem $\mathbf{v}$ určen jednoznačně,
   (c) $0\mathbf{v}=\mathbf{o}$ pro libovolný prvek $\mathbf{v}\in V$,
   (d) $a\mathbf{o}=\mathbf{o}$ pro libovolný skalár $a\in T$,
   (e) je-li $a\mathbf{v}=\mathbf{o}$, pak buď $a=0$ nebo $\mathbf{v}=\mathbf{o}$,
   (f) $-\mathbf{v}=(-1)\mathbf{v}$ pro libovolný prvek $\mathbf{v}\in V$, speciálně $-(-\mathbf{v})=\mathbf{v}$.

(5) Je-li $\mathbf{V}$ lineární prostor nad $\mathbf{T}$, pak lineární prostor $\mathbf{U}$ nad tělesem $\mathbf{T}$ 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 $\mathbf{U}\le\mathbf{V}$.

(6) Je-li $\mathbf{V}$ vektorový prostor nad tělesem $\mathbf{T}$, pak neprázdná podmnožina U množiny V je podprostorem $\mathbf{V}$ právě tehdy, když současně
   - („uzavřenost na sčítání“) pro libovolné $\mathbf{u},\mathbf{v}\in U$ platí $\mathbf{u}+\mathbf{v}\in U$,
   - („uzavřenost na násobení skalárem“) pro libovolné $\mathbf{v}\in U$ a $a\in T$ platí $a\mathbf{v}\in U$.

(7) Geometrický význam podprostorů $\mathbb{R}^2$ a $\mathbb{R}^3$.

(8) Pro libovolnou matici A typu $m\times n$ nad $\mathbf{T}$ platí, že $\operatorname{Ker}A$ je podprostor $\mathbf{T}^n$, neboli $\operatorname{Ker}A\le\mathbf{T}^n$.

(9) Jsou-li $\mathbf{v}_1,\mathbf{v}_2,\dots,\mathbf{v}_k$ prvky lineárního prostoru $\mathbf{V}$ nad $\mathbf{T}$ a $t_1,t_2,\dots,t_k\in\mathbf{T}$ skaláry, tj. prvky tělesa $\mathbf{T}$, pak prvek

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

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

Lineární kombinaci prázdného systému vektorů definujeme jako nulový vektor.

(10) Nechť $\mathbf{V}$ je lineární 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

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

(11) Pro libovolný lineární prostor $\mathbf{V}$ nad $\mathbf{T}$ a libovolnou $X \subseteq V$ je $\langle X \rangle$ podprostorem $\mathbf{V}$.

(12) Je-li $\mathbf{V}$ lineární prostor nad $\mathbf{T}$ a $X \subseteq U \leq \mathbf{V}$, pak $\langle X \rangle \subseteq \mathbf{U}$. Lineární obal $\langle X \rangle$ je proto nejmenší podprostor $\mathbf{V}$ obsahující množinu X.

(13) Jsou-li X, Y dvě podmnožiny lineárního prostoru $\mathbf{V}$ nad $\mathbf{T}$, pak platí

$$\langle X \rangle \subseteq \langle Y \rangle \quad \text{právě když pro každé } \ x \in X \ \text{ platí } \ x \in \langle Y \rangle \ .$$

(14) Je-li $\mathbf{V}$ lineární prostor nad $\mathbf{T}$ a $X \subseteq V$. Pokud $\langle X \rangle = V$, pak říkáme, že X je *množina generátorů prostoru* $\mathbf{V}$, nebo také že X *generuje* $\mathbf{V}$.

(15) Je-li $(\mathbf{v}_1, \ldots, \mathbf{v}_l)$ konečná posloupnost prvků lineárního prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$, pak

$$\langle \mathbf{v}_1, \ldots, \mathbf{v}_l \rangle = \{t_1\mathbf{v}_1 + \cdots + t_l\mathbf{v}_l : t_1, \ldots, t_l \in T\} \ .$$

(16) Je-li A matice typu $m \times n$ nad $\mathbf{T}$, pak *sloupcovým prostorem matice* A rozumíme podprostor $\mathbf{T}^m$ generovaný množinou sloupcových vektorů matice A a značíme jej $\operatorname{Im} A$.

$$\operatorname{Im} A = \langle \mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n \rangle \leq \mathbf{T}^m$$

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

$$\operatorname{Im} A^T = \langle \tilde{\mathbf{a}}_1, \tilde{\mathbf{a}}_2, \ldots, \tilde{\mathbf{a}}_m \rangle \leq \mathbf{T}^n$$

(17) Nechť $A = (\mathbf{a}_1 | \ldots | \mathbf{a}_n)$ je matice typu $m \times n$ nad $\mathbf{T}$ a R je regulární matice řádu m. Pak

$$\operatorname{Im}(RA) = \langle R\mathbf{a}_1, \ldots, R\mathbf{a}_n \rangle\,,\ \operatorname{Ker} A = \operatorname{Ker}(RA),\ \operatorname{Im} A^T = \operatorname{Im}(RA)^T.$$

(18) Elementární řádkové úpravy nemění $\operatorname{Ker} A$ a $\operatorname{Im} A^T$. Elementární sloupcové úpravy nemění $\operatorname{Ker} A^T$ a $\operatorname{Im} A$.

(19) Nechť $\mathbf{V}$ je lineární prostor nad tělesem $\mathbf{T}$. Posloupnost prvků $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$ prostoru $\mathbf{V}$ se nazývá *lineárně závislá*, pokud některý z prvků $\mathbf{v}_i$ je lineární kombinací zbývajících prvků $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{i-1}, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_k$.

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

(20) Nechť $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ je posloupnost prvků lineárního prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$. Následující tvrzení jsou ekvivalentní.

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

(b) Žádný z prvků $\mathbf{v}_i$ $(1 \leq i \leq k)$ nelze vyjádřit jako lineární kombinaci předchozích prvků $\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}$.

(c) Nulový prvek $\mathbf{o}$ lze vyjádřit jako lineární kombinaci prvků $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ 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 z rovnosti

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

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

(d) Každý prvek $\mathbf{b} \in V$ lze vyjádřit jako lineární kombinaci prvků $\mathbf{v}_1$, $\mathbf{v}_2$, …, $\mathbf{v}_k$ nejvýše jedním způsobem.

(21) Posloupnost sloupcových vektorů matice $A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ typu $m \times n$ nad tělesem $\mathbf{T}$ tvoří lineárně nezávislou posloupnost v $\mathbf{T}^m$ právě tehdy, když $\operatorname{Ker} A = \{\mathbf{o}\}$, tj. právě když má soustava $A\mathbf{x} = \mathbf{o}$ pouze triviální řešení $\mathbf{x} = \mathbf{o}$.

(22) Nechť $A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ je matice typu $m \times n$ nad tělesem $\mathbf{T}$, R je regulární matice řádu m a Q je regulární matice řádu n. Pak platí

(a) posloupnost $(\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n)$ sloupcových vektorů matice A je lineárně nezávislá právě tehdy, když je lineárně nezávislá posloupnost sloupcových vektorů matice AQ,

(b) posloupnost $(\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n)$ sloupcových vektorů matice A je lineárně nezávislá právě tehdy, když je lineárně nezávislá posloupnost sloupcových vektorů matice RA.

(23) Elementární řádkové úpravy nemění lineární (ne)závislost posloupnosti sloupcových vektorů ani posloupnosti řádkových vektorů matice.

Elementární sloupcové úpravy nemění lineární (ne)závislost posloupnosti sloupcových vektorů ani posloupnosti řádkových vektorů matice.

(24) Posloupnost řádkových vektorů matice v odstupňovaném tvaru je lineárně nezávislá právě tehdy, když matice neobsahuje nulový řádek.

(25) Posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ prvků lineárního prostoru $\mathbf{V}$ nad $\mathbf{T}$ se nazývá *báze*, pokud je lineárně nezávislá a $\langle \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n \rangle = \mathbf{V}$.

(26) Posloupnost prvků $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ tvoří bázi lineárního prostoru $\mathbf{V}$ právě tehdy, když lze každý prvek $\mathbf{b} \in V$ vyjádřit právě jedním způsobem jako lineární kombinaci prvků $\mathbf{v}_1$, $\mathbf{v}_2$, …, $\mathbf{v}_n$.

(27) *Kanonická báze* (též *standardní báze*) v aritmetickém prostoru $\mathbf{T}^n$ je posloupnost

$$(\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n) = \left(\begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \right) .$$

(28) Odvození formule pro n-tý člen Fibonacciho posloupnosti.

(29) Lineární prostor se nazývá *konečně generovaný*, pokud má nějakou konečnou množinu generátorů.

(30) Minimální posloupnost generátorů $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ lineárního prostoru $\mathbf{V}$ je báze $\mathbf{V}$.

(31) Z každé konečné množiny generátorů lineárního prostoru lze vybrat bázi.

(32) Každý konečně generovaný lineární prostor má bázi.

(33) **Steinitzova věta o výměně.** Nechť $N = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$ je lineárně nezávislá posloupnost prvků lineárního prostoru $\mathbf{V}$ nad $\mathbf{T}$ a nechť $G = (\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_l)$ generuje $\mathbf{V}$. Pak $k \leq l$ a při vhodném uspořádání $G' = (\mathbf{w}'_1, \mathbf{w}'_2, \ldots, \mathbf{w}'_l)$ posloupnosti G platí, že $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k, \mathbf{w}'_{k+1}, \mathbf{w}'_{k+2}, \ldots, \mathbf{w}'_l)$ generuje $\mathbf{V}$.

(34) Každé dvě báze konečně generovaného lineárního prostoru mají stejný počet prvků.

(35) *Dimenzí* konečně generovaného lineárního prostoru $\mathbf{V}$ nad $\mathbf{T}$ rozumíme počet prvků jeho libovolné báze. Dimenzi prostoru $\mathbf{V}$ značíme $\dim(V)$.

(36) Nechť G je konečná množina generátorů lineárního prostoru $\mathbf{V}$. Potom každou lineárně nezávislou posloupnost ve $\mathbf{V}$ jde doplnit prvky G na bázi $\mathbf{V}$.

(37) Maximální lineárně nezávislá posloupnost v konečně generovaném prostoru je bází.

Obecněji, maximální lineárně nezávislá posloupnost prvků konečné množiny generátorů je bází.

(38) V každém lineárním prostoru $\mathbf{V}$ dimenze n platí:
  (a) Každá množina generátorů $\mathbf{V}$ obsahuje alespoň n prvků.
  (b) Každá n-prvková posloupnost generátorů je bází $\mathbf{V}$.
  (c) Každá lineárně nezávislá posloupnost ve $\mathbf{V}$ obsahuje nejvýše n prvků.
  (d) Každá n-prvková lineárně nezávislá posloupnost ve $\mathbf{V}$ je bází $\mathbf{V}$.

(39) 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 $W = V$.

(40) Nechť $B = (\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$ je báze lineárního prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$ a $\mathbf{w} \in \mathbf{V}$. *Souřadnicemi* (též *vyjádřením*) *prvku* $\mathbf{w}$ *vzhledem k* B rozumíme (jednoznačně určený) aritmetický vektor $(a_1, a_2, \dots, a_n)^T \in \mathbf{T}^n$ 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.

$$[\mathbf{w}]_B = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \ .$$

(41) Nechť $B = (\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$ je báze lineární prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$, nechť $\mathbf{u}, \mathbf{w} \in V$ a $t \in T$. Pak platí
  (a) $[\mathbf{u} + \mathbf{w}]_B = [\mathbf{u}]_B + [\mathbf{w}]_B$ a
  (b) $[t\mathbf{u}]_B = t[\mathbf{u}]_B$

(42) Nechť B je báze lineárního prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$ dimenze n. Pak platí
  (a) 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 $\mathbf{T}^n$;
  (b) množina X generuje $\mathbf{V}$ právě tehdy, když $[X]_B$ generuje $\mathbf{T}^n$;
  (c) 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 $\mathbf{T}^n$.

(43) Nechť $B = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ a C jsou báze lineárního prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$. *Maticí přechodu od báze* B *k bázi* C rozumíme matici

$$[\mathrm{id}]_C^B = ([\mathbf{v}_1]_C \,|\, [\mathbf{v}_2]_C \,|\, \cdots \,|\, [\mathbf{v}_n]_C) \ .$$

(44) Nechť $\mathbf{V}$ je lineární prostor $\mathbf{V}$ nad tělesem $\mathbf{T}$ dimenze n a B, C jsou báze $\mathbf{V}$. Pak pro libovolný prvek $\mathbf{x} \in \mathbf{V}$ platí

$$[\mathbf{x}]_C = [\mathrm{id}]_C^B [\mathbf{x}]_B \ .$$

Navíc je matice $[\mathrm{id}]_C^B$ tímto vztahem určena jednoznačně.

(45) Nechť $A = (\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n)$ je matice nad $\mathbf{T}$. Říkáme, že i-tý sloupec matice A je *bázový*, pokud není lineární kombinací předchozích sloupců, tj. pokud platí

$$\mathbf{a}_i \notin \langle \mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{i-1} \rangle \quad .$$

(46) Pro libovolnou matici A tvoří bázové sloupce bázi sloupcového prostoru. Speciálně, dimenze $\operatorname{Im} A$ je rovna počtu bázových sloupců.

(47) Bázové sloupce matice A nad $\mathbf{T}$ typu $m \times n$ v odstupňovaném tvaru jsou právě sloupce $k_1, k_2, \ldots, k_r$, kde $r, k_1, \ldots, k_r$ jsou parametry z definice 2.12 odstupňovaného tvaru.

(48) 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.

(49) Pro libovolnou matici A platí $\dim(\operatorname{Im} A) = \dim(\operatorname{Im} A^T)$.

(50) *Hodností* matice A rozumíme dimenzi řádkového (sloupcového) prostoru matice A. Značíme $\operatorname{rank}(A)$.

(51) Pro libovolnou matici A typu $m \times n$ platí $\operatorname{rank}(A) = \operatorname{rank}(A^T) \leq m, n$. Hodnost se nemění elementárními řádkovými ani sloupcovými úpravami. Hodnost matice v řádkově odstupňovaném tvaru je rovna počtu nenulových řádků.

(52) Nechť A je matice nad $\mathbf{T}$ typu $m \times n$ a B matice nad $\mathbf{T}$ typu $n \times p$. Pak platí

$$\operatorname{rank}(AB) \leq \operatorname{rank}(A), \quad \operatorname{rank}(AB) \leq \operatorname{rank}(B) \quad .$$

(53) 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.

(54) Nechť A je čtvercová matice nad $\mathbf{T}$ řádu n. Následující tvrzení jsou ekvivalentní.

1. A je regulární.
11. $\operatorname{rank}(A) = n$.
12. Sloupce (řádky) matice A jsou lineárně nezávislé.
13. Sloupce (řádky) matice A generují $\mathbf{T}^n$.
14. Sloupce (řádky) matice A tvoří bázi $\mathbf{T}^n$.

(55) Matice je v *redukovaném (řádkově) odstupňovaném tvaru*, pokud je v řádkově odstupňovaném tvaru a každý bázový sloupec má jedinou nenulovou složku rovnou 1.

(56) Každou matici A lze převést do redukovaného odstupňovaného tvaru takto:

(a) Matici Gaussovo eliminací převedeme do odstupňovaného tvaru.
(b) Vynásobíme nenulové řádky tak, aby byl každý pivot roven 1.
(c) Postupně vynulujeme zbylé prvky v každém bázovém sloupci.

Tomuto procesu se říká Gaussova-Jordanova eliminace.

(57) Libovolná matice A typu $m \times n$ nad $\mathbf{T}$ s hodností r je rovná součinu $A = BC$, kde B je matice typu $m \times r$ tvořená bázovými sloupci matice A (v pořadí v jakém se vyskytují v A) a C je matice typu $r \times n$ tvořená nenulovými řádky v redukovaném odstupňovaném tvaru D matice A.

(58) Použití skeletního rozkladu k bezztrátové komprimaci dat uložených do matice.

(59) **Frobeniova věta.** Soustava $A\mathbf{x} = \mathbf{b}$ má řešení právě tehdy, když $\operatorname{rank}(A) = \operatorname{rank}(A \,|\, \mathbf{b})$.

(60) **Věta o dimenzi jádra a obrazu.** Pro libovolnou matici A nad $\mathbf{T}$ typu $m \times n$ platí
$$\dim(\mathrm{Ker}\, A) + \dim(\mathrm{Im}\, A) = n \ .$$
(61) Jsou-li $V_i, i \in I$ podprostory vektorového prostoru $\mathbf{V}$, pak $\bigcap_{i\in I} V_i$ je podprostorem $\mathbf{V}$.
(62) 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 $V_1 + V_2 + \cdots + V_k$.
(63) Pro podprostory $\mathbf{U}$, $\mathbf{W}$ lineárního prostoru $\mathbf{V}$ platí
$$\mathbf{U} + \mathbf{W} = \{\mathbf{u} + \mathbf{w} : \mathbf{u} \in U, \mathbf{w} \in W\}$$
(64) **Věta o dimenzi součtu a průniku podprostorů.** Pro libovolné dva konečně generované podprostory $\mathbf{U}, \mathbf{V}$ vektorového prostoru $\mathbf{W}$ platí
$$\dim(\mathbf{U}) + \dim(\mathbf{V}) = \dim(\mathbf{U} \cap \mathbf{V}) + \dim(\mathbf{U} + \mathbf{V}) \ .$$

Klíčové znalosti ze čtvrté kapitoly nezbytné pro průběžné sledování přednášek s pochopením

(1) Definice lineárního prostoru nad tělesem $\mathbf{T}$ a jednoduché vlastnosti počítání v něm, příklady lineárních prostorů.
(2) Pojem podprostoru lineárního prostoru a ekvivalentní definnice pomocí uzavřenosti na operace.
(3) Definice lineární kombinace prvků, lineárního obalu množiny prvků, množiny generátorů, a konečně generovaného lineárního prostoru.
(4) Lineární obal $\langle X \rangle$ množiny $X \subseteq \mathbf{V}$ je nejmenší podprostor $\mathbf{V}$ obsahující X, kdy platí inkluze $\langle X \rangle \subseteq \langle Y \rangle$.
(5) Lineární závislost a nezávislost konečné posloupnosti prvků lineárního prostoru, různé ekvivalentní definice.
(6) Báze konečně generovaného lineárního prostoru a ekvivalentní formulace pomocí jednoznačnosti vyjádření prvků prostoru jako lineární kombinace prvků báze.
(7) Steinitzova věta o výměně, rovnost počtu prvků libovolných dvou bází a definice dimenze konečně generovaného lineárního prostoru.
(8) Různé ekvivalentní definice báze (např. maximální lineárně nezávislá posloupnost, atd.).
(9) Sloupcový a řádkový prostor matice, čtyři podprostory určené maticí.
(10) Vliv elementárních řádkových a sloupcových úprav na čtyři základní prostory matice.
(11) Ekvivalentní definice lineární nezávislosti posloupnosti sloupcových vektorů matice pomocí jádra matice.
(12) Vliv elementárních řádkových a sloupcových úprav na lineární (ne)závislost posloupnosti sloupcových nebo řádkových vektorů matice.

(13) Bázové sloupce matice, báze sloupcového a řádkového prostoru matice v řádkově odstupňovaném tvaru.
(14) Rovnost dimenze řádkového a dimenze sloupcového prostoru matice, definice hodnosti matice.
(15) Další ekvivalentní podmínky s regularitou matice.
(16) Odhady hodnosti součinu matic pomocí hodností činitelů.
(17) Frobeniova věta a věta o dimenzi jádra a obrazu matice.
(18) Souřadnice vektoru vzhledem k bázi, souřadnice součtu dvou prvků a skalárního násobku prvku.
(19) Matice přechodu mezi dvěma bázemi lineárního prostoru, vzorec pro přepočet souřadnic vektoru vzhledem ke dvěma různým bázím.
(20) Průnik a součet podprostorů, ekvivalentní popis součtu dvou podprostorů.
(21) Věta o dimenzi součtu a průniku podprostorů.

6. Lineární zobrazení

Cíl. *Dosud jsme zobecnili počítání s reálnými čísly na počítání v tělese a počítání s aritmetickými vektory na počítání v lineárním prostoru. V této kapitole zobecníme matice do pojmu lineárního zobrazení. Ukážeme si základní vlastnosti lineárních zobrazení.*

6.1. Definice a příklady.

Připomeňme, že každá 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:** podprostor $\operatorname{Ker} A \leq \mathbf{T}^n$ se rovná 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:** podprostor $\operatorname{Im} A \leq \mathbf{T}^m$ se rovná obrazu zobrazení f_A. Hodnost $\operatorname{rank}(A)$ matice A se rovná dimenzi $\operatorname{Im} A$.
$$\operatorname{Im} A = \{f_A(\mathbf{x}) : \mathbf{x} \in \mathbf{T}^n\} = f_A(T^n) \leq \mathbf{T}^m, \quad \operatorname{rank}(A) = \dim(\operatorname{Im} A) \ .$$

Rovněž nám tento pohled poskytl geometrickou interpretaci řady tvrzení.

Ne každé zobrazení $f : T^n \to T^m$ 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 lineárními prostory (nejen aritmetickými vektorovými).

Definice 6.1. Nechť $\mathbf{V}, \mathbf{W}$ jsou lineární 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 prvek ve $\mathbf{V}$ na nulový prvek ve $\mathbf{W}$.

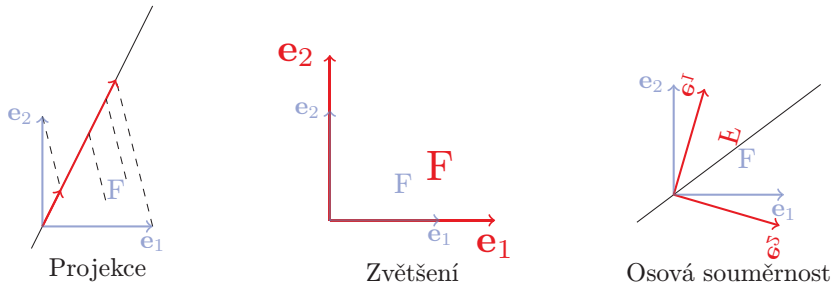
Pro libovolnou matici A nad $\mathbf{T}$ typu $m \times n$ je zobrazení $f_A : T^n \to T^m$ lineární, protože
$$f_A(\mathbf{u} + \mathbf{v}) = A(\mathbf{u} + \mathbf{v}) = A\mathbf{u} + A\mathbf{v} = f_A(\mathbf{u}) + f_A(\mathbf{v})$$
a
$$f_A(t\mathbf{u}) = A(t\mathbf{u}) = t(A\mathbf{u}) = tf_A(\mathbf{u}) \ .$$
To nám dává řadu příkladů lineárních zobrazení mezi aritmetickými vektorovými prostory (a jak jsme zmínili a za chvíli dokážeme, jiná lineární zobrazení mezi aritmetickými vektorovými prostory neexistují).

Příklad 6.2. Příklady lineárních zobrazení z $\mathbb{R}^2$ do $\mathbb{R}^2$:

- Otočení (rotace) o daný úhel.
- Zkosení

Obrázek 63. Zobrazení v rovině: otočení a zkosení

- Projekce na přímku procházející počátkem.
- Osová souměrnost podle přímky procházející počátkem.
- Zvětšení (zmenšení)



Obrázek 64. 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

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

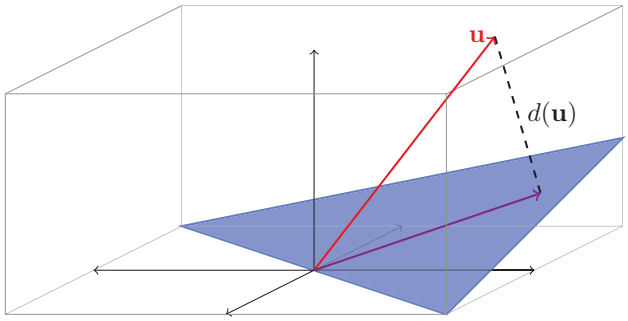
Lineární zobrazení z $\mathbb{R}^3$ do $\mathbb{R}^2$ používáme při kreslení trojrozměrných útvarů na tabuli (papír).

Příkladem lineárního zobrazení z $\mathbb{R}^3$ do $\mathbb{R}$ je zobrazení d udávající orientovanou vzdálenost od zvolené roviny procházející počátkem.

Ještě než popíšeme, jak vypadají lineární zobrazení obecně, podíváme se na další příklady.

Příklad 6.3.

- 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.



Obrázek 65. Lineární zobrazení z $\mathbb{R}^3$ do $\mathbb{R}$: orientovaná vzdálenost od plochy

- Nechť $B = (\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$ 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 5.69 o souřadnicích a operacích.
- Zobrazení přiřazující matici nad $\mathbf{T}$ typu $n \times n$ součet prvků na diagonále (tzn. stopu) je lineárním zobrazením $\mathbf{T}^{n\times n} \to \mathbf{T}$.
- 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 integrovatelných funkcí na $[1, 10]$ do $\mathbb{R}$.

6.2. **Matice lineárního zobrazení.**

Z definice lineárního zobrazení snadno indukcí dokážeme, že obrazem lineární kombinace je lineární kombinace obrazů, tj. že 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 6.4. *Jsou-li $\mathbf{V}$ a $\mathbf{W}$ lineární prostory nad tělesem $\mathbf{T}$, je-li $B = (\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$ báze v prostoru $\mathbf{V}$, a jsou-li $\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_n \in W$ 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 prvek $\mathbf{x} \in \mathbf{V}$ 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 prvky $\mathbf{x}, \mathbf{y} \in \mathbf{V}$, 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 $[\mathbf{x}+\mathbf{y}]_B = (t_1+s_1, t_2+s_2, \ldots, t_n+s_n)^T$ (viz tvrzení 5.69 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 prvků jsou pak určené linearitou.

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 aritmetický vektor $\mathbf{x} = (x_1, x_2, \ldots, x_n)^T \in \mathbf{T}^n$ 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

$$f(\mathbf{x}) = (f(\mathbf{e}_1) \,|\, f(\mathbf{e}_2) \,|\, \cdots \,|\, f(\mathbf{e}_n))\,\mathbf{x} \ ,$$

takže stačí položit $A = (f(\mathbf{e}_1) \,|\, f(\mathbf{e}_2) \,|\, \cdots \,|\, f(\mathbf{e}_n))$ a máme $f = f_A$. Matice A je určena jednoznačně, protože i-tý sloupec se musí rovnat $f(\mathbf{e}_i)$, kde $\mathbf{e}_i$ je i-tý vektor kanonické báze v $\mathbf{T}^n$.

Lineární zobrazení $f : \mathbf{V} \to \mathbf{W}$, kde $\mathbf{V}, \mathbf{W}$ jsou konečně generované lineární prostory, 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 prvek $\mathbf{x} \in V$. Této matici říkáme matice f vzhledem k B a C. Odvození, jak tato matice vypadá, se udělá podobně jako výše.

Definice 6.5. Nechť $\mathbf{V}, \mathbf{W}$ jsou konečně generované lineární prostory nad tělesem $\mathbf{T}$, $f : \mathbf{V} \to \mathbf{W}$, $B = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ je báze ve $\mathbf{V}$ a C je báze ve $\mathbf{W}$. *Maticí lineárního zobrazení f vzhledem k bázím B a C* rozumíme matici

$$[f]_C^B = ([f(\mathbf{v}_1)]_C \,|\, [f(\mathbf{v}_2)]_C \,|\, \cdots \,|\, [f(\mathbf{v}_n)]_C) \ .$$

V matici f vzhledem k B a C je tedy i-tý sloupec roven souřadnicím prvku $f(\mathbf{v}_i)$, tj. obrazu i-tého vektoru $\mathbf{v}_i$ báze B, vzhledem k bázi C. Matice je typu $\dim(\mathbf{W}) \times \dim(\mathbf{V})$.

Tvrzení 6.6. *Jsou-li $\mathbf{V}, \mathbf{W}$ konečně generované lineární prostory nad tělesem $\mathbf{T}$, $B = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ báze prostoru $\mathbf{V}$, C báze prostoru $\mathbf{W}$, a $f : \mathbf{V} \to \mathbf{W}$ lineární zobrazení, pak pro libovolný prvek $\mathbf{x} \in V$ platí*

$$[f(\mathbf{x})]_C = [f]_C^B\,[\mathbf{x}]_B \ .$$

Důkaz. Pro libovolný prvek $\mathbf{x} \in V$ s vyjádřením $\mathbf{x} = x_1\mathbf{v}_1 + x_2\mathbf{v}_2 + \cdots + x_n\mathbf{v}_n$ vzhledem k bázi B 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 5.69 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 pomocí násobení matic zapíšeme jako

$$[f(\mathbf{x})]_C = ([f(\mathbf{v}_1)]_C|[f(\mathbf{v}_2)]_C|\dots|[f(\mathbf{v}_n)]_C)\,(x_1, x_2, \dots, x_n)^T = [f]_C^B\,[\mathbf{x}]_B \ .$$

□

Matice $[f]_C^B$ tedy umožňuje počítat souřadnice $[f(\mathbf{x})]_C$ prvku $f(\mathbf{x})$ vzhledem k bázi C prostoru $\mathbf{W}$, známe-li souřadnice $[\mathbf{x}]_B$ vektoru $\mathbf{x}$ vzhledem k bázi B prostoru $\mathbf{V}$.

Matice $[f]_C^B$ je jediná matice splňující rovnost z předchozího tvrzení.

Tvrzení 6.7. *Jsou-li $\mathbf{V}, \mathbf{W}$ konečně generované lineární prostory nad tělesem $\mathbf{T}$, B báze $\mathbf{V}$, C báze $\mathbf{W}$ a $f : \mathbf{V} \to \mathbf{W}$ a M matice nad tělesem $\mathbf{T}$ splňující $[f(\mathbf{x})]_C = M\,[\mathbf{x}]_B$ pro každý prvek $\mathbf{x} \in \mathbf{V}$, pak $M = [f]_C^B$.*

Důkaz. Předně si uvědomíme, že M musí být typu $\dim(\mathbf{W}) \times \dim(\mathbf{V})$, aby mohl vztah $[f(\mathbf{x})]_C = M\,[\mathbf{x}]_B$ vůbec platit. Dosadíme-li do tohoto vztahu i-tý vektor $\mathbf{v}_i$ báze B, dostaneme $[f(\mathbf{v}_i)]_C = M\,[\mathbf{v}_i]_B = M\,\mathbf{e}_i$. Pravá strana je rovná i-tému sloupci matice M, tedy $M = ([f(\mathbf{v}_1)]_C \,|\, [f(\mathbf{v}_2)]_C \,|\, \cdots \,|\, [f(\mathbf{v}_n)]_C) = [f]_C^B$. □

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 v aritmetickám prostoru $\mathbf{T}^i$.

Příklad 6.8. 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 6.9. 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 4.6.1.

Příklad 6.10. Uvažujme zrcadlení $f : \mathbb{R}^2 \to \mathbb{R}^2$ podle přímky p procházející počátkem a bodem $(2,5)^T$. 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 6.11. 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

$$[f]_B^B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix} .$$

V definici 5.72 byl zaveden pojem matice přechodu od báze B k bázi C konečně generovaného prostoru $\mathbf{V}$. Pojem matice lineárního zobrazení nám umožňuje zdůvodnit zavedené značení $[\mathrm{id}]_C^B$.

Pozorování 6.12. *Jsou-li B, C dvě báze konečně generovaného prostoru $\mathbf{V}$, pak matice identického zobrazení z $\mathbf{V}$ do $\mathbf{V}$ se rovná matici přechodu od báze B k bázi C.*

Důkaz. Přímý důsledek definic. □

Přesnější označení pro matici přechodu by bylo $[\mathrm{id}_V]_C^B$, abychom zdůraznili, že se jedná o matici identického zobrazení id_V z V do V. Index V ale pro přehlednost většinou vynecháváme, obvykle víme, v jakém prostoru $\mathbf{V}$ počítáme.

Vztah $[\mathbf{x}]_C = [\mathrm{id}]_C^B [\mathbf{x}]_B$ z tvrzení 5.73 je nyní důsledkem tvrzení 6.6.

Příklad 6.13. 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 6.14. Matice přechodu od B k B je vždy identická matice, protože vyjádření i-tého vektoru báze B vzhledem k bázi B je $\mathbf{e}_i$.

6.3. **Skládání lineárních zobrazení.** 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. Podíváme se nejprve na skládání a invertování.

Tvrzení 6.15. *Jsou-li $\mathbf{U}, \mathbf{V}, \mathbf{W}$ lineární prostory nad tělesem $\mathbf{T}$ a jsou-li $f : \mathbf{U} \to \mathbf{V}$ a $g : \mathbf{V} \to \mathbf{W}$ lineární zobrazení, pak složené zobrazení gf je lineární zobrazení $gf : \mathbf{U} \to \mathbf{W}$.*

Jsou-li navíc prostory $\mathbf{U}, \mathbf{V}, \mathbf{W}$ konečně generované a jsou-li B báze v $\mathbf{U}$, C báze ve $\mathbf{V}$ a D báze ve $\mathbf{W}$, pak platí

$$[gf]_D^B = [g]_D^C [f]_C^B .$$

Důkaz. Pro libovolné dva vektory $\mathbf{x}, \mathbf{y} \in U$ dostáváme využitím předpokladu linearity f a g, že

$$gf(\mathbf{x}+\mathbf{y}) = g(f(\mathbf{x}+\mathbf{y})) = g(f(\mathbf{x})+f(\mathbf{y})) = gf(\mathbf{x}) + gf(\mathbf{y}) \ .$$

Zobrazení gf tedy zachovává sčítání. Podobně, pro každý vektor $\mathbf{x} \in U$ a každý skalár $t \in T$ platí

$$gf(t\mathbf{x}) = g(t\ f(\mathbf{x})) = t\ gf(\mathbf{x}) \ .$$

Zobrazení gf proto zachovává i násobení skalárem, takže je lineární.

K důkazu druhé části ověříme (dvojím užitím tvrzení 6.6 o matici lineárního zobrazení), že pro libovolné $\mathbf{x} \in \mathbf{U}$ platí

$$[gf(\mathbf{x})]_D = [g]_D^C\,[f(\mathbf{x})]_C = [g]_D^C\,([f]_C^B\,[\mathbf{x}]_B) = ([g]_D^C\,[f]_C^B)[\mathbf{x}]_B \ .$$

Z tvrzení 6.7 o jednoznačnosti matice lineárního zobrazení nyní vyplývá, že $[gf]_D^B = [g]_D^C\,[f]_C^B$. □

Tvrzení 6.16. *Nechť $\mathbf{U}, \mathbf{V}$ jsou lineární prostory nad tělesem $\mathbf{T}$ a $f : \mathbf{U} \to \mathbf{V}$ vzájemně jednoznačné lineární zobrazení. Pak $f^{-1} : \mathbf{V} \to \mathbf{U}$ je také lineární zobrazení.*

Jsou-li navíc $\mathbf{U}, \mathbf{V}$ konečně generované lineární prostory dimenze n, B báze v $\mathbf{U}$ a C báze ve $\mathbf{V}$, pak platí

$$[f^{-1}]_B^C = \left([f]_C^B\right)^{-1} \ .$$

Důkaz. Zvolíme libovolné dva libovolné prvky $\mathbf{x}, \mathbf{y} \in V$. Protože f je na V, existují $\mathbf{u}, \mathbf{v} \in U$ takové, že $f(\mathbf{u}) = \mathbf{x}$ a $f(\mathbf{v}) = \mathbf{y}$. Protože f je lineární, platí $f(\mathbf{u}+\mathbf{v}) = f(\mathbf{u}) + f(\mathbf{v}) = \mathbf{x}+\mathbf{y}$ a tedy $f^{-1}(\mathbf{x}+\mathbf{y}) = \mathbf{u}+\mathbf{v} = f^{-1}(\mathbf{x}) + f^{-1}(\mathbf{y})$.

Podobně, pro libovolný skalár $t \in T$ platí $f(t\mathbf{u}) = tf(\mathbf{u}) = t\mathbf{x}$ a tedy $f^{-1}(t\mathbf{x}) = t\mathbf{u} = tf^{-1}(\mathbf{x})$.

K důkazu druhé části využijeme druhou část tvrzení 6.15 o složeném zobrazení. Protože $f^{-1}f = \mathrm{id}_U$, platí $I_n = [\mathrm{id}_U]_B^B = [f^{-1}f]_B^B = [f^{-1}]_B^C\,[f]_C^B$. Matice $[f]_C^B$ je čtvercová, proto $[f^{-1}]_B^C = ([f]_C^B)^{-1}$. □

V druhé části tvrzení stačí předpokládat, že prostor $\mathbf{U}$ je konečně generovaný. Podle bodu (2) nebo (3) tvrzení 6.29 je pak prostor $\mathbf{V}$ také konečně generovaný a má stejnou dimenzi.

Ukážeme si použití předchozích dvou tvrzení na početních příkladech.

Příklad 6.17. 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 přímo z definice.

$$[\mathrm{id}]_{K_2}^B = \begin{pmatrix} 2 & -5 \\ 5 & 2 \end{pmatrix}$$

Využijeme $\mathrm{id}^{-1} = \mathrm{id}$ a tvrzení 6.16:

$$[\mathrm{id}]_B^{K_2} = [\mathrm{id}^{-1}]_B^{K_2} = ([\mathrm{id}]_{K_2}^B)^{-1} = \begin{pmatrix} 2 & -5 \\ 5 & 2 \end{pmatrix}^{-1} = \frac{1}{29}\begin{pmatrix} 2 & 5 \\ -5 & 2 \end{pmatrix} \ .$$

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 6.10 jsme nahlédli, že matice f vzhledem k B a kanonické bázi je

$$[f]_{K_2}^B = \begin{pmatrix} 2 & 5 \\ 5 & -2 \end{pmatrix} \ .$$

Pomocí tvrzení 6.15 a užitím $f = f\,\mathrm{id}$ nyní můžeme spočítat matici f vzhledem ke kanonickým bázím:

$$[f]_{K_2}^{K_2} = [f]_{K_2}^{B}\,[\mathrm{id}]_{B}^{K_2} = \begin{pmatrix} 2 & 5 \\ 5 & -2 \end{pmatrix} \frac{1}{29} \begin{pmatrix} 2 & 5 \\ -5 & 2 \end{pmatrix} = \frac{1}{29} \begin{pmatrix} -21 & 20 \\ 20 & 21 \end{pmatrix} .$$

Příklad 6.18. 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 tvrzení 6.15 a 6.16:

$$\begin{aligned}[\mathrm{id}]_{C}^{B} &= [\mathrm{id}]_{C}^{K_2}\,[\mathrm{id}]_{K_2}^{B} = \left([\mathrm{id}]_{K_2}^{C}\right)^{-1}[\mathrm{id}]_{K_2}^{B} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^{-1} \begin{pmatrix} 2 & 3 \\ 4 & 3 \end{pmatrix} \\ &= \frac{1}{3} \begin{pmatrix} 4 & 3 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 4 & 3 \end{pmatrix} = 2 \begin{pmatrix} 0 & 1 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 1 & 3 \end{pmatrix}\end{aligned}$$

Souřadnice $\mathbf{v}$ vzhledem k C jsou

$$[\mathbf{v}]_C = [\mathrm{id}]_{C}^{B}\,[\mathbf{v}]_B = \begin{pmatrix} 0 & 2 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 2x_2 \\ x_1 + 3x_2 \end{pmatrix} .$$

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 6.19. V příkladu 6.8 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 matice $[f]_{K_2}^{K_3}$, $[\mathrm{id}]_{K_3}^{B}$ a $[\mathrm{id}]_{K_2}^{C}$. Pomocí těchto matic lze spočítat $[f]_{C}^{B}$:

$$\begin{aligned}[f]_{C}^{B} &= [\mathrm{id}]_{C}^{K_2}\,[f]_{K_2}^{K_3}\,[\mathrm{id}]_{K_3}^{B} = \left([\mathrm{id}]_{K_2}^{C}\right)^{-1}[f]_{K_2}^{K_3}\,[\mathrm{id}]_{K_3}^{B} \\ &= \begin{pmatrix} 1 & 3 \\ 2 & 3 \end{pmatrix}^{-1} \begin{pmatrix} 2 & 3 & 1 \\ 4 & 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 4 \\ 2 & 0 & 4 \end{pmatrix} \\ &= \frac{1}{2} \begin{pmatrix} 3 & 2 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 & 2 \\ 3 & 3 & 0 \end{pmatrix} = 3 \begin{pmatrix} 2 & 1 & 1 \\ 4 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 3 \\ 2 & 4 & 3 \end{pmatrix} .\end{aligned}$$

Následující důsledek tvrzení 6.15 a 6.16 je obzvláště důležitý, jak zjistíme v kapitole o vlastních číslech. Proto jej formulujeme jako samostatné tvrzení.

Tvrzení 6.20. *Je-li $\mathbf{V}$ konečně generovaný lineární prostor nad tělesem $\mathbf{T}$, $f : \mathbf{V} \to \mathbf{V}$ lineární zobrazení, B, C dvě báze prostoru $\mathbf{V}$, a R matice přechodu od báze B k bázi C, pak*

$$[f]_{B}^{B} = R^{-1}\,[f]_{C}^{C}\,R .$$

Důkaz. Protože $f = \mathrm{id}_V \; f \; \mathrm{id}_V$ máme

$$[f]_B^B = [\mathrm{id}_V]_B^C \, [f]_C^C \, [\mathrm{id}_V]_C^B = \left([\mathrm{id}_V]_C^B\right)^{-1} \, [f]_C^C \, [\mathrm{id}_V]_C^B = R^{-1} \, [f]_C^C \, R \ .$$

□

6.4. **Typy lineárních zobrazení.** Následující definice zavádí terminologii pro různé typy lineárních zobrazení.

Definice 6.21. Nechť $\mathbf{V}$, $\mathbf{W}$ jsou lineární prostory nad tělesem $\mathbf{T}$ a $f : \mathbf{V} \to \mathbf{W}$ je lineární zobrazení.

- Pokud je f prosté, říkáme že f je *monomorfismus*,
- pokud je f na prostor $\mathbf{W}$, říkáme že f je *epimorfismus*,
- pokud f je vzájemně jednoznačné, říkáme že f je *izomorfismus*,
- pokud $\mathbf{V} = \mathbf{W}$, říkáme že f je *endomorfismus* prostoru $\mathbf{V}$ (nebo také *lineární operátor* na prostoru $\mathbf{V}$),
- pokud $\mathbf{W} = \mathbf{T} = \mathbf{T}^1$, říkáme že f je *lineární forma* na $\mathbf{V}$,
- pokud je f izomorfismus a endomorfismus, říkáme, že f je *automorfismus* prostoru $\mathbf{V}$.

Příklad 6.22. Rotace a osové souměrnosti jsou automorfismy $\mathbb{R}^2 \to \mathbb{R}^2$.

Zobrazení přiřazující vektoru z $\mathbf{V}$ souřadnice ve zvolené bázi $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ 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.

6.4.1. *Jádro a obraz.* Jako defekt prostoty zavedeme jádro $\mathrm{Ker}\, f$ lineárního zobrazení f, je tvořeno těmi vektory, které f zobrazí na nulový vektor. Obraz lineárního zobrazení f budeme značit $\mathrm{Im}\, f$.

Definice 6.23. Nechť $f : \mathbf{V} \to \mathbf{W}$ je lineární zobrazení. *Jádrem* f rozumíme množinu

$$\mathrm{Ker}\, f = \{\mathbf{x} \in V : f(\mathbf{x}) = \mathbf{o}\} \ .$$

Obraz (obor hodnot) f značíme $\mathrm{Im}\, f$, tj.

$$\mathrm{Im}\, f = \{f(\mathbf{x}) : \mathbf{x} \in V\} \ .$$

Všimněte si, že nulový vektor leží v jádru jakéhokoliv lineárního zobrazení. Pokud ale v jádru žádný jiný vektor neleží, je již zobrazení prosté (tj. monomorfismus).

Tvrzení 6.24. *Nechť $f : \mathbf{V} \to \mathbf{W}$ je lineární zobrazení. Pak f je prosté právě tehdy, když* $\mathrm{Ker}\, f = \{\mathbf{o}\}$.

Důkaz. Je-li f prosté a $\mathbf{x} \in \mathrm{Ker}\, f$, pak $f(\mathbf{x}) = \mathbf{o} = f(\mathbf{o})$, a protože f je prosté, plyne odtud $\mathbf{x} = \mathbf{o}$. Proto $\mathrm{Ker}\, f \subseteq \{\mathbf{o}\}$. Opačná inkluze je triviální.

Je-li naopak $\mathrm{Ker}\, f = \{\mathbf{o}\}$ a $f(\mathbf{x}) = f(\mathbf{y})$ pro nějaké vektory $\mathbf{x}, \mathbf{y} \in V$, pak z linearity f plyne $f(\mathbf{x} - \mathbf{y}) = f(\mathbf{x}) - f(\mathbf{y}) = \mathbf{o}$, takže $\mathbf{x} - \mathbf{y} \in \mathrm{Ker}\, f$, odkud plyne $\mathbf{x} = \mathbf{y}$. To dokazuje, že f je prosté. □

Z důkazu je patrné, že jádro lineárního zobrazení určuje, které dvojice vektorů se zobrazí na stejný vektor. Vztah $f(\mathbf{x}) = f(\mathbf{y})$ totiž platí právě tehdy, když $\mathbf{x} - \mathbf{y} \in \operatorname{Ker} f$.

Obraz i jádro lineárního zobrazení mezi dvěma konečně generovanými prostory 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 6.25. *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*

- *jádro* $\operatorname{Ker} f$ *je podprostorem* $\mathbf{V}$ *a platí*
$$[\operatorname{Ker} f]_B = \operatorname{Ker} [f]_C^B \ ,$$
- *obraz* $\operatorname{Im} f$ *je podprostorem* $\mathbf{W}$ *a platí*
$$[\operatorname{Im} f]_C = \operatorname{Im} [f]_C^B \ .$$

Důkaz.

- 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 lineárního zobrazení:
$$\begin{aligned}[\operatorname{Ker} f]_B &= [\{\mathbf{v} : f(\mathbf{v}) = \mathbf{o}\}]_B = \{[\mathbf{v}]_B : f(\mathbf{v}) = \mathbf{o}\} = \{[\mathbf{v}]_B : [f(\mathbf{v})]_C = \mathbf{o}\} \\ &= \{[\mathbf{v}]_B : [f]_C^B [\mathbf{v}]_B = \mathbf{o}\} = \{\mathbf{x} \in T^{\dim(V)} : [f]_C^B \mathbf{x} = \mathbf{o}\} = \operatorname{Ker} [f]_C^B\end{aligned}$$
- 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 $\mathbf{v}_1, \mathbf{v}_2 \in V$ 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 6.6 o matici lineárního zobrazení dostáváme
$$\begin{aligned}[f(V)]_C &= [\{f(\mathbf{v}) : \mathbf{v} \in V]_C = \{[f(\mathbf{v})]_C : \mathbf{v} \in V\} = \{[f]_C^B [\mathbf{v}]_B : \mathbf{v} \in V\} \\ &= \{[f]_C^B \mathbf{x} : \mathbf{x} \in T^{\dim(V)}\} = \operatorname{Im} [f]_C^B \ .\end{aligned}$$

□

Příklad 6.26. Lineární zobrazení $f : \mathbb{R}^3 \to \mathbb{R}^2$ máme dáno maticí vzhledem k následujícím bázím B v $\mathbb{R}^3$ a C v $\mathbb{R}^2$:
$$B = \left(\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ 3 \\ 0 \end{pmatrix} \right), \quad C = \left(\begin{pmatrix} 3 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \end{pmatrix} \right),$$
$$A = [f]_C^B = \begin{pmatrix} 2 & 1 & -3 \\ -4 & -2 & 6 \end{pmatrix} \ .$$

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

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

$$[\operatorname{Im} f]_C = \operatorname{Im} A = \left\langle \begin{pmatrix} 1 \\ -2 \end{pmatrix} \right\rangle$$

a

$$\operatorname{Im} f = \left\langle 1 \begin{pmatrix} 3 \\ 1 \end{pmatrix} - 2 \begin{pmatrix} -1 \\ 1 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} 5 \\ -1 \end{pmatrix} \right\rangle \ .$$

Dimenze jádra f je 2 a dimenze obrazu f je 1, což je v souladu s větou o dimenzi jádra a obrazu pro matice.

6.4.2. *Charakterizace mono/epi/izomorfismů.* Monomorfismy zobrazují lineárně nezávislé posloupnosti na lineárně nezávislé posloupnosti a tato vlastnost je charakterizuje.

Tvrzení 6.27. *Nechť $\mathbf{V}$ a $\mathbf{W}$ jsou lineární prostory nad tělesem $\mathbf{T}$, $\mathbf{V}$ je konečně generovaný a $f : \mathbf{V} \to \mathbf{W}$ je lineární zobrazení. Pak následující tvrzení jsou ekvivalentní.*

(1) *Zobrazení f je prosté (monomorfismus),*
(2) *pro každou lineárně nezávislou posloupnost $(\mathbf{v}_1, \dots, \mathbf{v}_k)$ ve $\mathbf{V}$ je posloupnost $(f(\mathbf{v}_1), \dots, f(\mathbf{v}_k))$ lineárně nezávislá ve $\mathbf{W}$,*
(3) *existuje báze $(\mathbf{v}_1, \dots, \mathbf{v}_n)$ prostoru $\mathbf{V}$ taková, že posloupnost $(f(\mathbf{v}_1), \dots, f(\mathbf{v}_n))$ je lineárně nezávislá v $\mathbf{W}$.*

Důkaz. (1) $\Rightarrow$ (2). Předpokládejme, že f je prosté a $(\mathbf{v}_1, \dots, \mathbf{v}_k)$ lineárně nezávislá posloupnost ve $\mathbf{V}$. Platí-li pro nějaké skaláry $t_1, \dots, t_k \in T$

$$t_1 f(\mathbf{v}_1) + \cdots + t_k f(\mathbf{v}_k) = \mathbf{o} \ ,$$

pak v důsledku linearity f platí rovněž

$$f(t_1 \mathbf{v}_1 + \cdots + t_k \mathbf{v}_k) = \mathbf{o} = f(\mathbf{o}) \ .$$

Protože f je prosté zobrazení, platí $t_1 \mathbf{v}_1 + \cdots + t_k \mathbf{v}_k = \mathbf{o}$, a protože $(\mathbf{v}_1, \dots, \mathbf{v}_k)$ je lineárně nezávislá, dostáváme $t_1 = \cdots = t_k = 0$.

(2) $\Rightarrow$ (3). Plyne z toho, že každá báze je lineárně nezávislá posloupnost.

(3) $\Rightarrow$ (1). Podle tvrzení 6.24 stačí dokázat, že $\operatorname{Ker} f$ obsahuje pouze nulový vektor. Uvažujme libovolný vektor $\mathbf{x} \in \operatorname{Ker} f$. Vyjádříme jej jako lineární kombinaci prvků báze $(\mathbf{v}_1, \dots, \mathbf{v}_n)$:

$$\mathbf{x} = t_1\mathbf{v}_1 + \cdots + t_n\mathbf{v}_n \ .$$

Pak

$$\mathbf{o} = f(\mathbf{x}) = f(t_1\mathbf{v}_1 + \cdots + t_n\mathbf{v}_n) = t_1 f(\mathbf{v}_1) + \cdots + t_n f(\mathbf{v}_n) \ .$$

Protože je $(f(\mathbf{v}_1), \dots, f(\mathbf{v}_n))$ je lineárně nezávislá, plyne odtud $t_1 = \cdots = t_n = 0$ a tedy $\mathbf{x} = \mathbf{o}$. □

Následuje obdobné tvrzení pro epimorfismy. Ty převádějí množiny generátorů na množiny generátorů.

Tvrzení 6.28. *Nechť $\mathbf{V}$ a $\mathbf{W}$ jsou lineární prostory nad tělesem $\mathbf{T}$, $\mathbf{V}$ je konečně generovaný a $f : \mathbf{V} \to \mathbf{W}$ je lineární zobrazení. Pak následující tvrzení jsou ekvivalentní.*

(1) *Zobrazení f je na W (epimorfismus),*
(2) *pro každou množinu generátorů $\{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ ve $\mathbf{V}$ je $\{f(\mathbf{v}_1), \dots, f(\mathbf{v}_k)\}$ množina generátorů ve $\mathbf{W}$,*
(3) *existuje báze $(\mathbf{v}_1, \dots, \mathbf{v}_n)$ prostoru $\mathbf{V}$ taková, že $\{f(\mathbf{v}_1), \dots, f(\mathbf{v}_n)\}$ generuje $\mathbf{W}$.*

Důkaz. (1) $\Rightarrow$ (2). Pro libovolný vektor $\mathbf{w} \in W$ existuje $\mathbf{x} \in V$ tak, že $f(\mathbf{x}) = \mathbf{w}$, protože f je epimorfismus. Protože $\{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ generuje $\mathbf{V}$, můžeme vektor $\mathbf{x}$ vyjádřit jako lineární kombinaci $\mathbf{x} = t_1\mathbf{v}_1 + \cdots + t_k\mathbf{v}_k$. Díky linearitě f nyní máme $\mathbf{w} = f(\mathbf{x}) = f(t_1\mathbf{v}_1 + \cdots + t_k\mathbf{v}_k) = t_1 f(\mathbf{v}_1) + \cdots + t_k f(\mathbf{v}_k)$. Zjistili jsme, že každý vektor $\mathbf{w}$ lze vyjádřit jako lineární kombinaci vektorů $f(\mathbf{v}_1), \dots, f(\mathbf{v}_k)$, což znamená, že $\{f(\mathbf{v}_1), \dots, f(\mathbf{v}_k)\}$ množina generátorů ve $\mathbf{W}$.

(2) $\Rightarrow$ (3). Plyne z toho, že každá báze $\mathbf{V}$ generuje $\mathbf{V}$.

(3) $\Rightarrow$ (1). Potřebujeme ukázat, že každý vektor $\mathbf{w} \in W$ má vzor při zobrazení f. Protože $\{f(\mathbf{v}_1, \dots, f(\mathbf{v}_n)\}$ generuje $\mathbf{W}$, můžeme $\mathbf{w}$ vyjádřit jako $\mathbf{w} = t_1 f(\mathbf{v}_1) + \cdots + t_n f(\mathbf{v}_n)$. Pak pro vektor $\mathbf{x} = t_1\mathbf{v}_1 + \cdots + t_n\mathbf{v}_n$ platí $f(\mathbf{x}) = f(t_1\mathbf{v}_1 + \cdots + t_n\mathbf{v}_n) = t_1 f(\mathbf{v}_1) + \cdots + t_n f(\mathbf{v}_n) = \mathbf{w}$. □

Důsledkem předchozích dvou tvrzení je charakterizace izomorfismů.

Tvrzení 6.29. *Nechť $\mathbf{V}$ a $\mathbf{W}$ jsou lineární prostory nad tělesem $\mathbf{T}$, $\mathbf{V}$ je konečně generovaný a $f : \mathbf{V} \to \mathbf{W}$ je lineární zobrazení. Pak následující tvrzení jsou ekvivalentní:*

(1) *zobrazení f je izomorfismus,*
(2) *pro každou bázi $(\mathbf{v}_1, \dots, \mathbf{v}_k)$ ve $\mathbf{V}$ je $(f(\mathbf{v}_1), \dots, f(\mathbf{v}_k))$ báze ve $\mathbf{W}$,*
(3) *existuje báze $(\mathbf{v}_1, \dots, \mathbf{v}_n)$ prostoru $\mathbf{V}$ taková, že $(f(\mathbf{v}_1), \dots, f(\mathbf{v}_n))$ je báze ve $\mathbf{W}$.*

6.4.3. *Izomorfismus.* Dva prostory $\mathbf{V}$, $\mathbf{W}$ nazýváme *izomorfní*, pokud existuje izomorfismus $f : \mathbf{V} \to \mathbf{W}$. (Rozmyslete si, že relace "být izomorfní" je reflexivní, symetrická a tranzitivní, tj. je to ekvivalence, viz cvičení.) Skutečnost, že $\mathbf{V}$ a $\mathbf{W}$ jsou izomorfní, zapisujeme

$$\mathbf{V} \cong \mathbf{W}$$

Izomorfní prostory jsou „v podstatě" stejné, liší se jenom přejmenováním vektorů. Podrobněji, uvažujme izomorfismus $f : \mathbf{V} \to \mathbf{W}$. Přejmenováním každého

vektoru $\mathbf{v} \in V$ na $f(\mathbf{v})$ a zachováním původních operací vznikne prostor $\mathbf{W}$. Skutečně, přejmenováním dvou vektorů $\mathbf{u}, \mathbf{v}$ ve $\mathbf{V}$ vzniknou vektory $f(\mathbf{u})$, $f(\mathbf{v})$, jejichž součet ve $\mathbf{W}$ je $f(\mathbf{u})+f(\mathbf{v})$, což je z linearity totéž jako přejmenovaný vektor $\mathbf{u}+\mathbf{v}$, tj. vektor $f(\mathbf{u}+\mathbf{v})$. Podobně pro násobení skalárem. Proto izomorfismy zachovávají mnoho vlastností.

Pozorování 6.30. *Nechť $f : \mathbf{V} \to \mathbf{W}$ je izomorfismus konečně generovaných prostorů. Pak platí*

(1) *posloupnost $(\mathbf{v}_1, \dots, \mathbf{v}_k)$ je lineárně nezávislá ve $\mathbf{V}$ právě tehdy, když je posloupnost $(f(\mathbf{v}_1), \dots, f(\mathbf{v}_k))$ lineárně nezávislá v $\mathbf{W}$,*
(2) *množina $\{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ generuje $\mathbf{V}$ právě tehdy, když množina $\{f(\mathbf{v}_1), \dots, f(\mathbf{v}_k)\}$ generuje $\mathbf{W}$,*
(3) *posloupnost $(\mathbf{v}_1, \dots, \mathbf{v}_k)$ je báze $\mathbf{V}$ právě tehdy, když je posloupnost $(f(\mathbf{v}_1), \dots, f(\mathbf{v}_k))$ báze $\mathbf{W}$,*
(4) *$\dim V = \dim W$,*
(5) *množina $M \subseteq V$ je podprostorem prostoru $\mathbf{V}$ právě tehdy, když je $f(M) = \{f(\mathbf{m}) : \mathbf{m} \in M\}$ podprostorem prostoru $\mathbf{W}$,*
(6) *pokud $\mathbf{U} \leq \mathbf{V}$, pak f zúžené na U je izomorfismem $\mathbf{U} \to f(\mathbf{U})$. Speciálně $\dim \mathbf{U} = \dim f(\mathbf{U})$.*

Důkaz. □

Pro libovolný konečně generovaný prostor $\mathbf{V}$ nad tělesem $\mathbf{T}$ s bází $B = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ je zobrazení $s : V \to T^n$ definované vztahem $s(\mathbf{v}) = [\mathbf{v}]_B$ izomorfismus $\mathbf{V} \to \mathbf{T}^n$: Zobrazení s je prosté, protože každý vektor je jednoznačně určen souřadnicemi vzhledem k B. Zobrazení s je na T^n, protože každá n-tice je souřadnicemi nějakého vektoru ve $\mathbf{V}$. Konečně s je lineární podle tvrzení 5.69. (Vlastnosti uvedené v pozorování 5.71 jsou tak speciálním případem pozorování 6.30.)

Použitím vlastností z pozorování 6.30 na tento "souřadnicový izomorfismus" získáme obecnější verzi věty o dimenzi jádra a obrazu, dříve dokázané v maticové verzi.

Věta 6.31 (o dimenzi jádra a obrazu)**.** *Jsou-li $\mathbf{V}, \mathbf{W}$ konečně generované vektorové prostory nad tělesem $\mathbf{T}$ a $f : \mathbf{V} \to \mathbf{W}$ lineární zobrazení, pak*

$$\dim(\operatorname{Ker} f) + \dim(\operatorname{Im} f) = \dim \mathbf{V} \ .$$

Důkaz. Vezmeme libovolnou bázi B prostoru $\mathbf{V}$ a bázi C prostoru $\mathbf{W}$. Označme $A = [f]_C^B$ (jde o matici typu $\dim W \times \dim V$). Podle tvrzení 6.25 o výpočtu jádra a obrazu platí $[\operatorname{Ker} f]_B = \operatorname{Ker} A$ a $[\operatorname{Im} f]_C = \operatorname{Im} A$. Z bodu (6) pozorování 6.30 nyní vyplývá $\dim \operatorname{Ker} f = \dim \operatorname{Ker} A$ a $\dim \operatorname{Im} f = \dim A$. Vztah nyní vyplývá z věty 5.94 o dimenzi jádra a obrazu pro matice. □

Souřadnicový izomorsmus také ukazuje, že každý vektorový prostor $\mathbf{V}$ nad $\mathbf{T}$ dimenze n je izomorfní aritmetickému prostoru $\mathbf{T}^n$. Ze symetrie a tranzitivity relace "být izomorfní" plyne, že libovolné dva prostory nad stejným tělesem stejné dimenze jsou izomorfní. Předvedeme "bezsouřadnicový" důkaz.

Věta 6.32. *Nechť $\mathbf{V}$ a $\mathbf{W}$ jsou dva konečně generované prostory nad tělesem $\mathbf{T}$. 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) je bod (4) v pozorování 6.30.

Pro důkaz 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 $\mathbf{W}$. Podle tvrzení 6.4 (o rozšiřování lineárního zobrazení definovaného na bázi) existuje lineární zobrazení $f : \mathbf{V} \to \mathbf{W}$ splňující $f(\mathbf{v}_i) = \mathbf{w}_i$ pro každé $i \in \{1, 2, \dots, n\}$. Toto lineární zobrazení je izomorfismem podle bodu (3) tvrzení 6.29 charakterizující izomorfismy. □

Dokázaná věta přesný význam heslu, že vektorový prostor nad daným tělesem dané dimenze je "v podstatě" jen jeden.

Věta platí i pro prostory, které nejsou konečně generované. Těmi se detailněji nezabýváme, ukážeme ale příklad izomorfismu mezi takovými prostory.

Příklad 6.33. Označíme $\mathbf{V}$ prostor všech reálných polynomů a $\mathbf{W}$ podprostor prostoru všech posloupností reálných čísel tvořený posloupnostmi, které obsahují konečně mnoho nenulových prvků. Definujeme zobrazení $f : V \to W$ vztahem

$$f(a_0 + a_1 x + \cdots + a_n x^n) = (a_0, a_1, \dots, a_n, 0, 0, \dots) \ .$$

Snadno se ověří, že f je bijekce (prosté a na) a že je lineární, tedy f je izomorfismus.

6.5. **Prostor lineárních zobrazení.** Uvažujme dva vektorové prostory $\mathbf{V}$, $\mathbf{W}$ nad stejným tělesem. Následující tvrzení ukazuje, že na množině všech lineárních zobrazení z $\mathbf{V}$ do $\mathbf{W}$ lze přirozeným způsobem zavést sčítání a skalární násobení. Další tvrzení ukazuje, že tímto získáme vektorový prostor.

Tvrzení 6.34. *Jsou-li $\mathbf{V}, \mathbf{W}$ vektorové prostory nad stejným tělesem $\mathbf{T}$, $f, g : \mathbf{V} \to \mathbf{W}$ dvě lineární zobrazení 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 $\mathbf{V} \to \mathbf{W}$.

(2) *Zobrazení $f + g$ definované vztahem*

$$(f + g)(\mathbf{x}) = f(\mathbf{x}) + g(\mathbf{x}), \quad \mathbf{x} \in V$$

je lineární zobrazení $\mathbf{V} \to \mathbf{W}$.

Tvrzení 6.35. *Jsou-li $\mathbf{V}$, $\mathbf{W}$ vektorové prostory nad stejným tělesem $\mathbf{T}$, pak množina všech lineárních zobrazení z $\mathbf{V}$ do $\mathbf{W}$ s operacemi definovanými v tvrzení 6.34 tvoří vektorový prostor nad $\mathbf{T}$.*

Důkaz. Přenecháme jako cvičení □

Definice 6.36. Vektorový prostor všech lineárních zobrazení z $\mathbf{V}$ do $\mathbf{W}$ značíme $\mathrm{Hom}(\mathbf{V}, \mathbf{W})$.

Tvrzení 6.37. *Jsou-li $\mathbf{V}$, $\mathbf{W}$ konečně generované vektorové prostory nad tělesem $\mathbf{T}$, $\dim \mathbf{V} = n$ a $\dim \mathbf{W} = m$, pak prostor $\mathrm{Hom}(\mathbf{V}, \mathbf{W})$ je izomorfní prostoru $\mathbf{T}^{m \times n}$ všech matic typu $m \times n$ nad $\mathbf{T}$*

Důkaz. Zvolíme bázi B prostoru $\mathbf{V}$ a bázi C prostoru $\mathbf{W}$. Zobrazení $s : \mathrm{Hom}(\mathbf{V}, \mathbf{W}) \to T^{m \times n}$ definujeme vztahem $s(f) = [f]_C^B$.

Zobrazení s je prosté, protože každé lineární zobrazení je jednoznačně určeno svou maticí vzhledem k B a C. Zobrazení s je na $T^{m \times n}$, protože každá matice typu $m \times n$ je maticí nějakého lineárního zobrazení $\mathbf{V} \to \mathbf{W}$. K ověření toho, že s je lineární, potřebujeme ukázat, že pro libovolné $f, g : \mathbf{V} \to \mathbf{W}$ a $t \in T$ platí $[tf]_C^B = t[f]_C^B$, $[f + g]_C^B = [f]_C^B + [g]_C^B$. To přenecháme jako cvičení. □

6.5.1. *Lineární formy.* Připomeňme, že lineární forma na vektorovém prostoru $\mathbf{V}$ nad tělesem $\mathbf{T}$ je lineární zobrazení z $\mathbf{V}$ do (jednodimenzionálního) prostoru $\mathbf{T}$.

Množinu všech lineárních forem na $\mathbf{V}$ spolu s přirozenými operacemi sčítání a násobení (zavedenými ve tvrzení 6.34) nazýváme duál prostoru $\mathbf{V}$:

Definice 6.38. Nechť $\mathbf{V}$ je vektorový prostor nad tělesem $\mathbf{T}$. *Duálem prostoru* $\mathbf{V}$ rozumíme prostor

$$\mathbf{V}^d = \mathrm{Hom}(\mathbf{V}, \mathbf{T}) \ .$$

Předpokládejme, že $\mathbf{V}$ je konečně generovaný prostor dimenze n. Prostor $\mathrm{Hom}(\mathbf{V}, \mathbf{T})$ je podle tvrzení 6.37 izomorfní prostoru $\mathbf{T}^{1\times n}$ všech matic nad $\mathbf{T}$ typu $1 \times n$ tj. prostoru řádkových vektorů. Speciálně:

Tvrzení 6.39. *Nechť* $\mathbf{V}$ *je konečně generovaný prostor, pak*

$$\dim \mathbf{V} = \dim \mathbf{V}^d \ .$$

Důkaz. $\mathbf{V}^d = \mathrm{Hom}(\mathbf{V}, \mathbf{T})$ je izomorfní $\mathbf{T}^{1\times n}$ (kde $n = \dim \mathbf{V}$) a tento prostor má dimenzi n. Protože izomorfní prostory mají stejnou dimenzi (viz např. pozorování 6.30), platí $\dim \mathbf{V}^d = n$. □

Podle důkazu tvrzení 6.37 izomorfismus $\mathrm{Hom}(\mathbf{V}, \mathbf{T}) \cong \mathbf{T}^{1\times n}$ získáme volbou báze B prostoru $\mathbf{V}$ a báze C prostoru $\mathbf{T}$. Pro lineární formy bázi C volíme vždy "kanonickou", tj. $C = (1)$.

Definice 6.40. Nechť $\mathbf{V}$ je konečně generovaný prostor nad tělesem $\mathbf{T}$, f je lineární forma na $\mathbf{V}$ a B je báze prostoru $\mathbf{V}$. *Maticí* formy f vzhledem k bázi B rozumíme řádkový vektor

$$[f]^B = [f]^B_{(1)} \ .$$

Podle definice matice lineárního zobrazení je matice f vzhledem k $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ rovná

$$[f]^B = (f(\mathbf{v}_1), f(\mathbf{v}_2), \ldots, f(\mathbf{v}_n)) \ .$$

Vzorec z tvrzení 6.6 o matici lineárního zobrazení má pro lineární formy tvar

$$f(\mathbf{x}) = [f]^B [\mathbf{x}]_B \ .$$

Označíme-li $[f]^B = (a_1, \ldots, a_n)$ a $[\mathbf{x}]_B = (x_1, \ldots, x_n)$, máme

$$f(\mathbf{x}) = (a_1, \ldots, a_n)(x_1, \ldots, x_n)^T = a_1x_1 + a_2x_2 + \cdots + a_nx_n \ .$$

6.5.2. *Řádkový pohled na soustavy lineárních rovnic.* Rozebereme nyní podrobněji řádkový pohled na soustavy lineárních rovnic. Diskuzi budeme provádět pouze pro homogenní soustavy rovnic, jejichž řešení je základem pro řešení obecných soustav.

Nechť tedy $A = (a_{ij})$ je matice typu $m \times n$ nad tělesem $\mathbf{T}$ s řádkovými vektory $\tilde{\mathbf{a}}_1, \ldots, \tilde{\mathbf{a}}_m$. Pro $i = 1, \ldots, m$ označme f_i lineární formu na $\mathbf{T}^n$, jejíž matice vzhledem ke kanonické bázi je $\tilde{\mathbf{a}}_i$, tj.

$$f_i(x_1, \ldots, x_n)^T = a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n \ .$$

Vektor $\mathbf{x} \in T^n$ je řešením soustavy $A\mathbf{x} = \mathbf{o}$ právě tehdy, když $f_1(\mathbf{x}) = 0, f_2(\mathbf{x}) = 0, \ldots, f_m(\mathbf{x}) = 0$. Jinými slovy, $A\mathbf{x} = \mathbf{o}$ právě tehdy, když $\mathbf{x} \in \mathrm{Ker}\, f_1$, …, $\mathbf{x} \in \mathrm{Ker}\, f_m$, neboli $\mathbf{x} \in \mathrm{Ker}\, f_1 \cap \cdots \cap \mathrm{Ker}\, f_m$. Jádro je, kromě případu nulové formy, vždy nadrovina (tj. podprostor dimenze $n-1$ v $\mathbf{T}^n$), jak ukazuje následující obecnější tvrzení.

Tvrzení 6.41. *Nechť* $\mathbf{V}$ *je vektorový prostor dimenze* n *nad tělesem* $\mathbf{T}$ *a* f *je lineární forma na* $\mathbf{V}$*. Je-li* f *nenulová, pak* $\dim \operatorname{Ker} f = n - 1$.

Důkaz. Podle věty 6.31 o dimenzi jádra a obrazu platí

$$\dim \operatorname{Ker} f + \dim \operatorname{Im} f = n$$

Je-li f nenulová forma, její obraz je celé T a $\dim \operatorname{Im} f = 1$, takže $\dim \operatorname{Ker} f + 1 = n$, čili $\dim \operatorname{Ker} f = n - 1$. □

Vraťme se k diskuzi řešení soustavy. Předpokládejme pro přehlednost, že žádná z forem $f_1, \dots, f_m$ není nulová. Každý řádek v takovém případě určuje nadrovinu $\operatorname{Ker} f_i$ a množina řešení je rovna průniku těchto nadrovin. Počítejme průniky postupně: uvažujme posloupnost

$$\mathbf{W}_1 = \operatorname{Ker} f_1,\ \mathbf{W}_2 = \operatorname{Ker} f_1 \cap \operatorname{Ker} f_2, \dots, \mathbf{W}_m = \operatorname{Ker} f_1 \cap \operatorname{Ker} f_2 \cap \dots \cap \operatorname{Ker} f_m.$$

W_{i+1} je tedy průnikem W_i a nadroviny $\operatorname{Ker} f_{i+1}$. Důsledkem věty o dimenzi součtu a průniku je (viz následující tvrzení 6.42), že $\mathbf{W}_{i+1}$ je buď rovno $\mathbf{W}_i$ (to nastane v případě, že $\operatorname{Ker} f_{i+1} \supseteq W_i$) a nebo má o jedničku menší dimenzi. Další věta pak ukazuje, že první možnost nastane právě tehdy, když je forma f_{i+1} lineární kombinací forem $f_1, \dots, f_i$. (Ekvivalentně, když je $\tilde{\mathbf{a}}_{i+1}$ lineární kombinací vektorů $\tilde{\mathbf{a}}_1, \dots, \tilde{\mathbf{a}}_i$.)

Tvrzení 6.42. *Nechť* $\mathbf{V}$ *je vektorový prostor dimenze* n*,* $\mathbf{W}$ *je podprostor* $\mathbf{V}$ *a* $\mathbf{U}$ *je podprostor* $\mathbf{V}$ *dimenze* $n-1$*. Pokud neplatí* $W \subseteq U$*, pak* $\dim(\mathbf{W} \cap \mathbf{U}) = \dim \mathbf{W} - 1$.

Důkaz. Pokud neplatí $W \subseteq U$, tak je $\mathbf{U}$ je vlastním podprostorem $\mathbf{W} + \mathbf{U}$, z čehož plyne, že $\mathbf{W} + \mathbf{U}$ má dimenzi alespoň n. Vyšší dimenzi ale mít nemůže jakožto podprostor prostoru $\mathbf{V}$, který má dimenzi n. Z věty 5.98 o dimenzi součtu a průniku dostáváme

$$\dim(\mathbf{W} \cap \mathbf{U}) = \dim \mathbf{W} + \dim \mathbf{U} - \dim(\mathbf{W} + \mathbf{U}) = \dim \mathbf{W} + n - 1 - n = \dim \mathbf{W} - 1\ .$$

□

Věta 6.43. *Nechť* $\mathbf{V}$ *je vektorový prostor dimenze* n *nad tělesem* $\mathbf{T}$ *a* $f_1, f_2, \dots, f_k, g$ *lineární formy na* $\mathbf{V}$*. Pak následující tvrzení jsou ekvivalentní.*

(1) $g \in \langle f_1, \dots, f_k \rangle$
(2) $\operatorname{Ker} g \supseteq \operatorname{Ker} f_1 \cap \dots \cap \operatorname{Ker} f_k$

Důkaz. Jednodušší je implikace (1) ⇒ (2). Předpokládejme, že $g = t_1 f_1 + \dots + t_k f_k$ pro nějaké skaláry $t_1, \dots, t_k \in T$. Pak pro libovolný vektor $\mathbf{x} \in \operatorname{Ker} f_1 \cap \dots \cap \operatorname{Ker} f_k$ platí $f_1(\mathbf{x}) = f_2(\mathbf{x}) = \dots = f_k(\mathbf{x}) = \mathbf{o}$, tedy také $g(\mathbf{x}) = (t_1 f_1 + \dots + t_k f_k)(\mathbf{x}) = t_1 f_1(\mathbf{x}) + \dots + t_k f_k(\mathbf{x}) = \mathbf{o}$.

Pro důkaz (2) ⇒ (1) zvolme nějakou bázi B prostoru $\mathbf{V}$. Označme C matici (typu $k \times n$) s řádkovými vektory $[f_1]^B, \dots, [f_k]^B$ a D matici (typu $(k+1) \times n$) s řádkovými vektory $[f_1]^B, \dots, [f_k]^B, [g]^B$.

Ukážeme, že $\operatorname{Ker} C = [\operatorname{Ker} f_1 \cap \dots \cap \operatorname{Ker} f_k]_B$. Uvažujme libovolný vektor $\mathbf{y} \in T^n$ a vektor $\mathbf{x} \in V$ takový, že $[\mathbf{x}]_B = \mathbf{y}$. Vektor $\mathbf{y}$ leží v $[\operatorname{Ker} f_1 \cap \dots \cap \operatorname{Ker} f_k]_B$ právě tehdy, když $\mathbf{x}$ leží v $\operatorname{Ker} f_1 \cap \dots \operatorname{Ker} f_k$, neboli $f_1(\mathbf{x}) = \dots = f_k(\mathbf{x}) = 0$. To nastane právě tehdy, když $[f_1]^B[\mathbf{x}]_B = \dots = [f_k]^B[\mathbf{x}]_B = 0$ (podle tvrzení 6.6). Podle definice matice C, toto je ekvivalentní podmínce $C[\mathbf{x}]_B = \mathbf{o}$, neboli $\mathbf{y} \in \operatorname{Ker} C$.

Podobně se ukáže, že $\operatorname{Ker} D = [\operatorname{Ker} f_1 \cap \dots \cap \operatorname{Ker} f_k \cap \operatorname{Ker} g]_B$. Z předpokladu, že $\operatorname{Ker} g$ obsahuje $\operatorname{Ker} f_1 \cap \dots \cap \operatorname{Ker} f_k$ ale plyne $\operatorname{Ker} f_1 \cap \dots \cap \operatorname{Ker} f_k \cap \operatorname{Ker} g = \operatorname{Ker} f_1 \cap \dots \cap \operatorname{Ker} f_k$. Platí proto $\operatorname{Ker} C = \operatorname{Ker} D$.

Podle věty 5.94 o dimenzi jádra a obrazu pak platí $\dim \operatorname{Im} C = \dim \operatorname{Im} D$ $(= n - \dim \operatorname{Ker} C = n - \dim \operatorname{Ker} D)$ a z věty 5.82 o rovnosti dimenze řádkového a sloupcového prostoru dostáváme $\dim \operatorname{Im} C^T = \dim \operatorname{Im} D^T$. Řádkový prostor matice C je podprostorem řádkového prostoru matice D, proto z rovnosti dimenzí vyplývá $\operatorname{Im} C^T = \operatorname{Im} D^T$. Tím pádem je poslední řádek $[g]^B$ matice D lineární kombinací řádků matice C, takže existují skaláry $t_1, \ldots, t_k$ takové, že

$$[g]^B = t_1[f_1]^B + \cdots + t_k[f_k]^B = [t_1 f_1 + \cdots + t_k f_k]^B$$

Rovnají-li se matice lineárních forem vzhledem k nějaké bázi, pak se lineární formy rovnají, tedy konečně dostáváme

$$g = t_1 f_1 + \cdots + t_k f_k \ .$$

□

Předchozí diskuze nám rovněž umožňuje lépe nahlédnout, proč se dimenze sloupcového prostoru matice A (typu $m \times n$) rovná dimenzi řádkového prostoru matice A.

Vypočítáme dvěma způsobu dimenzi $\operatorname{Ker} A$. Nejprve sloupcově. Podle věty o dimenzi jádra a obrazu platí $\dim \operatorname{Ker} A = n - \dim \operatorname{Im} A$. To si můžeme představovat tak, že každý bázový sloupec nám ubere jeden stupeň volnosti při řešení soustavy $A\mathbf{x} = \mathbf{o}$. Dimenze množiny řešení této soustavy je tak rovná n minus počet bázových sloupců, čili $n - \dim \operatorname{Im} A$.

Nyní řádkový pohled. Analogicky jako pro sloupce řekneme, že řádek matice A je bázový, pokud není lineární kombinací předchozích řádků. Dimenze $\dim \operatorname{Im} A^T$ řádkového prostoru je rovna počtu bázových řádků. Přechozí diskuze ukazuje, že při postupném přidávání rovnic (=řádků matice A), každý bázový řádek sníží dimenzi prostoru řešení o 1, takže $\dim \operatorname{Ker} A$ je rovno n minus počet bázových řádků, čili $n - \dim \operatorname{Im} A^T$.

Zdůvodnili jsme, že $\dim \operatorname{Ker} A = n - \dim \operatorname{Im} A = n - \dim \operatorname{Im} A^T$. Z toho okamžitě vidíme, že $\dim \operatorname{Im} A = \dim \operatorname{Im} A^T$.

Shrnutí šesté kapitoly

(1) Jsou-li $\mathbf{V}, \mathbf{W}$ lineární prostory nad stejným tělesem $\mathbf{T}$, pak zobrazení $f : V \to W$ nazýváme *lineární zobrazení* (nebo *homomorfismus*) z $\mathbf{V}$ do $\mathbf{W}$, pokud
   (a) $f(\mathbf{u}+\mathbf{v}) = f(\mathbf{u}) + f(\mathbf{v})$ pro libovolné $\mathbf{u}, \mathbf{v} \in V$ a
   (b) $f(t\mathbf{u}) = tf(\mathbf{u})$ pro libovolné $\mathbf{u} \in V$ a $t \in T$.

(2) Příklady lineárních zobrazení z $\mathbb{R}^2$ do $\mathbb{R}^2$.

(3) Jsou-li $\mathbf{V}$ a $\mathbf{W}$ lineární prostory nad tělesem $\mathbf{T}$, je-li $B = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ báze v prostoru $\mathbf{V}$, a jsou-li $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n \in W$ libovolné vektory, pak existuje právě jedno lineární zobrazení $f : \mathbf{V} \to \mathbf{W}$ splňující $f(\mathbf{v}_i) = \mathbf{w}_i$ pro každé $i \in \{1, 2, \ldots, n\}$.

(4) Jsou-li $\mathbf{V}, \mathbf{W}$ konečně generované lineární prostory nad tělesem $\mathbf{T}$, $f : \mathbf{V} \to \mathbf{W}$ lineární zobrazení, $B = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ báze ve $\mathbf{V}$, a C báze ve $\mathbf{W}$, pak *matice lineárního zobrazení f vzhledem k bázím B a C* je matice
$$[f]_C^B = ([f(\mathbf{v}_1)]_C \,|\, [f(\mathbf{v}_2)]_C \,|\, \cdots \,|\, [f(\mathbf{v}_n)]_C) \ .$$

(5) Jsou-li $\mathbf{V}, \mathbf{W}$ konečně generované lineární prostory nad tělesem $\mathbf{T}$, $B = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ báze prostoru $\mathbf{V}$, C báze prostoru $\mathbf{W}$, a $f : \mathbf{V} \to \mathbf{W}$ lineární zobrazení, pak pro libovolný prvek $\mathbf{x} \in V$ platí
$$[f(\mathbf{x})]_C = [f]_C^B \, [\mathbf{x}]_B \ .$$

(6) Jsou-li $\mathbf{V}, \mathbf{W}$ konečně generované lineární prostory nad tělesem $\mathbf{T}$, B báze $\mathbf{V}$, C báze $\mathbf{W}$ a $f : \mathbf{V} \to \mathbf{W}$ a M matice nad tělesem $\mathbf{T}$ splňující $[f(\mathbf{x})]_C = M\,[\mathbf{x}]_B$ pro každý prvek $\mathbf{x} \in \mathbf{V}$, pak $M = [f]_C^B$.

(7) 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 v aritmetickám prostoru $\mathbf{T}^i$.

(8) Jsou-li B, C dvě báze konečně generovaného prostoru $\mathbf{V}$, pak matice identického zobrazení z $\mathbf{V}$ do $\mathbf{V}$ se rovná matici přechodu od báze B k bázi C.

(9) Matice přechodu od B k B je vždy identická matice.

(10) Jsou-li $\mathbf{U}, \mathbf{V}, \mathbf{W}$ lineární prostory nad tělesem $\mathbf{T}$ a jsou-li $f : \mathbf{U} \to \mathbf{V}$ a $g : \mathbf{V} \to \mathbf{W}$ lineární zobrazení, pak složené zobrazení gf je lineární zobrazení $gf : \mathbf{U} \to \mathbf{W}$.

Jsou-li navíc prostory $\mathbf{U}, \mathbf{V}, \mathbf{W}$ konečně generované a jsou-li B báze v $\mathbf{U}$, C báze ve $\mathbf{V}$ a D báze ve $\mathbf{W}$, pak platí
$$[gf]_D^B = [g]_D^C \, [f]_C^B \ .$$

(11) Jsou-li $\mathbf{U}, \mathbf{V}$ lineární prostory nad tělesem $\mathbf{T}$ a $f : \mathbf{U} \to \mathbf{V}$ vzájemně jednoznačné lineární zobrazení, pak $f^{-1} : \mathbf{V} \to \mathbf{U}$ je také lineární zobrazení.

Jsou-li navíc $\mathbf{U}, \mathbf{V}$ konečně generované lineátní prostory dimenze n, B báze v $\mathbf{U}$ a C báze ve $\mathbf{V}$, pak platí
$$[f^{-1}]_B^C = \left([f]_C^B\right)^{-1} \ .$$

(12) Je-li $\mathbf{V}$ konečně generovaný lineární prostor nad tělesem $\mathbf{T}$, $f : \mathbf{V} \to \mathbf{V}$ lineární zobrazení, B, C dvě báze prostoru $\mathbf{V}$, a R matice přechodu od báze B k bázi C, pak
$$[f]_B^B = R^{-1} \, [f]_C^C \, R \ .$$

(13) Nechť $\mathbf{V}$, $\mathbf{W}$ jsou lineární prostory nad tělesem $\mathbf{T}$ a $f : \mathbf{V} \to \mathbf{W}$ je lineární zobrazení.
- Pokud je f prosté, říkáme že f je *monomorfismus*,
- pokud je f je prostor $\mathbf{W}$, říkáme že f je *epimorfismus*,
- pokud f je vzájemně jednoznačné, říkáme že f je *izomorfismus*,
- pokud $\mathbf{V} = \mathbf{W}$, říkáme že f je *endomorfismus* prostoru $\mathbf{V}$ (nebo také *lineární operátor* na prostoru $\mathbf{V}$),
- pokud $\mathbf{W} = \mathbf{T} = \mathbf{T}^1$, říkáme že f je *lineární forma* na $\mathbf{V}$,
- pokud je f izomorfismus a endomorfismus, říkáme, že f je *automorfismus* prostoru $\mathbf{V}$.

(14) Nechť $f : \mathbf{V} \to \mathbf{W}$ je lineární zobrazení. *Jádrem* f rozumíme množinu

$$\operatorname{Ker} f = \{\mathbf{x} \in V : f(\mathbf{x}) = \mathbf{o}\} \ .$$

Obraz (obor hodnot) f značíme $\operatorname{Im} f$, tj.

$$\operatorname{Im} f = \{f(\mathbf{x}) : \mathbf{x} \in V\} \ .$$

(15) Je-li $f : \mathbf{V} \to \mathbf{W}$ lineární zobrazení, pak f je prosté právě tehdy, když $\operatorname{Ker} f = \{\mathbf{o}\}$.

(16) Jsou-li $\mathbf{V}, \mathbf{W}$ konečně generované vektorové prostory, B je báze $\mathbf{V}$, C je báze $\mathbf{W}$, a $f : \mathbf{V} \to \mathbf{W}$ lineární zobrazení, pak
- jádro $\operatorname{Ker} f$ je podprostorem $\mathbf{V}$ a platí
$$[\operatorname{Ker} f]_B = \operatorname{Ker} [f]_C^B \ ,$$
- obraz $\operatorname{Im} f$ je podprostorem $\mathbf{W}$ a platí
$$[\operatorname{Im} f]_C = \operatorname{Im} [f]_C^B \ .$$

(17) Jsou-li $\mathbf{V}$ a $\mathbf{W}$ lineární prostory nad tělesem $\mathbf{T}$, $\mathbf{V}$ konečně generovaný lineární prostor, a $f : \mathbf{V} \to \mathbf{W}$ lineární zobrazení, pak jsou následující tvrzení ekvivalentní.
(a) Zobrazení f je prosté (monomorfismus),
(b) pro každou lineárně nezávislou posloupnost $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ ve $\mathbf{V}$ je posloupnost $(f(\mathbf{v}_1), \ldots, f(\mathbf{v}_k))$ lineárně nezávislá ve $\mathbf{W}$,
(c) existuje báze $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ prostoru $\mathbf{V}$ taková, že posloupnost $(f(\mathbf{v}_1), \ldots, f(\mathbf{v}_n))$ je lineárně nezávislá v $\mathbf{W}$.

(18) Jsou-li $\mathbf{V}$ a $\mathbf{W}$ lineární prostory nad tělesem $\mathbf{T}$, $\mathbf{V}$ konečně generovaný lineární prostor, a $f : \mathbf{V} \to \mathbf{W}$ lineární zobrazení, pak jsou následující tvrzení ekvivalentní.
(a) Zobrazení f je na W (epimorfismus),
(b) pro každou množinu generátorů $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ ve $\mathbf{V}$ je $\{f(\mathbf{v}_1), \ldots, f(\mathbf{v}_k)\}$ množina generátorů ve $\mathbf{W}$,
(c) existuje báze $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ prostoru $\mathbf{V}$ taková, že $\{f(\mathbf{v}_1), \ldots, f(\mathbf{v}_n)\}$ generuje $\mathbf{W}$.

(19) Jsou-li $\mathbf{V}$ a $\mathbf{W}$ lineární prostory nad tělesem $\mathbf{T}$, $\mathbf{V}$ konečně generovaný lineární prostor, a $f : \mathbf{V} \to \mathbf{W}$ lineární zobrazení, pak následující tvrzení jsou ekvivalentní.
(a) Zobrazení f je izomorfismus,
(b) pro každou bázi $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ ve $\mathbf{V}$ je $(f(\mathbf{v}_1), \ldots, f(\mathbf{v}_k))$ báze ve $\mathbf{W}$,
(c) existuje báze $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ prostoru $\mathbf{V}$ taková, že $(f(\mathbf{v}_1), \ldots, f(\mathbf{v}_n))$ je báze ve $\mathbf{W}$.

(20) Je-li $f : \mathbf{V} \to \mathbf{W}$ izomorfismus konečně generovaných prostorů, pak platí

(a) posloupnost $(\mathbf{v}_1, \dots, \mathbf{v}_k)$ je lineárně nezávislá ve $\mathbf{V}$ právě tehdy, když je posloupnost $(f(\mathbf{v}_1), \dots, f(\mathbf{v}_k))$ lineárně nezávislá v $\mathbf{W}$,
(b) množina $\{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ generuje $\mathbf{V}$ právě tehdy, když množina $\{f(\mathbf{v}_1), \dots, f(\mathbf{v}_k)\}$ generuje $\mathbf{W}$,
(c) posloupnost $(\mathbf{v}_1, \dots, \mathbf{v}_k)$ je báze $\mathbf{V}$ právě tehdy, když je posloupnost $(f(\mathbf{v}_1), \dots, f(\mathbf{v}_k))$ báze $\mathbf{W}$,
(d) $\dim V = \dim W$,
(e) množina $M \subseteq V$ je podprostorem prostoru $\mathbf{V}$ právě tehdy, když je $f(M) = \{f(\mathbf{m}) : \mathbf{m} \in M\}$ podprostorem prostoru $\mathbf{W}$,
(f) pokud $\mathbf{U} \leq \mathbf{V}$, pak f zúžené na U je izomorfismem $\mathbf{U} \to f(\mathbf{U})$. Speciálně $\dim \mathbf{U} = \dim f(\mathbf{U})$.

(21) Jsou-li $\mathbf{V}, \mathbf{W}$ konečně generované vektorové prostory nad tělesem $\mathbf{T}$ a $f : \mathbf{V} \to \mathbf{W}$ lineární zobrazení, pak

$$\dim(\operatorname{Ker} f) + \dim(\operatorname{Im} f) = \dim \mathbf{V} \ .$$

(22) Jsou-li $\mathbf{V}$ a $\mathbf{W}$ dva konečně generované prostory nad tělesem $\mathbf{T}$, pak následující tvrzení jsou ekvivalentní.
(a) Existuje izomorfismus $f : \mathbf{V} \to \mathbf{W}$.
(b) $\dim(\mathbf{V}) = \dim(\mathbf{W})$.

Část **6.5. Prostor lineárních zobrazení** byla vynechána a nebude zkoušena.

Klíčové znalosti ze šesté kapitoly nezbytné pro průběžné sledování přednášek s pochopením

(1) Definice lineárního zobrazení.
(2) Každé lineární zobrazení na konečně generovaném lineárním prostoru je jednoznačně určené svými hodnotami na prvcích jakékoliv báze. Tyto hodnoty můžeme zvolit libovolně.
(3) Matice $[f]_C^B$ lineárního zobrazení $f : \mathbf{V} \to \mathbf{W}$ vzhledem k bázi B v prostoru $\mathbf{V}$ a bázi C v prostoru $\mathbf{W}$.
(4) Formule $[f(\mathbf{x})]_C = [f]_C^B [\mathbf{x}]_B$.
(5) Složení dvou lineárních zpobrazení je lineární zobrazení.
(6) Formule $[gf]_D^B = [g]_D^C [f]_C^B$ pro matici složeného zobrazení.
(7) Inverzní zobrazení ke vzájemně jednoznačnému lineárnímu zobrazení je opět lineární zobrazení.
(8) Formule $[f^{-1}]_B^C = \left([f]_C^B\right)^{-1}$ pro matici inverzního zobrazení.
(9) Formule $[f]_B^B = [\mathrm{id}]_B^C [f]_C^C [\mathrm{id}]_C^B$ vyjadřující vztah mezi maticemi endomorfismu f vzhledem ke dvěma různým bázím.
(10) Definice jádra a oboru hodnot lineárního zobrazení.
(11) Charakterizace monomorfismů, epimorfismů a isomorfismů pomocí hodnot na nějaké bázi.
(12) Dva konečně generované lineární prostory jsou isomorfní právě když mají stejnou dimenzi.
(13) Věta o dimenzi jádra a obrazu lineárního zobrazení definovaného na konečně generovaném lineárním prostoru.

7. Determinant

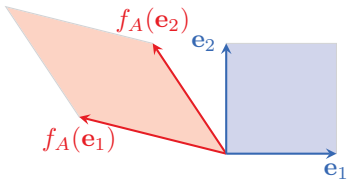
Cíl. *Budeme se věnovat pojmu determinantu matice. Motivací je porozumění, jak zobrazení určené maticí mění obsah (v $\mathbb{R}^2$) a objem (v $\mathbb{R}^3$). K definici budeme potřebovat permutace, naučíme se je různými způsoby zapisovat a určovat znaménko.*

7.1. **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.

7.1.1. *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 $\mathbf{v}$.

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

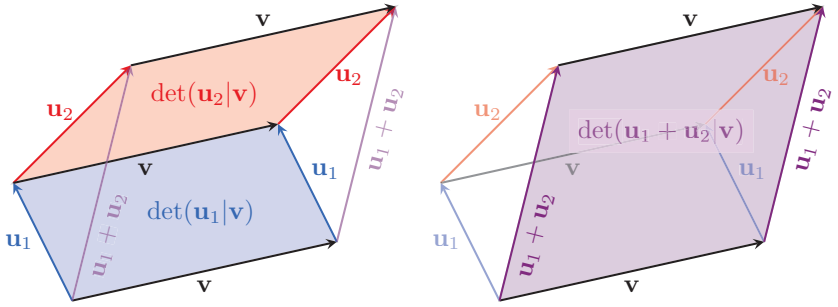
$$\det(t\mathbf{u}|\mathbf{v}) = t\det(\mathbf{u}|\mathbf{v}) = \det(\mathbf{u}|t\mathbf{v}) \quad .$$

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

$$\det(\mathbf{e}_1, \mathbf{e}_2) = 1, \quad \det(\mathbf{e}_2, \mathbf{e}_1) = -1 \ , \quad \det(\mathbf{e}_1, \mathbf{e}_1) = \det(\mathbf{e}_2, \mathbf{e}_2) = 0$$

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

$$A = (\mathbf{u}|\mathbf{v}) = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \quad .$$

$$\begin{aligned}
\det(A) &= \det(\mathbf{u}|\mathbf{v}) = \det(a_{11}\mathbf{e}_1 + a_{21}\mathbf{e}_2|a_{12}\mathbf{e}_1 + a_{22}\mathbf{e}_2) \\
&= \det(a_{11}\mathbf{e}_1|a_{12}\mathbf{e}_1 + a_{22}\mathbf{e}_2) + \det(a_{21}\mathbf{e}_2|a_{12}\mathbf{e}_1 + a_{22}\mathbf{e}_2) = \\
&= \det(a_{11}\mathbf{e}_1|a_{12}\mathbf{e}_1) + \det(a_{11}\mathbf{e}_1|a_{22}\mathbf{e}_2) + \\
&\quad + \det(a_{21}\mathbf{e}_2|a_{12}\mathbf{e}_1) + \det(a_{21}\mathbf{e}_2|a_{22}\mathbf{e}_2) = \\
&= a_{11}a_{12}\det(\mathbf{e}_1|\mathbf{e}_1) + a_{11}a_{22}\det(\mathbf{e}_1|\mathbf{e}_2) + \\
&\quad + a_{21}a_{12}\det(\mathbf{e}_2|\mathbf{e}_1) + a_{21}a_{22}\det(\mathbf{e}_2|\mathbf{e}_2) = \\
&= a_{11}a_{22} - a_{21}a_{12}
\end{aligned}$$

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.

7.1.2. *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 $\mathbb{R}^2$.

$$\det(t\mathbf{u}|\mathbf{v}|\mathbf{w}) = \det(\mathbf{u}|t\mathbf{v}|\mathbf{w}) = \det(\mathbf{u}|\mathbf{v}|t\mathbf{w}) = t\,\det(\mathbf{u}|\mathbf{v}|\mathbf{w})$$

$$\det(\mathbf{u}_1+\mathbf{u}_2+\mathbf{u}_3|\mathbf{v}|\mathbf{w}) = \det(\mathbf{u}_1|\mathbf{v}|\mathbf{w}) + \det(\mathbf{u}_2|\mathbf{v}|\mathbf{w}) + \det(\mathbf{u}_3|\mathbf{v}|\mathbf{w})$$

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.

$$A = (\mathbf{u}|\mathbf{v}|\mathbf{w}) = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \quad .$$

$$\begin{aligned}
\det(A) &= \det(\mathbf{u}|\mathbf{v}|\mathbf{w}) = \\
&= \det(a_{11}\mathbf{e}_1 + a_{21}\mathbf{e}_2 + a_{31}\mathbf{e}_3 | a_{12}\mathbf{e}_1 + a_{22}\mathbf{e}_2 + a_{32}\mathbf{e}_3 | a_{13}\mathbf{e}_1 + a_{23}\mathbf{e}_2 + a_{33}\mathbf{e}_3) \\
&= \sum_{k=1}^{3}\sum_{l=1}^{3}\sum_{m=1}^{3} a_{k1}a_{l2}a_{m3}\det(\mathbf{e}_k,\mathbf{e}_l,\mathbf{e}_m) = \\
&= a_{11}a_{22}a_{33}\det(\mathbf{e}_1,\mathbf{e}_2,\mathbf{e}_3) + a_{11}a_{32}a_{23}\det(\mathbf{e}_1,\mathbf{e}_3,\mathbf{e}_2) + \\
&\quad + a_{21}a_{12}a_{33}\det(\mathbf{e}_2,\mathbf{e}_1,\mathbf{e}_3) + a_{21}a_{32}a_{13}\det(\mathbf{e}_2,\mathbf{e}_3,\mathbf{e}_1) + \\
&\quad + a_{31}a_{12}a_{23}\det(\mathbf{e}_3,\mathbf{e}_1,\mathbf{e}_2) + a_{31}a_{22}a_{13}\det(\mathbf{e}_3,\mathbf{e}_2,\mathbf{e}_1) = \\
&= a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} + a_{31}a_{12}a_{23} - a_{11}a_{32}a_{23} - a_{31}a_{22}a_{13} - a_{21}a_{12}a_{33}
\end{aligned}$$

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).

7.2. **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 7.1. *Permutací* množiny X rozumíme bijekci $X \to X$. Množinu všech permutací na množině X značíme S_X. Pro množinu permutací na množině $X = \{1, 2, \ldots, n\}$, kde n je přirozené číslo, také používáme značení S_n.

Nejčastěji budeme používat permutace na konečné množině, konkrétně množině $\{1, 2, \ldots, n\}$. 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 $\pi\pi^{-1} = \pi^{-1}\pi = \mathrm{id}_X$.

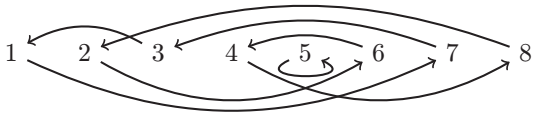
Tím pádem nemusíme při skládání psát závorky a také můžeme řešit jednoduché rovnice typu $\alpha\rho\beta = \gamma$, kde α, β, γ jsou dané permutace, podobným způsobem jako pro čísla, akorát musíme dát pozor na nekomutativitu.

7.2.1. *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.

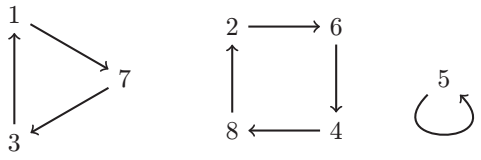


Obrázek 66. Obrázek permutace

Když graf trochu překreslíme, vidíme, že permutace je sjednocením nezávislých cyklů.

To není náhoda, každá permutace je složením nezávislých cyklů.

Definice 7.2. *Cyklus délky k* je permutace na X splňující $\pi(x_1) = x_2$, $\pi(x_2) = x_3$, $\ldots$, $\pi(x_{k-1}) = x_k$, $\pi(x_k) = x_1$ a $\pi(y) = y$ pro každé $y \in X \setminus \{x_1, x_2, \ldots, x_k\}$, kde x_1, x_2, $\ldots$, x_k jsou po dvou různé prvky X. Zapisujeme $\pi = (x_1\ x_2\ \ldots\ x_k)$.



OBRÁZEK 67. Lepší obrázek permutace

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 7.3. *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 7.4. 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 7.5. 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 7.6. *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

$$(1\ 2\ 3) = (1\ 3)(1\ 2) = (1\ 2)(2\ 3) = (1\ 2)(2\ 3)(1\ 2)(1\ 2) = (1\ 2)(1\ 3)(2\ 3)(1\ 2) = \dots$$

7.2.2. *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 7.7. *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 7.8. *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 7.9. Permutace π na konečné množině X se nazývá *sudá*, pokud nastane možnost (1) v důsledku 7.8. 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 7.10.

$$\operatorname{sgn}\left((1\ 2\ 3\ 4)(5\ 6\ 7)(8\ 9)(10\ 11)\right) = -1$$

protože má permutace v cyklickém zápisu 3 cykly sudé délky.

Znaménko inverzní permutace a složené permutace je určené znaménkem původních permutací.

Tvrzení 7.11. *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) $\operatorname{sgn}(\pi\rho) = \operatorname{sgn}(\pi)\operatorname{sgn}(\rho)$.

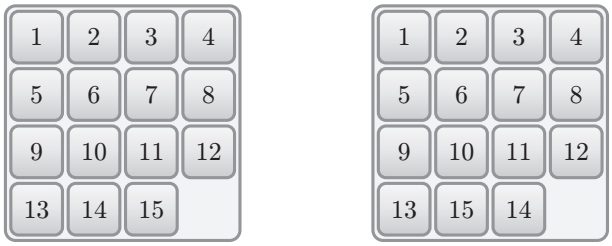
Důkaz.

(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 7.12. 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 68. 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).

7.2.3. *Počet permutací.* Jak již asi víte, počet permutací na n-prvkové množině $X = \{x_1, x_2, \ldots, x_n\}$ je $n!$. Máme totiž n možností, kam zobrazit x_1, pak $n-1$ možností, kam zobrazit x_2, atd. Dohromady $n(n-1)\ldots 1 = n!$.

Počet lichých permutací spočítáme z následujícího pozorování, které také použijeme pro důkazy tvrzení o determinantech.

Tvrzení 7.13. *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 7.11). 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 $n!/2$.

7.3. **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.

7.3.1. *Definice.* Podobně definujeme determinant libovolné **čtvercové** matice nad libovolným tělesem.

Definice 7.14. 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 7.15. 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:

$$\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{21}a_{12}$$

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 7.16. V případě $n = 3$ máme šest permutací v S_3 – identické permutace a trojcykly jsou sudé, transpozice jsou liché. Odpovídající sčítanci jsou:

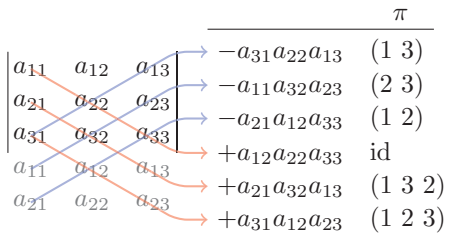
π	
id	$a_{11}a_{22}a_{33}$
(1 2 3)	$a_{21}a_{32}a_{13}$
(1 3 2)	$a_{31}a_{12}a_{23}$
(2 3)	$-a_{11}a_{32}a_{23}$
(1 3)	$-a_{31}a_{22}a_{13}$
(1 2)	$-a_{21}a_{12}a_{33}$

a opět dostáváme vzorec odvozený výše. Mnemotechnickou pomůckou je tzv. *Sarrusovo pravidlo* na obrázku.

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**.

7.3.2. *Základní vlastnosti.* Pro horní trojúhelníkové matice vypočítáme determinant jako součin prvků na diagonále.

Tvrzení 7.17. *Je-li A horní trojúhelníková matice, pak* $\det(A) = a_{11}a_{22} \dots a_{nn}$.



Obrázek 69. Sarrusovo pravidlo

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 $\pi(3) = 3$, $\pi(4) = 4$, $\dots$, $\pi(n) = n$.

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 7.18. *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 7.11) 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 7.13). □

Dokázané tvrzení jinými slovy říká, že

$$\det(A) = \sum_{\pi\in S_n} \operatorname{sgn}(\pi) a_{1,\pi(1)} a_{2,\pi(2)} \dots a_{n,\pi(n)} \ ,$$

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 7.19. *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

$$\begin{aligned}
&\det\left(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_{i-1}|\ \mathbf{v}_i + \mathbf{u}\ |\mathbf{v}_{i+1}|\dots|\mathbf{v}_n\right)\\
&= \sum_{\pi\in S_n} \operatorname{sgn}(\pi) a_{\pi(1),1}a_{\pi(2),2}\dots a_{\pi(i-1),i-1}(a_{\pi(i),i} + b_{\pi(i)})a_{\pi(i+1),i+1}\dots a_{\pi(n),n}\\
&= \sum_{\pi\in S_n} (\operatorname{sgn}(\pi) a_{\pi(1),1}a_{\pi(2),2}\dots a_{\pi(n),n} +\\
&\qquad + \operatorname{sgn}(\pi) a_{\pi(1),1}a_{\pi(2),2}\dots a_{\pi(i-1),i-1}b_{\pi(i)}a_{\pi(i+1),i+1}\dots a_{\pi(n),n})\\
&= \sum_{\pi\in S_n} \operatorname{sgn}(\pi) a_{\pi(1),1}a_{\pi(2),2}\dots a_{\pi(n),n}\\
&\qquad + \sum_{\pi\in S_n} \operatorname{sgn}(\pi) a_{\pi(1),1}a_{\pi(2),2}\dots a_{\pi(i-1),i-1}b_{\pi(i)}a_{\pi(i+1),i+1}\dots a_{\pi(n),n}\\
&= \det\left(\mathbf{v}_1|\dots|\mathbf{v}_{i-1}|\ \mathbf{v}_i\ |\mathbf{v}_{i+1}|\dots|\mathbf{v}_n\right) + \det\left(\mathbf{v}_1|\dots|\mathbf{v}_{i-1}|\ \mathbf{u}\ |\mathbf{v}_{i+1}|\dots|\mathbf{v}_n\right)\ .
\end{aligned}$$

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 7.13).

(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 7.13). 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.

$$\begin{aligned}
& \det(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_{i-1}|\mathbf{v}_i + t\mathbf{v}_j|\mathbf{v}_{i+1}|\dots|\mathbf{v}_n) \\
& = \det(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_n) + \det(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_{i-1}|\ t\mathbf{v}_j\ |\mathbf{v}_{i+1}|\dots|\mathbf{v}_n) \\
& = \det(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_n) + t\det(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_{i-1}|\ \mathbf{v}_j\ |\mathbf{v}_{i+1}|\dots|\mathbf{v}_n) \\
& = \det(\mathbf{v}_1|\mathbf{v}_2|\dots|\mathbf{v}_n)
\end{aligned}$$

□

Protože determinant matice se shoduje s determinantem transponované matice (tvrzení 7.18), 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 7.17), 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.

Příklad 7.20. 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 7.21. 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.

7.3.3. *Další kriterium regularity.* Z tvrzení 7.19 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 7.22. *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 7.17). Tento součin je nulový právě tehdy, když má B nulový řádek, což se stane právě tehdy, když A je singulární podle bodu (5) věty 4.59 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 7.23. *Minorem* řádu k matice A rozumíme determinant matice vzniklé z A výběrem k řádků a k sloupců.

Příklad 7.24. 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 7.25. *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.

7.3.4. *Determinant součinu.* Další aplikací tvrzení 7.19 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 4.66), 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 7.26 (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 5.86 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 7.27. *Je-li A regulární matice, pak* $\det\left(A^{-1}\right) = \det(A)^{-1}$.

Důkaz. Podle věty o determinantu součinu je

$$1 = \det(I) = \det\left(AA^{-1}\right) = \det(A)\det\left(A^{-1}\right) \ ,$$

z čehož dostaneme vzorec vydělením $\det(A)$. (Determinant matice A je nenulový podle tvrzení 7.22.) □

7.3.5. *Cramerovo pravidlo.* Jako poslední aplikaci základních vlastností determinantu dokážeme *Cramerovo pravidlo* pro řešení soustav lineárních rovnic s regulární maticí.

Věta 7.28 (Cramerovo pravidlo)**.** *Nechť $A = (\mathbf{a}_1|\dots|\mathbf{a}_n)$ 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.

$$A_j = (\mathbf{a}_1|\mathbf{a}_2|\dots|\mathbf{a}_{j-1}|\mathbf{b}|\mathbf{a}_{j+1}|\dots|\mathbf{a}_n) \ .$$

Důkaz. Vztah $A\mathbf{x} = \mathbf{b}$ můžeme zapsat jako

$$x_1\mathbf{a}_1 + x_2\mathbf{a}_2 + \cdots + x_n\mathbf{a}_n = \mathbf{b} \ .$$

Dostáváme

$$\begin{aligned}
\det(A_j) &= \det(\mathbf{a}_1|\mathbf{a}_2|\dots|\mathbf{a}_{j-1}|\mathbf{b}|\mathbf{a}_{j+1}|\dots|\mathbf{a}_n) \\
&= \det\left(\mathbf{a}_1|\mathbf{a}_2|\dots|\mathbf{a}_{j-1}|\sum_{k=1}^{n} x_k\mathbf{a}_k|\mathbf{a}_{j+1}|\dots|\mathbf{a}_n\right) \\
&= \det(\mathbf{a}_1|\mathbf{a}_2|\dots|\mathbf{a}_{j-1}|x_j\mathbf{a}_j|\mathbf{a}_{j+1}|\dots|\mathbf{a}_n) \\
&= x_j \det(\mathbf{a}_1|\mathbf{a}_2|\dots|\mathbf{a}_{j-1}|\mathbf{a}_j|\mathbf{a}_{j+1}|\dots|\mathbf{a}_n) = x_j \det(A) \ ,
\end{aligned}$$

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 7.19) 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 7.22). Spíše než pro praktické počítání se využívá ve výpočtech a úvahách, kdy se může hodit explicitní vzorec pro nějakou složku řešení.

Příklad 7.29. 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

$$x_3 = \frac{3}{2} = 4 \ .$$

7.4. **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 7.30. 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 7.31. 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 7.32 (o rozvoji podle sloupce)**.** *Je-li A čtvercová matice řádu n a $j \in \{1, 2, \ldots, n\}$, 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

$$\begin{aligned}
\det(A) &= \sum_{\pi \in S_n} \operatorname{sgn}(\pi) a_{\pi(1),1} a_{pi(2),2} \cdots a_{\pi(n),n} \\
&= \sum_{\pi \in S_n, \pi(n)=n} \operatorname{sgn}(\pi) a_{\pi(1),1} a_{pi(2),2} \cdots a_{\pi(n),n} \\
&= \sum_{\pi \in S_n, \pi(n)=n} \operatorname{sgn}(\pi) a_{\pi(1),1} a_{pi(2),2} \cdots a_{\pi(n-1),n-1} = \\
&= (-1)^{n+n} \sum_{\pi \in S_{n-1}} \operatorname{sgn}(\pi) a_{\pi(1),1} a_{pi(2),2} \cdots a_{\pi(n-1),n-1} = A_{nn} \ .
\end{aligned}$$

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 $\{1, 2, \ldots, n-1\}$ (to platí, protože tyto dvě permutace mají stejný redukovaný cyklický zápis).

2. krok. Pro libovolné $i, j \in \{1, 2, \ldots, n\}$, 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 $\sigma = (n\ (n-1)\ \ldots\ i)$ a posunutí j-tého sloupce na n-té místo odpovídá permutaci sloupců $\rho = (n\ (n-1)\ \ldots\ j)$. Podle bodu (3) tvrzení 7.19 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. Označme $A = (\mathbf{a}_1|\dots|\mathbf{a}_n)$. Pomocí 2.kroku a bodů (1) a (2) z tvrzení 7.19 nyní výpočet dokončíme.

$$\begin{aligned}\det(A) &= \det(\mathbf{a}_1|\mathbf{a}_2|\dots|\mathbf{a}_n)\\ &= \det\left(\mathbf{a}_1|\mathbf{a}_2|\dots|\mathbf{a}_{j-1}|\ \sum_{i=1}^{n} a_{ij}\mathbf{e}_i\ |\mathbf{a}_{j+1}|\dots|\mathbf{a}_n\right)\\ &= \sum_{i=1}^{n} a_{ij}\det(\mathbf{a}_1|\mathbf{a}_2|\dots|\mathbf{a}_{j-1}|\ \mathbf{e}_i\ |\mathbf{a}_{j+1}|\dots|\mathbf{a}_n)\\ &= \sum_{i=1}^{n} a_{ij}A_{ij}\ .\end{aligned}$$

(Rovněž jsme využili triviální skutečnosti, že algebraický doplněk prvku a_{ij} se nezmění, změníme-li j-tý sloupec.) □

Díky tvrzení 7.18 o transponování můžeme provádět rozvoj podle řádku:

$$\det(A) = \sum_{j=1}^{n} a_{ij}A_{ij} = a_{i1}A_{i1} + a_{i2}A_{i2} + \dots + a_{in}A_{in}\ .$$

Příklad 7.33. 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 7.34. Spočítáme znovu determinant v příkladu 7.20.

$$\begin{vmatrix} 2 & 4 & 2\\ 7 & -1 & 4\\ 5 & 0 & -6 \end{vmatrix} = \begin{vmatrix} 30 & 0 & 18\\ 7 & -1 & 4\\ 5 & 0 & -6 \end{vmatrix} = (-1)^{2+2}(-1)\begin{vmatrix} 30 & 18\\ 5 & -6 \end{vmatrix}$$

$$= 180 + 90 = 270$$

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 7.35. 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.

7.4.1. *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 7.36 (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 jejím j-tým sloupcem. Protože B má dva sloupce stejné, je B singulární (má lineárně závislé sloupce, takže můžeme použít bod (3) pozorování 5.88), a proto $\det(B) = 0$ podle kritéria v tvrzení 7.22. 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 7.37. *Adjungovanou maticí* ke čtvercové matici A rozumíme matici $\mathrm{adj}(A)$ 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 7.38. *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 $A_{1i}a_{1j} + A_{2i}a_{2j} + \dots A_{ni}a_{nj}$. 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 7.39. 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 7.40. Spočítáme inverzní matici k reálné matici

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

Nejdřív spočítáme adjungovanou matici.

$$\begin{aligned} \operatorname{adj}(A) &= \begin{pmatrix} \begin{vmatrix} 4 & -2 \\ 2 & 5 \end{vmatrix} & -\begin{vmatrix} 1 & -3 \\ 2 & 5 \end{vmatrix} & \begin{vmatrix} 1 & -3 \\ 4 & -2 \end{vmatrix} \\ -\begin{vmatrix} 3 & -2 \\ 0 & 5 \end{vmatrix} & \begin{vmatrix} -2 & -3 \\ 0 & 5 \end{vmatrix} & -\begin{vmatrix} -2 & -3 \\ 3 & -2 \end{vmatrix} \\ \begin{vmatrix} 3 & 4 \\ 0 & 2 \end{vmatrix} & -\begin{vmatrix} -2 & 1 \\ 0 & 2 \end{vmatrix} & \begin{vmatrix} -2 & 1 \\ 3 & 4 \end{vmatrix} \end{pmatrix} \\ &= \begin{pmatrix} 24 & -11 & 10 \\ -15 & -10 & -13 \\ 6 & 4 & -11 \end{pmatrix} \end{aligned}$$

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

$$A^{-1} = -\frac{1}{81} \begin{pmatrix} 24 & -11 & 10 \\ -15 & -10 & -13 \\ 6 & 4 & -11 \end{pmatrix} = \frac{1}{81} \begin{pmatrix} -24 & 11 & -10 \\ 15 & 10 & 13 \\ -6 & -4 & 11 \end{pmatrix} \ .$$

7.5. **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

$$c^k - d^k = (c-d)(c^{k-1} + c^{k-2}d + c^{k-3}d^2 + \cdots + cd^{k-2} + d^{k-1}) \ .$$

$$\begin{vmatrix} a_2-a_1 & a_2^2-a_1^2 & \dots & a_2^{n-1}-a_1^{n-1} \\ a_3-a_1 & a_3^2-a_1^2 & \dots & a_3^{n-1}-a_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_n-a_1 & a_n^2-a_1^2 & \dots & a_n^{n-1}-a_1^{n-1} \end{vmatrix} = (a_2-a_1)(a_3-a_1)\dots(a_n-a_1)\cdot$$

$$\cdot \begin{vmatrix} 1 & a_2+a_1 & a_2^2+a_2a_1+a_1^2 & \dots & a_2^{n-2}+a_2^{n-3}a_1+\dots+a_1^{n-2} \\ 1 & a_3+a_1 & a_3^2+a_3a_1+a_1^2 & \dots & a_3^{n-2}+a_3^{n-3}a_1+\dots+a_1^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n+a_1 & a_n^2+a_na_1+a_1^2 & \dots & a_n^{n-2}+a_n^{n-3}a_1+\dots+a_1^{n-2} \end{vmatrix}$$

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.

$$\begin{vmatrix} 1 & a_2+a_1 & a_2^2+a_2a_1+a_1^2 & \dots & a_2^{n-2}+a_2^{n-3}a_1+\dots+a_1^{n-2} \\ 1 & a_3+a_1 & a_3^2+a_3a_1+a_1^2 & \dots & a_3^{n-2}+a_3^{n-3}a_1+\dots+a_1^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n+a_1 & a_n^2+a_na_1+a_1^2 & \dots & a_n^{n-2}+a_n^{n-3}a_1+\dots+a_1^{n-2} \end{vmatrix}$$

$$= \begin{vmatrix} 1 & a_2+a_1 & a_2^2+a_2a_1+a_1^2 & \dots & a_2^{n-2} \\ 1 & a_3+a_1 & a_3^2+a_3a_1+a_1^2 & \dots & a_3^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n+a_1 & a_n^2+a_na_1+a_1^2 & \dots & a_n^{n-2} \end{vmatrix} = \dots = \begin{vmatrix} 1 & a_2+a_1 & a_2^2 & \dots & a_2^{n-2} \\ 1 & a_3+a_1 & a_3^2 & \dots & a_3^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n+a_1 & a_n^2 & \dots & a_n^{n-2} \end{vmatrix}$$

$$= \begin{vmatrix} 1 & a_2 & a_2^2 & \dots & a_2^{n-2} \\ 1 & a_3 & a_3^2 & \dots & a_3^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \dots & a_n^{n-2} \end{vmatrix} = V(a_2,\dots,a_n)$$

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 $\mathbf{u}, \mathbf{v}$.

2. Promyslete si detailně důkaz tvrzení 7.3.

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 každou množinu X a permutaci $\pi \in S_X$ je zobrzení $f : S_X \to S_X$ definované předpisem $f(\rho) = \pi^{-1}\rho\pi$ vzájemně jednoznačné.

5. Dokažte, že pro libovolné $k \in \mathbb{N}$ má permutace $\pi\rho\pi^{-1}$ na konečné množině X 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 $\rho\pi$.

6. Označme k počet cyklů v cyklickém zápisu permutace $\pi \in S_n$ (počítáme i cykly délky 1!). Dokažte, že $\operatorname{sgn}(\pi) = (-1)^{n+k}$.

7. Vypište z definice výraz pro determinant matice řádu 4.

8. Najděte vzorec pro determinant čtvercových matic $A = (a_{ij})$ řádu n takových, že $a_{ij} = 0$ kdykoliv $i > n + 1 - j$.

9. 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 $\det(A) = \det(A_{11}) \det(A_{22}) \dots \det(A_{rr})$.

10. 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 $\det(A) \neq \det(A_{11}) \det(A_{22}) - \det(A_{12}) \det(A_{21})$.

11. Dokažte, že pro regulární matici A řádu n platí $\det(\operatorname{adj}(A)) = \det(A)^{n-1}$.

12. Dokažte tvrzení 7.25

Shrnutí sedmé kapitoly

(1) Je-li $A = (a_{ij})$ matice řádu 2 nad tělesem $\mathbf{T}$, pak definujeme determinant $\det A$ jako skalár $a_{11}a_{22} - a_{12}a_{21}$.
(2) Geometrický význam absolutní hodnoty $|\det A|$ determinantu matice $A = (\mathbf{a}_1|\mathbf{a}_2)$ řádu 2 je obsah rovnoběžníku určeného vektory $\mathbf{a}_1, \mathbf{a}_2$.
(3) Je-li $A = (a_{ij})$ matice řádu 3 nad tělesem $\mathbf{T}$, pak definujeme determinant $\det A$ jako skalár

$$a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} + a_{31}a_{12}a_{23} - a_{11}a_{32}a_{23} - a_{31}a_{22}a_{13} - a_{21}a_{12}a_{33} \ .$$

(4) Geometrický význam absolutní hodnoty $|\det A|$ determinantu matice $A = (\mathbf{a}_1|\mathbf{a}_2|\mathbf{a}_3)$ řádu 3 je objem rovnoběžnostěnu určeného vektory $\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3$.
(5) *Permutací* na množině X rozumíme vzájemně jednoznačné zobrazení $X \to X$. Množinu všech permutací na množině X značíme S_X. Pro množinu permutací na množině $X = \{1, 2, \ldots, n\}$, kde n je přirozené číslo, také používáme značení S_n.
(6) Permutace π, ρ na množině X můžeme složit (jako zobrazení), složení $\pi\,\rho$ je opět permutace na X. Inverzní zobrazení ρ^{-1} k permutaci $\rho \in S_X$ je opět permutace na množině X. Identické zobrazení ι_X na množině X je permutace na X.
(7) Skládání permutací na množině X je binární operace na S_X, která má následující vlastnosti.
   (a) Pro libovolné $\pi, \rho, \sigma \in S_X$ platí $\pi(\rho\sigma) = (\pi\rho)\sigma$.
   (b) Pro libovolné $\pi \in S_X$ platí $\mathrm{id}_X\,\pi = \pi\,\mathrm{id}_X = \pi$.
   (c) Pro libovolné $\pi \in S_X$ platí $\pi\pi^{-1} = \pi^{-1}\pi = \mathrm{id}_X$.
(8) Permutaci na konečné množině X můžeme zapsat buď tabulkou nebo grafem.
(9) *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 $x_1, x_2, \ldots, x_k$ jsou po dvou různé prvky X. Zapisujeme $\pi = (x_1\ x_2\ \ldots\ x_k)$.
(10) Cykly nazýváme *nezávislé*, pokud jsou množiny prvků vyskytující se v cyklech disjunktní.
(11) *Transpozice* je cyklus délky 2, tj. permutace tvaru $\pi = (x\ y)$.
(12) Každou permutaci na konečné množině X lze zapsat jako složení nezávislých cyklů. Tento zápis je jednoznačný až na pořadí cyklů (a cykly délky 1).
(13) *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*.
(14) Každá permutace na konečné množině je složením transpozic.
(15) Je-li X 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.
(16) Pro libovolnou permutaci π na konečné množině X nastane jedna z následujících možností:
   (a) 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.

(b) 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.

(17) Permutace π na konečné množině X se nazývá *sudá*, pokud nastane možnost (1) z předchozího bodu. Rovněž říkáme, že *znaménko* π *je* 1 a píšeme $\operatorname{sgn}(\pi) = 1$.

V opačném případě je π *lichá*, má znaménko -1 a píšeme $\operatorname{sgn}(\pi) = -1$.

(18) Nechť X je konečná množina a $\pi, \rho \in S_X$. Pak platí
(a) $\operatorname{sgn}(\mathrm{id}_X) = 1$,
(b) $\operatorname{sgn}(\pi^{-1}) = \operatorname{sgn}(\pi)$ a
(c) $\operatorname{sgn}(\pi\rho) = \operatorname{sgn}(\pi)\operatorname{sgn}(\rho)$.

(19) Pro libovolnou množinu X a permutaci $\pi \in S_X$ jsou následující zobrazení vzájemně jednoznačná:
(a) $f : S_X \to S_X$ definované předpisem $f(\rho) = \rho^{-1}$,
(b) $g : S_X \to S_X$ definované předpisem $g(\rho) = \pi\,\rho$,
(c) $h : S_X \to S_X$ definované předpisem $h(\rho) = \rho\,\pi$.

(20) Důsledkem předchozího bodu je, že počet sudých permutací konečné množiny s $n \geq 2$ prvky je stejný jako počet lichých permutací a rovná se tedy $n!/2$.

(21) Je-li $A = (a_{ij})$ čtvercová matice nad tělesem $\mathbf{T}$ řádu n, pak definujeme *determinant* matice A předpisem

$$\det(A) = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) a_{\pi(1),1} a_{\pi(2),2} \dots a_{\pi(n),n} \ .$$

(22) Je-li $A = (a_{ij})$ horní trojúhelníková matice řádu n, pak $\det(A) = a_{11}a_{22}\dots a_{nn}$.

(23) Pro libovolnou čtvercovou matici A platí $\det(A) = \det\left(A^T\right)$.

(24) Pro libovolnou matici $A = (a_{ij})$ řádu n platí

$$\det(A) = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) a_{1,\pi(1)} a_{2,\pi(2)} \dots a_{n,\pi(n)} \ .$$

(25) Pro čtvercovou matici $A = (a_{ij}) = (\mathbf{a}_1|\cdots|\mathbf{a}_n)$ řádu n nad $\mathbf{T}$, libovolný vektor $\mathbf{b} = (b_1, \dots, b_n)^T$, každé $j \in \{1, \dots, n\}$ a skalár $t \in \mathbf{T}$ platí
(a) $\det(\mathbf{a}_1|\cdots|\mathbf{a}_{j-1}|\mathbf{a}_j+\mathbf{b}|\mathbf{a}_{j+1}|\cdots|\mathbf{a}_n) = \det(\mathbf{a}_1|\cdots|\mathbf{a}_{j-1}|\mathbf{a}_j|\mathbf{a}_{j+1}|\cdots|\mathbf{a}_n) + \det(\mathbf{a}_1|\cdots|\mathbf{a}_{j-1}|\mathbf{b}|\mathbf{a}_{j+1}|\cdots|\mathbf{a}_n)$,
(b) $\det(\mathbf{a}_1|\cdots|\mathbf{a}_{j-1}|t\mathbf{a}_j|\mathbf{a}_{j+1}|\cdots|\mathbf{a}_n) = t\det(\mathbf{a}_1|\cdots|\mathbf{a}_{j-1}|\mathbf{a}_j|\mathbf{a}_{j+1}|\cdots|\mathbf{a}_n) = t\det A$.

(26) Prohození dvou řádků čtvercové matice $A = (a_{ij})$ změní znaménko $\det A$. Podobně prohození dvou sloupců matice A změní znaménko $\det A$.

(27) Má-li matice $A = (a_{ij}) = (\mathbf{a}_1|\cdots|\mathbf{a}_n)$ nad $\mathbf{T}$ dva stejné sloupce, platí $\det A = 0$.

(28) Přičteme-li v matici $A = (\mathbf{a}_1|\cdots|\mathbf{a}_n)$ násobek jednoho řádku (sloupce) k jinému řádku (sloupci), determinant $\det(A)$ se nezmění.

(29) Pro každou elementární matici E a libovolnou matici A, obě řádu n, platí $\det(EA) = \det(E) \cdot \det(A)$.

(30) Čtvercová matice je regulární právě tehdy, když $\det(A) \neq 0$.

(31) Pro libovolné matice A, B řádu n nad stejným tělesem platí $\det(AB) = \det(A)\det(B)$.

(32) Je-li A regulární matice, pak $\det\left(A^{-1}\right) = \det(A)^{-1}$.

(33) *Cramerovo pravidlo.* Je-li $A = (\mathbf{a}_1|\dots|\mathbf{a}_n)$ 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.

$$A_j = (\mathbf{a}_1|\mathbf{a}_2|\dots|\mathbf{a}_{j-1}|\mathbf{b}|\mathbf{a}_{j+1}|\dots|\mathbf{a}_n) \ .$$

(34) Je-li $A = (a_{ij})$ čtvercová matice řádu n a $i, j \in \{1, 2, \dots, n\}$, pak *algebraickým doplňkem* (též *kofaktorem*) prvku a_{ij} matice A rozumíme skalár

$$m_{ij} = (-1)^{i+j} \det(M_{ij}) \ ,$$

kde M_{ij} je matice řádu $n-1$, která vznikne z A vynecháním i-tého řádku a j-tého sloupce.

(35) *Věta o rozvoji podle sloupce.* Je-li A čtvercová matice řádu n a $j \in \{1, 2, \dots, n\}$, pak

$$\det(A) = \sum_{i=1}^{n} a_{ij} m_{ij} = a_{1j} m_{1j} + a_{2j} m_{2j} + \dots + a_{nj} m_{nj} \ .$$

(36) *Kofaktorová matice* ke čtvercové matici $A = (a_{ij})$ je matice $M = (m_{ij})$ tvořená algebraickými doplňky prvků a_{ij}. *Adjungovaná matice* k matici A je matice M^T transponovaná ke kofaktorové matici M, značíme ji $\operatorname{adj}(A)$

(37) *Věta o falešném rozvoji.* Je-li A čtvercová matice řádu n a $j, k \in \{1, 2, \dots, n\}$, $j \neq k$, pak

$$0 = \sum_{i=1}^{n} a_{ij} m_{ik} = a_{1j} m_{1k} + a_{2j} m_{2k} + \dots + a_{nj} m_{nk} \ .$$

(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

$$A^{-1} = \frac{\operatorname{adj}(A)}{\det(A)} \ .$$

(39) Úloha na nalezení polynomu stupně nejvýše $n-1$ s koeficienty v tělese $\mathbf{T}$, který má předepsané hodnoty v n bodech $a_1, a_2, \dots, a_n \in \mathbf{T}$ vede na řešení soustavy lineární rovnic a maticí

$$\begin{pmatrix} 1 & a_1 & a_1^2 & \dots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \dots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \dots & a_n^{n-1} \end{pmatrix} \ .$$

(40) Tato matice se nazývá *Vandermondova matice* a její determinant *Vandermondův determinant* určený prvky $a_1, a_2, \dots, a_n$.

(41) Hodnota Vandermondova determinantu určeného prvky $a_1, a_2, \dots, a_n$ je

$$\prod_{1 \leq i < j \leq n} a_j - a_i \ .$$

(42) Vandermondova matice určená prvky $a_1, a_2, \dots, a_n$ je regulární právě když jsou prvky $a_1, a_2, \dots, a_n$ navzájem různé.

Klíčové znalosti ze sedmé kapitoly nezbytné pro průběžné sledování přednášek s pochopením

(1) Geometrický význam determinantu matic řádu 2 a 3.
(2) Definice permutace a skládání permutací, jejich základní vlastnosti.
(3) Znaménko permutace, známenko inverzní permutace a znaménko složení dvou permutací, sudé a liché permutace.
(4) Definice determinantu, rovnost $\det(A) = \det(A)^T$, determinant trojúhelníkové matice.
(5) Vliv elementárních úprav matice na hodnotu jejího determinantu.
(6) Věta o součinu determinantů.
(7) Matice je regulární právě když má nenulový determinant.
(8) Věta o rozvoji determinantu podle řádku nebo podle sloupce.

Obsah